

**AMERICA UNDER CYBER SIEGE: PREVENTING
AND RESPONDING TO RANSOMWARE ATTACKS**

HEARING
BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

—————
JULY 27, 2021
—————

Serial No. J-117-30

—————

Printed for the use of the Committee on the Judiciary



www.judiciary.senate.gov
www.govinfo.gov

—————
U.S. GOVERNMENT PUBLISHING OFFICE

COMMITTEE ON THE JUDICIARY

RICHARD J. DURBIN, Illinois, *Chair*

| | |
|----------------------------------|--|
| PATRICK J. LEAHY, Vermont | CHARLES E. GRASSLEY, Iowa, <i>Ranking Member</i> |
| DIANNE FEINSTEIN, California | LINDSEY O. GRAHAM, South Carolina |
| SHELDON WHITEHOUSE, Rhode Island | JOHN CORNYN, Texas |
| AMY KLOBUCHAR, Minnesota | MICHAEL S. LEE, Utah |
| CHRISTOPHER A. COONS, Delaware | TED CRUZ, Texas |
| RICHARD BLUMENTHAL, Connecticut | BEN SASSE, Nebraska |
| MAZIE K. HIRONO, Hawaii | JOSH HAWLEY, Missouri |
| CORY A. BOOKER, New Jersey | TOM COTTON, Arkansas |
| ALEX PADILLA, California | JOHN KENNEDY, Louisiana |
| JON OSSOFF, Georgia | THOM TILLIS, North Carolina |
| | MARSHA BLACKBURN, Tennessee |

JOSEPH ZOGBY, *Chief Counsel and Staff Director*

KOLAN L. DAVIS, *Republican Chief Counsel and Staff Director*

C O N T E N T S

OPENING STATEMENTS

| | Page |
|--------------------------------|------|
| Durbin, Hon. Richard J. | 1 |
| Grassley, Hon. Charles E. | 3 |
| Feinstein, Hon. Dianne | 4 |

WITNESSES

| | |
|---|-----|
| Downing, Richard W. | 5 |
| Prepared statement | 39 |
| Responses to written questions | 85 |
| Goldstein, Eric | 8 |
| Prepared statement | 55 |
| Responses to written questions | 99 |
| Sheridan, Jeremy | 10 |
| Prepared statement | 62 |
| Responses to written questions | 113 |
| Vorndran, Bryan A. | 6 |
| Prepared statement | 69 |
| Questions submitted with no response returned | 79 |

APPENDIX

| | |
|--------------------------------------|-----|
| Items submitted for the record | 171 |
|--------------------------------------|-----|

AMERICA UNDER CYBER SIEGE: PREVENTING AND RESPONDING TO RANSOMWARE ATTACKS

TUESDAY, JULY 27, 2021

UNITES STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m., in Room 226, Dirksen Senate Office Building, Hon. Richard J. Durbin, Chair of the Committee, presiding.

Present: Senators Durbin [presiding], Feinstein, Whitehouse, Klobuchar, Coons, Blumenthal, Hirono, Booker, Ossoff, Grassley, Graham, Cornyn, Cruz, Sasse, Hawley, Cotton, Tillis, and Blackburn.

OPENING STATEMENT OF HON. RICHARD J. DURBIN, A U.S. SENATOR FROM THE STATE OF ILLINOIS

Chair DURBIN. The hearing will come to order. Today, the Committee will discuss the growing number of ransomware attacks which are increasingly disrupting our economy and our lives. Today's hearing is the first ever Full Committee hearing of the Judiciary Committee on ransomware. Marks the first congressional testimony this year by the Justice Department and FBI on this threat.

Majority Leader Schumer asked the Senate Committees to review how the agencies under their jurisdiction are responding to the ransomware threat. Ranking Member Grassley also requested today's hearing, and we consulted with his staff on choosing the witness panel. We'll hear from a panel of experts from the Department of Justice, the FBI, Cybersecurity and Infrastructure Security Agency, a.k.a. CISA, I believe, and the Secret Service.

They will discuss the scope of the threat and what the agencies are doing to prevent it. They'll also provide guidance on best practices on how businesses and organizations can protect themselves. Before we get started, I'd like to turn to a brief video that gives us a sense of the ransomware threat.

[Video is shown.]

Chair DURBIN. It's about more than money and inconvenience. The harm of ransomware can affect real lives. An example: On October 28th of last year, an oncology nurse named Colleen Kargil was preparing a patient for a chemotherapy infusion when she made an unsettling discovery. She couldn't log in to her computer. Every time she typed in her credentials, the system would boot her out. She tried logging in from a back-up computer. That didn't

work either. Instead, she was greeted by a red circle with a diagonal line drawn through it.

At that moment, she realized that her hospital, the largest medical system in the State of Vermont, had been infiltrated. The network had been shut down. The hackers behind the attack were holding the hospital's data hostage, which meant Colleen and her colleagues couldn't access patient data for their cancer patients. They had to try to recreate patient chemotherapy protocols from memory and copies of old faxes. The hospital's electronic medical system would remain offline for nearly a month.

Colleen told the New York Times those weeks were the worst of her life. She's not alone. Colleen and her patients are just a few of the many Americans who've been victimized by ransomware attacks.

Nearly every organization and industry is vulnerable. Hospitals, school districts, local governments, nonprofits, businesses large and small. Here's how it works: Hackers break into your computer system, lock up your data, demand a ransom payment, often through untraceable cryptocurrency, for the return of the data. Though any person or entity can be targeted in a ransomware attack, it's been estimated that small businesses make up over half of the victims.

These attacks can have permanent damage. Last year, it took an average of 9 months for a business to fully recover from a ransomware attack. Even the biggest and most profitable companies in the world are at risk. Earlier this year, we remember the cybercrime syndicate knocking out Colonial Pipeline, the largest pipeline operator in the United States. That shutdown sparked a nationwide panic that had customers waiting in line at gas stations for hours. The incident brought the ransomware attack into plain view.

They're becoming more frequent, more destructive. The tools needed to commit them are easily accessible. Last year, global ransom payments reached \$350 million. A recent New Yorker piece talked about the average payment for ransomware; 2018, average payment, \$7,000. 2019, \$41,000; 2020, somewhere between \$200 and \$300,000.

In recent months, barely a day has gone by without news of a ransomware attack. By one estimate, American businesses, healthcare facilities and organizations and State and local governments are projected to endure more than 65,000 ransomware attacks this year alone.

This is a criminal business model that is spreading. If someone wants to commit an attack, they can easily purchase or lease ready-to-use ransomware. According to one expert, it's quote "way too easy to get into this. Just hire it out." There's been an incredible commoditization of the entire process. I'm concerned, as well, that ransomware criminals often operate with impunity in Russia and other nations. Those nations are unwilling to prosecute or pursue the evildoers.

We need to attack this new reality. We need new protocols for preventing and responds—responding to ransomware attacks. The President understands it. His administration is taking a whole-of-Government approach to prevent, deter, and respond. They recently launched a cross-Government task force to coordinate offensive and

defensive measures against these attacks and to help businesses. The administration also launched *stopransomware.gov*, a new website that provides one central location for ransomware resources.

These efforts are welcome because when it comes to ransomware, it's not just our money that's at stake. It's sensitive information, a personal sense of security, and, truthfully, our Nation's security. It's a critical challenge, and this Committee will do its part to meet it, starting with today's hearing. I turn to my friend and Ranking Member, Chuck Grassley.

**STATEMENT OF HON. CHARLES E. GRASSLEY,
A U.S. SENATOR FROM THE STATE OF IOWA**

Senator GRASSLEY. Thank you, Chairman Durbin, for holding this hearing. I thank you for agreeing—I'd better turn this off. I thank you for agreeing to hold this hearing, an important bipartisan hearing on a problem of ransomware. You hear about it every day. I've appreciated working with you on this subject and look forward to continuing to work if we decide that legislation is necessary.

The threat that we face from ransomware is increasing. Criminal actors are using techniques like phishing emails to gain access to data of business, nonprofit or government. The criminal actors then lock the data down and demand a large ransom. Usually very difficult to trace. Virtual currency like Bitcoin is used to pay for it. Yet paying the ransom is no guarantee that the victim will have their data returned, and that they will not be victimized again and asked to pay yet another ransom.

Earlier this year, we had FBI director, Chris Wray, compare the challenge of fighting ransomware to those we faced after 9/11. Estimates on the amount of ransom paid in 2020 ran into the hundreds of millions of dollars. Ransomware has targeted schools, local governments, and during this pandemic, can you believe it, even hospitals and healthcare providers.

In May, two massive ransomware attacks hit a critical supply of gas, the Colonial Pipeline and a major supplier of meat, the JBS slaughtering operation. These events created very disturbing questions about the security of our supply of essential goods like fuels and food.

Since that time, I've received questions from many Iowans about what we can do as a nation and as individuals to fight the threat of ransomware. This hearing will help us answer those questions.

Ransomware does not just affect the deeper pockets of large companies like Colonial Pipeline and JBS. An estimated three out of every four victims of ransomware is a small business. Small businesses already operate on thin margins, and many have been pushed to a brink by the pandemic. I'm glad that we'll be hearing today what Government agencies like Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security can do to help small business owners to practice good cyber protection to avoid ransomware attacks.

We will also be hearing which investigators like FBI and the Secret Service can do for those who have been victimized. Ransomware often originates from countries with permissive law

enforcement environments that allow these cybercriminals to flourish. So-called ransomware as a service is a business model—can you believe that? Employed by Congress—criminal networks, such as Dark Side and Revil. Dark Side and Revil are behind many of the recent acts—recent attacks.

These criminal organizations work like illicit software providers, creating ransomware and leasing it to other criminal actors like—known as affiliates for a share of the profits. We will be hearing from the Department of Justice how these criminal actors can be targeted and punished.

The situation would be dire enough if ransomware was used only by sophisticated criminal actors in countries unwilling to help bring them to justice. However, just last week, the Biden administration and many countries which are allies of the United States formally blamed China for a massive hack of Microsoft Exchange email servers. Hackers operating under the umbrella of China’s own Ministry of State Security appeared to have used the hack to engage in ransomware schemes for their own profit. They will have extorted millions in ransom from our own U.S. victims.

I have spoken many times on the dangers of cyberattacks, theft of intellectual property, and other aggressive behavior by China. I fear that ransomware will be a new method used by the Chinese Communist Party against Americans and I will be pursuing opportunities to combat that danger. I look forward to hearing the testimony about what the executive branch agencies are doing to fight ransomware and what we as a country can do, and I thank all of our witnesses for attending.

Chair DURBIN. Thanks, Senator Grassley. Senator Feinstein asked to say a few words.

**STATEMENT OF HON. DIANNE FEINSTEIN,
A U.S. SENATOR FROM THE STATE OF CALIFORNIA**

Senator FEINSTEIN. Yes. Just a brief comment, Mr. Chairman. I’ve been on this Committee a long time. It’s really not often that you pick up your binder and something in it immediately alerts you. Ransomware immediately alerts me to a real problem. We’ve had 2,474 complaints related to them presented to the FBI, and all I wanted to say is that I think we’ve got to take this very seriously and pass some legislation to deal with it. Thank you.

Chair DURBIN. Thank you, Senator. I want to thank this panel of four witnesses. We have extraordinary career Federal employees who are involved in pursuing this issue.

Richard Downing served since 2015 as the Deputy Assistant Attorney General for the Criminal Division in the Department of Justice. He oversees the work of the Criminal Division’s computer crime and intellectual property section, child exploitations, obscenity section.

Bryan Vorndran is appointed Assistant Director for the FBI’s Cyber Division in March. Previously Deputy Assistant Director of Criminal Investigation, the Assistant Special Agent in charge of cyber and counter-intelligence programs in Baltimore.

Eric Goldstein, appointed in February as the Executive Assistant Director for Cybersecurity at the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security.

Finally, Jeremy Sheridan, appointed in April as the Assistant Director of the Office of Investigations at the United States Secret Service.

Each witness will have 5 minutes, and then there will be follow-up questions asked for 5 minutes by each member of the panel. We start this off with swearing in the witnesses. Ask you all please rise. Raise your right hand.

[Witnesses are sworn in.]

Chair DURBIN. May the record reflect that the witnesses agreed in the affirmative. Mr. Downing, you're first up.

**STATEMENT OF RICHARD W. DOWNING, DEPUTY
ASSISTANT ATTORNEY GENERAL CRIMINAL DIVISION,
U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC**

Mr. DOWNING. Good morning, Chairman Durbin, Ranking Member Grassley, and Members of the Committee. Thank you for the opportunity to testify about the Department of Justice's efforts against ransomware.

I'd like to emphasize three themes from my statement for the record. First, ransomware is a very serious problem, but it is also a tough problem to solve. Second, the Department has had some recent successes in addressing that problem, but we are redoubling our efforts. Third, Congress can help.

The ransomware attacks over the past months have made it very clear that ransomware is a serious threat to our public safety and our national and economic security. It has been used to attack governments, police departments, and even hospitals during the pandemic. The number of attacks and the size of demands has skyrocketed in the last year. Some demands now exceed \$50 million. Even worse, many actors now steal information from victims, like trade secrets or client files, and release that information on the internet if the ransom is not paid.

A number of factors make it hard to solve this problem in the way that we might normally address a crime problem. Ransomware attacks are often committed by offenders outside our borders. Investigators often need to make requests for assistance to foreign law enforcement agencies to gather evidence in other countries, a process that can be cumbersome and time-consuming. Countries like Russia have refused to extradite offenders living within their borders or prosecute them themselves.

To make matters worse, many of these crimes involve anonymizing technologies, such as the Tor network and anonymity-enhanced cryptocurrencies, making it hard to identify perpetrators.

Finally, investigations are hindered because many victim companies choose not to report to Federal authorities. I'll touch on this more in a moment.

Despite these difficulties, we have had some recent successes, and we're keenly focused on doing more. In May, most of the ransom paid by the Colonial Pipeline was recovered. In January, the United States, Canada, and Bulgaria disrupted NetWalker, a ransomware variant that was used to attack hospitals during the pandemic. Also in January, the Department and international partners disrupted Emotet, a Botnet that was used to send ransomware to victim computers.

We are not resting on these laurels. Department leadership created a ransomware and digital exploitation task force to focus attention on this problem. This task force will help to make sure that the Department is doing all it can to arrest offenders and disrupt their crimes, as well as to assure robust coordination with partners across the Federal Government and within the private sector. It is a key part of what must be a whole-of-Government solution. We are committed to working with partner agencies across the executive branch to address the threat.

What can Congress do to help? First and foremost, we face a gap in reporting from victims. Without prompt reporting, investigative opportunities are lost. Our ability to assist other victims facing the same attacks is degraded, and the Government and Congress does not have a full picture of the threat facing American companies. Congress should enact legislation to require victims to report.

We recommend that a reporting requirement include ransomware attacks, critical infrastructure attacks and other high impact breaches. We think reports should be prompt and should include details about any ransom demand or payment. Legislation should designate a single point where victims can file reports, with immediate sharing to all Federal—relevant Federal agencies. Victims should not be worse off for helping the Government. They should maintain whatever legal privilege they had on that information prior to sharing the information.

Finally, we would ask Congress to enact legislation that would help the Department disrupt ransomware and mass hacking. This legislation would give courts the authority to enjoin ransomware and botnets affecting 100 or more computers. Our proposal also contains other helpful amendments that would enhance our ability to charge offenders and disrupt attacks.

I want to thank the Committee again for providing me the opportunity to discuss these important issues, and I'm happy to answer your questions when that time comes. Thank you.

[The prepared statement of Mr. Downing appears as a submission for the record.]

Chair DURBIN. Thanks, Mr. Downing. Mr. Vorndran.

**STATEMENT OF BRYAN A. VORNDRAN, ASSISTANT
DIRECTOR, CYBER DIVISION, FEDERAL BUREAU
OF INVESTIGATION, WASHINGTON, DC**

Mr. VORNDRAN. Good morning, Chairman Durbin, Ranking Member Grassley, and Members of this Committee. Thank you for the opportunity to be here to represent the FBI in our cyber program, and to sit with our Federal partners as a unified front against this growing ransomware threat in the country.

As you know, this hearing comes at an important time. Your title says it all. As the cyber community learns from past incidents and works to ensure all the Nation's people, companies, and levels of government are protected from future ransomware attacks.

At the FBI, we've been sounding the alarm on ransomware for some time now. The 5-year cyber strategy Director Wray announced last year gives us a road map to continue to mitigate this threat. Using this strategy, our goal is to not only pursue our own actions, but also work seamlessly with our domestic and inter-

national partners to defend our networks, attribute malicious activity, sanction bad behavior, and take the fight to our adversaries overseas. Our success relies on our ability together to impose risk and consequences on malicious cyber actors, and to do so through joint operations sequence for maximum, durable impact.

We have to target the entire criminal ecosystem, including malware developers, money launderers, and shady infrastructure providers, and bring together the insight of Government partners, cyber security firms, service providers, and victims in this common fight.

Two successes made possible by our cyber strategy were the recent Emotet and NetWalker disruptions, as mentioned by Mr. Downing. In January, in coordination with the Intelligence Community, an unprecedented number of foreign law enforcement partners in the private sector, we disrupted Emotet, one of the longest lasting, costly, and sophisticated cybercrime services.

In the 9-months leading up to the takedown, it's estimated Emotet caused hundreds of millions of dollars in damage and infected more than 1.6 million computers. That same month, we also worked with international partners to disrupt the NetWalker ransomware variant, which had been responsible for impacting numerous victim companies, municipalities, and schools. As part of that operation, we obtained Federal charges, a subject was arrested, and we seized nearly \$27.5 million in cryptocurrency.

Today, you'll hear from four agencies working together on the front lines of this fight, but ransomware has become so widespread it can't be solved by Federal action alone. We need Congress and the public to assist. We need a Federal cyber incident-reporting standard for breaches that pose significant risks because inconsistent voluntary reporting is simply not enough. We need affected entities to report to the Federal Government as promptly as possible and within a defined timeframe because we must act swiftly.

We need ransomware reports to include all information about the ransom demand and any potential ransom payment information because we can't let cybercriminals extort victims without repercussions.

This may scare some folks out there. We understand why you may be hesitant to report an attack and to work with law enforcement. We do get that. I want you to know we're here to help you. As the FBI does with all victims we encounter in our work, we aim to inform, support, and assist ransomware victims in navigating the aftermath of crime and the criminal justice process with dignity and resilience.

We want to empower victims of cybercrime because by working with law enforcement you move us closer to the day when the people who victimized you can't strike again. When we receive information from you, we're going to use it to help limit damage to you and others, to improve our national security, and to keep others from being victimized. When victims work with us, everybody wins except the bad guys.

You all have constituents who have been hurt by ransomware, and I had personal experience with this issue as an FBI Special Agent in charge. When I was in New Orleans in 2019, the Louisiana Governor's office declared two separate states of emergency

following a wave of ransomware attacks against school districts across the State and Government Agencies. As the father of school-age children, this hits home.

We're here today to inform you, your constituents, and the American public about ransomware to make sure everyone knows this is a whole-of-Government, but perhaps more importantly, a whole-of-society issue, and to make it clear what people can do to protect themselves and how to respond if they unfortunately become a victim. Again, thank you for inviting us to address this important topic, and I look forward to answering your questions.

[The prepared statement of Mr. Vorndran appears as a submission for the record.]

Chair DURBIN. Thank you, Mr. Vorndran. Mr. Goldstein.

**STATEMENT OF ERIC GOLDSTEIN, EXECUTIVE
ASSISTANT DIRECTOR FOR CYBERSECURITY,
CYBERSECURITY AND INFRASTRUCTURE SECURITY
AGENCY, ARLINGTON, VIRGINIA**

Mr. GOLDSTEIN. Chairman Durbin, Ranking Member Grassley, Members of the Committee, thank you for the chance to speak with you today on behalf of CISA and about this urgent threat. Thank you, Mr. Chairman, for your opening video, which really reflects the urgency of this issue, and the fact that ransomware intrusions can now impact the national critical functions upon which American families, businesses, and all levels of government depend.

As the lead agency for civilian cybersecurity, CISA plays a key role in managing the risk of ransomware. We don't do it alone. One theme today will be that this is truly a whole-of-Government and whole-of-Nation effort in which all agencies are aligned toward a shared outcome, reducing the prevalence and impact of ransomware intrusions affecting our country.

Many of CISA's efforts to mitigate ransomware are focused on ensuring that all organizations in this country, big and small, across sectors, understand three key points. The first is that ransomware intrusions can affect any organization, from a small business to a Fortune 100 corporation. The second is that ransomware intrusions can cause prolonged downtime, significant financial implications, and potential impacts to public health and safety. The third is that investing in cybersecurity best practices has been shown to be demonstrably effective in reducing the prevalence and impact of these intrusions.

To this latter point, Chairman, as you mentioned, just last week, CISA and our partners across the interagency, including the FBI and the Secret Service, launched *stopransomware.gov* a new whole-of-Government website intended to provide organizations across the country with access to resources to prevent intrusions, respond to intrusions, and report them when they occur. This website builds upon our earlier campaigns on this topic, including our secretary's Ransomware Sprint and our earlier Reduce the Risk of Ransomware campaign.

We also offer a variety of no-cost voluntary services that businesses around the can take advantage of to help secure their networks and identify risks. In particular, I'll call out a ransomware readiness assessment, which is a self-assessment tool that helps or-

ganizations identify their preparedness for responding to and managing a ransomware intrusion.

Going forward, it is very clear that we, as a Government and as a Nation, need to do more to address ransomware intrusions and the broader cybersecurity risks we face. The stakes are simply too high.

First, CISA and our partners across Government must gain increased visibility into cybersecurity intrusions and threats affecting our Nation's businesses and State, local, Tribal, and Territorial entities. Without this visibility, we are unable to effectively share information, develop timely alerts, help victims, and understand impacts of these intrusions to the national critical functions upon which we all depend.

As my colleagues have noted, we look forward to working with Congress on incident-reporting legislation that will significantly increase the volume of incidents that are reported to CISA and our Government partners today to ensure that we can act with urgency to render assistance and understand the breadth of these campaigns affecting American companies.

Second, we must continue to invest in and mature our voluntary partnerships with the private sector and our State and local partners across the country. Over the past several months, the inter-agency has worked in collaboration with the private sector to focus on cyber-defense against known ransomware campaigns, and, going forward, we are shortly launching our new cyber-defense collaboration effort, as established by last year's NDAA to formalize and bring together the private sector and Government in a way that will allow us to exercise the best of the private sector and Government in managing these risks.

Last, we must recognize that at least in the near term, we cannot prevent all intrusions and must drive a focus on resilience and functional continuity to ensure that intrusions don't impact the critical functions upon which Americans depend. To this end, the Cyber Response and Recovery Fund, an effort recommended by the Cyberspace Solarium Commission, and recently passed by the Senate, would provide CISA with additional resources and capacity to respond rapidly to catastrophic cyber incidents.

Our Nation is facing unprecedented risk from these kind of intrusions. CISA and our partners across the agency are deeply focused on this risk, and we all must continue to redouble this focus, working with the private sector, with our State, local, Tribal, and Territorial partners, and with Congress to make sure that we are minimizing risks to our people, to our businesses, and to our Government.

Thank you again for the chance to be here, and I very much look forward to your questions.

[The prepared statement of Mr. Goldstein appears as a submission for the record.]

Chair DURBIN. Thanks, Mr. Goldstein. Mr. Sheridan.

**STATEMENT OF JEREMY SHERIDAN, ASSISTANT
DIRECTOR, OFFICE OF INVESTIGATIONS, UNITED
STATES SECRET SERVICE, WASHINGTON, DC**

Mr. SHERIDAN. Good morning, Chairman Durbin, Ranking Member Grassley, and Members of this Committee. Thank you for inviting me to testify on the threat of ransomware, the growing risks it poses to the American people, and the work of the U.S. Secret Service and our partners to hold criminal actors accountable.

In my role as the Assistant Director of Investigations, I lead our more than 160 global field offices and direct our network of cyber fraud task forces. I work to ensure that we are effectively detecting and arresting those actors engaging in the criminal violations we are authorized to investigate, while fully supporting our diverse protective requirements across the world.

The U.S. Secret Service is a relatively small, specialized agency within the broader Federal law enforcement community. Our investigative expertise capabilities and statutory authorities are all focused on our mission to protect America's financial infrastructure and payment systems from criminal abuse.

The Secret Service's distinct focus allows us to keep pace with rapid changes in the financial sector, and with the criminal schemes seeking to exploit those changes. Indeed, the Secret Service has been conducting investigations of cybercrime since well before they were even called cybercrimes.

Our approach has remained consistent over the decades. By pursuing a list of proceeds, developing detailed evidence on transnational cybercrime networks, and by working with our partners around the globe, we have brought to justice some of the world's most infamous cybercriminals, including many who were thought to be beyond the reach of law enforcement. In particular, we have prioritized the investigation of key enablers of cybercrime, such as illicit digital money platforms, dark web forums, and other services that enable transnational cybercriminal activities, like the use of ransomware.

Our long investigative tradition focused specifically on financial crimes leads us to view today's ransomware crisis through a historical lens, one driven by three complex and interrelated factors.

First, the swelling profitability of these attacks, largely as the result of the growth of cryptocurrencies as a form of extortion payment. Second, the inadequate security systems connected to the internet. Third, perhaps most importantly, the maturation of a cybercriminal ecosystem that we have not sufficiently suppressed and is now engaged in increasingly brazen attacks.

It does us no service to sugar coat the reality of today's situation. Cybercriminal networks are emboldening and expanding. Today, ransomware is menacing our economy and our Homeland Security. Cybercriminals are making more money and doing more harm to our society than ever before. They are creating a highly destabilizing force in international relations and risking unintended escalation as States look to consider their response options.

To reiterate what my colleagues here today have all emphasized, there's no silver bullet for addressing the ransomware threat or our mounting cybersecurity risks. Federal law enforcement can act in meaningful ways to improve the current situation.

First, we must reduce the profitability of ransomware campaigns by improving our ability to detect and interdict cybercrime proceeds. This will require a significant investment in tools, training, and personnel at home, as well as strengthened partnerships overseas.

Second, we must work with technology companies and internet users to improve their defenses and resilience against cyber threats.

Third, we must dramatically intensify our national and international efforts to investigate, arrest, and prosecute those engaged in transnational cybercrimes, including ransomware.

Absent these combined efforts, I anticipate an increase in both the severity and frequency of highly disruptive ransomware attacks. Attacks that will make recent incidents seem rather mild by comparison. This should not be a political or geopolitical debate. Ransomware is endangering us all. Criminals are not targeting just big businesses, but schools, city governments, local police departments, and other services upon which the American people depend.

Progress is possible. The Secret Service's successful investigations of the recent ransomware attacks on the Washington, DC, Metropolitan Police Department and the City of Atlanta show that we can hold criminals accountable.

Our March, 2020 alert, which notified dozens of U.S. hospitals and healthcare providers of criminal presence in their networks, potentially preventing numerous ransomware attacks shows the ways that proactive information sharing can tangibly reduce cybersecurity risk. However, going forward, meaningful gains will require a renewed commitment on the part of the international community to make it clear that such destructive criminal activities are acceptable in a civilized world.

Thank you again for the opportunity to appear before you today, and for your continued support of the U.S. Secret Service. I look forward to working closely with this Committee and with other Members of Congress on our shared priorities and welcome your questions.

[The prepared statement of Mr. Sheridan appears as a submission for the record.]

Chair DURBIN. Thank you very much, Mr. Sheridan. Mr. Downing, on June 7th, the Department of Justice announced that it seized \$2.3 million in cryptocurrency paid to the hackers behind the May ransomware attack on Colonial Pipeline. The criminal syndicate named Dark Side demanded a ransom in Bitcoins and Colonial Pipeline paid it. According to DOJ press release, law enforcement was able to review the Bitcoin public ledger, track transfers of Bitcoin, and identify \$2.3 million in proceeds from these ransom payments.

It seems, for lack of a better reference, that cryptocurrency and Bitcoins are the coin of the realm when it comes to this ransomware. What can we do? What specific laws should we enact in the United States to be responsive to this and diminish the role of cryptocurrency?

Mr. DOWNING. Thank you very much for the question. I agree completely that the cryptocurrency has, unfortunately, fueled this rise of crime. It has two key aspects to it. It's often anonymous and

it is nonreversible. That is, once it's passed to the criminals, it's very difficult claw it back.

We do not have a current proposal to enhance our authority to track or to interdict these kinds of things, but it's something that's very much under consideration. We definitely see this as an increased problem and look to the laws that we already have on the books, like the Bank Secrecy Act, to enforce the rules and regulations that are already applying to cryptocurrency exchanges and other actors in this space.

Chair DURBIN. That's exactly the point. We enacted laws so that the transfer of certain amounts really required disclosures to the Government so we could monitor those. It's not a perfect system by any means. It would seem that the Bitcoin and cryptocurrency need to be subject to some sort of review, surveillance, or regulation, as well.

Let me ask you another question and to the panel, and maybe someone else would like to take it on. There was an article on June 7th in the New Yorker entitled, "The Go-Between," by Rachel Monroe. It talked about the similarities between kidnapping and ransomware, and she wrote that about three-quarters of Fortune 500 companies eventually invested in kidnap and ransom insurance. There was some discomfort in the industry that they were funneling money to the mafia, terrorist groups, and criminal gangs, but by establishing some sort of a method to this madness, they were able to recover 97 percent of the kidnap victims without harm.

Several countries went an extra step. Particularly Italy, Colombia, and the United Kingdom banned kidnap and ransom insurance. The argument was made in this article that that really had a negative impact. Countries that banned kidnap insurance drove negotiations underground.

We're dealing in a world of cyber-insurance, and those who are trying to buy some protection through the insurance mechanism for their vulnerability. Is there any value to looking at the kidnapping experience in banning that insurance and deciding whether that has any beneficial aspects to it?

Mr. VORNDRAN. Sir, I can start the conversation on that question. When we go back several years, it's at least our belief and understanding from public records that the insurance industry really started within cyber so that we could drive better cyber hygiene. You know, I think the question that we should all be asking ourselves: Is that what has actually happened? Has the implementation of cybersecurity insurance driven better cyber hygiene?

From our perspective with dealing with target entities or victims, when we talk with them, the insurance availability is a big piece of their decision calculus about whether they do or don't pay, and my opinion would be that within the interagency, there's ongoing conversations about the value or lack thereof insurance. I think it's probably a conversation that should be had within this Committee, as well.

Chair DURBIN. It certainly would—is an important one, and I suppose I can argue both sides. I'm glad to see you're making a review of it at this point. It seems to me it facilitates the payment in these circumstances, and it may set up the mechanism therefore,

too, with the kidnap insurance, I don't know. What is your impression? Are there special negotiators in this ransomware world that try to diminish the amounts that are being paid with any effect?

Mr. VORNDRAN. There are special negotiators in this space for private sector companies that take on the negotiations with the cyber-adversaries that are overseas. From our conversations with people making decisions in companies about whether to pay or not to pay, we would ensure you that the insurance availability or lack thereof becomes a relevant component of their decision-making.

Chair DURBIN. Thank you. Senator Grassley.

Senator GRASSLEY. Yes. Mr. Goldstein, I'm going to start with you. I understand that CISA helps businesses large and small in preventing ransomware attacks. This is partially through a recently launched one-stop website called *stopransomware.gov*. Can you describe the services you offer directly to small businesses beyond advice on best practices, and are businesses able to reach out to CISA for help and support if they have questions?

Mr. GOLDSTEIN. Senator, thank you so much for that question. One of the core elements of CISA's mission is providing proactive assistance to organizations, particularly and including small and medium businesses across the country before an intrusion occurs. Because we know once an intrusion happens, there's already likely going to be some damage done. Our goal is to get there and deliver guidance, best practices, and services before the ransomware intrusion happens.

We offer a variety of services to this end. One option that we offer is self-assessment tools, via our *stopransomware.gov* website, so that an organization that wants to assess their own cybersecurity can download an easy-to-use tool, walk through a process, and understand the work that they have to do.

If an organization also wants CISA's technical help, we offer assistance in identifying cybersecurity vulnerabilities, conducting technical penetration tests or even red team assessments of an organization's infrastructure, looking at the security of design architectures of a given network and on down the line.

Of course, when an incident does occur, we work closely with our colleagues in Federal law enforcement to provide incident response and threat hunting services to determine where the adversary went, what they did, and get them out.

All of these services can be easily accessed via the *stopransomware.gov* portal. They are all, of course, free of charge, and we encourage any organization in the country, public or private, to take advantage of our services, many of which can be delivered through our field personnel assigned throughout the country.

Senator GRASSLEY. I'm going to go to Mr. Downing. Cyber threats from China are sadly nothing new. From stealing our intellectual property to hacking records of Government employees, the Chinese are clearly comfortable using cyberattacks. On July 19th, the present administration announced that Chinese government-affiliated hackers were responsible for hacking the Microsoft Exchange email server and launching a number of cyber ransomware attacks against U.S.-based companies.

Do you—I'm concerned that the Department of Justice's China Initiative, a successful initiative to focus resources on combating

Chinese espionage from the Trump administration may not be continued in the Biden administration. Would maintaining the China Initiative be helpful in combating cyber offensives from China?

Mr. DOWNING. Thank you very much for the question, Senator. I would like to reassure you that, indeed, the Department continues to be keenly focused on the problem of the theft of intellectual property by Chinese actors and by the Chinese government. We have a close partnership between our National Security Division and the Criminal Division, where I work, which continues to look at these questions and to aggressively investigate and prosecute individuals who are responsible for them, both inside the United States and outside.

We use this—we see this as part of a larger effort that, of course, the Biden administration is very concerned about Chinese overreach, and is aggressively looking at these questions, as well.

Senator GRASSLEY. Also, do you—ransomware—ransomware as a service is basically a form of high-tech organized crime. It's a business model where cybercriminals design a product, ransomware, which can be leased to other criminal actors. Some ransomware as a service provider even provide tech help like black market IT solution providers. Do you—are traditional cyber and organized crime tools available to fight ransomware as a service, or are new tools needed?

Mr. DOWNING. Thank you for that question, as well. The—it is true that many of these cyberorganizations have organized structures not unlike traditional organized crime. We have aggressively prosecuted them, as well, using the tools that we have today.

I don't have a particular proposal that addresses that point that has been cleared for—by the interagency, but we would continue to look at that and work with the Committee absolutely on that question.

Senator GRASSLEY. Does it mean that you have interagency conversations that you're thinking about something along that line if it gets clearance?

Mr. DOWNING. We are always looking at all different kinds of tools and shortcomings to the extent that they exist in our authorities. We have put forward a couple of those kinds of shortcomings for the Committee's consideration as part of my statement for the record, and we very much look forward to working with you on that.

Chair DURBIN. Thank you, Senator Grassley. Senator Feinstein.

Senator FEINSTEIN. I'm not a lawyer, but I'm really perplexed by this because what it says to me is that there is a criminal organization operating this process, and we can't do anything about it. If I understand it, in 2020, the FBI received 2,500 complaints relating to ransomware, with adjusted losses of over \$29.1 million. This figure probably underestimates the severity of the problem because victims of these attacks are not recorded—are not required to report their data breaches to the FBI.

For example, one private security firm reported last year there were nearly 2,400 attacks against United States State and local governments. They're attacking the government, as well. Healthcare facilities and schools alone, with 1,300 companies

around the world losing intellectual property or sensitive information to attack.

Why can they just exist, and we can't do anything about it? What can we do? It seems to me it's a criminal operation.

Mr. VORNDRAN. Thank you for the question, Senator. You described the problem correctly, and we would articulate to you that many of the people who attack U.S.-based equities, whether that's small government, municipality government, small businesses, all of your constituents, most of them are overseas. Some of them are in hard-to-reach countries while others are not in hard-to-reach countries.

I think from the FBI's perspective, this brings the value proposition in focus about our international reach. Secret Service has a similar international reach. Through the Department of Justice, we have had success in cooperative third-party countries that aren't Russia, right, in terms of safe harboring criminals. Those people have been brought to justice. They may be on criminal charges in a different country, and they may—

Senator FEINSTEIN. Excuse me. Could you just speak to what the FBI advises us to do?

Mr. VORNDRAN. Very simply put, the FBI's advisement is build a relationship with your field office leader as soon as possible for cyber incidents. Then, second, if you unfortunately become a victim, report those incidents to the FBI or any of our counterparts here, and we will immediately share with the rest of our counterparts.

The last thing I would offer is that's very, very important for each of the companies or municipal governments to have well-rehearsed incident response plans. That they understand who to call when they become a victim, they understand the scope of those incident response plans, and to routinely exercise those would be some important messages to share with your constituents.

Senator FEINSTEIN. Thank you.

Chair DURBIN. Senator Graham.

Senator GRAHAM. Thank you all. As a matter of fact, I think one of the proposals you have is taking a couple of bills that we've introduced, Senator Whitehouse and myself, and we'd like to work with you on that. The bottom line, from the Secret Service point of view, if cryptocurrency didn't exist, would it be harder to do ransomware attacks and get paid for it?

Mr. SHERIDAN. That's an interesting question, sir. It would be harder to facilitate the payment of the attacks. The crypto—excuse me, the ransomware attacks themselves would still occur, it would just be through a different payment mechanism.

Senator GRAHAM. If you took cryptocurrency off the table, how would they get paid?

Mr. SHERIDAN. They would utilize other payment structures. Regular fiat currency, the traditional financing of crime that has occurred for all existence prior to cryptocurrency.

Senator GRAHAM. If they ask for cash, would that be tougher on them?

Mr. SHERIDAN. It would be more difficult for them to facilitate, yes, sir.

Senator GRAHAM. Okay. How many ransomware attacks are there every year against Russian businesses?

Mr. SHERIDAN. I don't have that information, sir.

Senator GRAHAM. What about Chinese businesses?

Mr. SHERIDAN. Similarly, I'd have to research that.

Senator GRAHAM. What about Iran?

Mr. SHERIDAN. Same answer, sir.

Senator GRAHAM. What about North Korea? Same?

Mr. SHERIDAN. Yes, sir.

Senator GRAHAM. I bet you not many. The point is that we have criminal enterprises interconnected to nation-states. Do you agree with that from a Secret Service point of view?

Mr. SHERIDAN. Yes, sir, that's accurate.

Senator GRAHAM. If we've compiled a terrorist list of state-sponsored terrorism, do we have such a list for state sponsors or safe havens for cyberterrorists?

Mr. SHERIDAN. We have a list of suspects and identified individuals that—

Senator GRAHAM. Do you have—do you think it would be helpful for the United States to create a list of countries that we believe are aiding and abetting ransomware attacks throughout the free world?

Mr. SHERIDAN. From a law enforcement perspective, we focus more on the individual than the country, sir. I would defer to a larger geopolitical discussion about that.

Senator GRAHAM. Would it help the FBI?

Mr. VORNDRAN. Sir, we have a very good handle on what countries are behaving in what way—

Senator GRAHAM. We have a list of terrorist organizations, right? Every year, the State Department—

Mr. VORNDRAN. Correct, sir.

Senator GRAHAM [continuing]. And coordination comes out with a list of terrorist groups. I think we have a list of state-sponsored terrorism every year, is that correct?

Mr. VORNDRAN. Yes, sir.

Senator GRAHAM. Is that right, Mr. Downing?

Mr. DOWNING. Yes, sir.

Senator GRAHAM. How about let's look at putting a list of state-sponsored or aiding and abetting countries when it comes to ransomware and cyberattacks. Does that make sense?

Mr. DOWNING. Perhaps I could jump in on that one. It's something that I don't know that I've thoroughly considered, so I'm not ready to give you a quick answer, but I do think that finding ways to press the countries that are harboring these criminals is important.

Senator GRAHAM. Let's make a list of those countries. Who are they?

Mr. DOWNING. Certainly, Russia is at the top of the list. They have been consistently—

Senator GRAHAM. Let's stop right there. Russia is at the top of list of aiding and abetting ransomware attacks and other cybercrimes, do you agree with that?

Mr. DOWNING. Sir, aiding and abetting has a particular legal definition. I wouldn't say that the government of Russia is behind these attacks. However, we do believe that they are not doing what they could be to suppressing them within their borders.

Senator GRAHAM. Why aren't they doing what they could be doing?

Mr. DOWNING. There probably are various different reasons for that that I could speculate on, including that, as you pointed out, sir—

Senator GRAHAM. Have we had—have we ever seen a connection between the cybercriminals and Russian intelligence agencies?

Mr. DOWNING. At times, yes, sir, we have found—

Senator GRAHAM. As a matter of fact, we found more than one time where the Russian Intelligence Agency Members were actually involved in cybercrimes, right?

Mr. DOWNING. That also is true, sir. We—

Senator GRAHAM. I don't know what they're moonlighting policy is, but it seems to me—I don't know what the CIA does in their off time, but—I think the point we're trying to make is that deterrence has been lost when it comes to cybercrime, particularly ransomware. Do you all agree?

Mr. DOWNING. Sir, I would say we have a significant deterrence. Could we do more? Yes, we would need to do more.

Senator GRAHAM. Is it working?

Mr. DOWNING. It is having some effect, but it is not solving the problem—

Senator GRAHAM. Are the crimes going up or down?

Mr. DOWNING. Up, sir.

Senator GRAHAM. Dramatically up or slightly up?

Mr. DOWNING. Certainly, significantly up. Yes, sir.

Senator GRAHAM. Seems to me that deterrence is not working. From a Secret Service point of view, do you believe the network of laws we have today create enough deterrence in this space?

Mr. SHERIDAN. I believe the network of laws does, sir. I think there needs to be greater enforcement of those laws. Greater resources—

Senator GRAHAM. It's an enforcement problem, not legal authority problem?

Mr. SHERIDAN. From my perspective, sir, it's resourcing and enforcement of those laws and better equipping those law enforcement agencies that are tasked with—

Senator GRAHAM. You really don't need much help from us.

Mr. SHERIDAN. We need significant help, sir, in authorities and in—

Senator GRAHAM. You just said two different things.

Mr. SHERIDAN [continuing]. In authorities related to—

Senator GRAHAM. Thank you, thank you.

Chair DURBIN. Senator Whitehouse.

Senator WHITEHOUSE. Thank you, Chairman. First, I'm delighted to be following Senator Graham in the order of questioning, because we have a bill with Senator Blumenthal and Senator Tillis. It looks to me a lot like the Appendix A, Mr. Downing, that you have attached as your proposed legislation. Has a section two that is essentially the same as our section four and has a section three that is essentially the same as our section six. I'm wondering if you might sit down with us and come the rest of the way. We're glad you've made these two steps, we'd like to understand why you didn't recommend the entire bill. If there are technical changes

that you think we should make, then we're eager to work that out. We think that this is a bill that has bipartisan support that could potentially move by unanimous consent, and we'd like to get this straightened out.

Again, our appreciation for copying our two sections. Let's try to get together on all of them if we can. Can you do that?

Mr. DOWNING. Thank you, Senator. We really appreciate your and Senator Graham's leadership on this. We—

Senator WHITEHOUSE. Senator Blumenthal and Tillis.

Mr. DOWNING. And Tillis.

Senator WHITEHOUSE. We have Tillis right here.

Mr. DOWNING. Sir. Of course, we would be more than happy to work with your staff on these questions. Absolutely, sir.

Senator WHITEHOUSE. Great. This is kind of a moment of frustration for me, as well, because we have known about critical infrastructure as a prime target since I wrote the original Intelligence Committee cyber report probably a decade ago.

We've known for years and years and years and years that ransomware was a method for attacking. We have spent billions of dollars, particularly at Homeland Security on trying to solve the problem of protecting critical infrastructure, and boom, what happens? A bunch of people in a basement someplace are able to take down Colonial Pipeline, a significant piece of Colonial infrastructure, with a ransomware attack.

That's not a success story. That's a failure story. That's something is wrong in the way we're doing business right now. It strikes me that the thing that is wrong in the way we're doing business right now is that you can be critical infrastructure in this country, providing essential services to our economy and to our national security, and not have to meet any real standards.

I think we've shown in the defense industrial base that, with the right kind of pressures, companies can step up and do a better than average job. I think we've shown in the financial sector that, with regulators looking over the shoulders of the big banks, they have stepped up and done a better job than average. Here we sit with Colonial Pipeline, with your voluntary, Mr. Goldstein, your voluntary standards. The NIST Framework and the C3 and your offers. It obviously failed. I mean a total face-plant failure.

What I would like to ask is that you and Homeland Security provide to this Committee a summary of what Colonial Pipeline accepted by way of all those voluntary offers that you talked about. How vigorous were they about participating in your voluntary programs? How was the response? I think if there is ever a moment where we have a case study of a failure of critical infrastructure from cyberattack, this is it.

I think we're entitled to a bit of a test case here on this voluntary method that we followed and how it's working. Because it sure didn't work for Colonial Pipeline, and I'd like to know what they did and did not take up of your series of offers. Can you get that information to us?

Mr. GOLDSTEIN. Thank you, sir. We'd be glad to provide you with that, and I will note we fully agree that the environment for critical infrastructure that's essential in national critical functions is able to operate insecurely with no insecurity weaknesses, as we

know is often the case throughout this country, is untenable. We as a nation need to act.

I will note that if you wait—

Senator WHITEHOUSE. I'm angry right now, you know, at you because of this situation. I actually understand that it's not your fault. The fault is here in Congress, where over and over again, groups like the U.S. Chamber of Commerce have come in and said, "Don't regulate us. We're against all this cyber regulation. We don't want any of this. Make it all go away. We're against this bill. We're against that bill. We're going to tell the leader to, you know, block this legislation if it tries to go forward."

We now have a situation in which you can have critical infrastructure companies fail at meeting basic standards of cyber hygiene, and we're okay with that. As a legal matter, we're okay with that. We shouldn't be okay with that. We don't have to regulate everybody in the world, but if you're critical infrastructure, we should no longer tolerate this voluntary regime with big companies who know that their infrastructure is critical, and who fail.

Mr. GOLDSTEIN. Yes, sir. Could I ask the Chairman for a response?

Chair DURBIN. Sure.

Mr. GOLDSTEIN. Thank you, sir. Senator, as you are aware, in the wake of the Colonial Pipeline intrusion, CISA worked closely with our colleagues at TSA and the security regulator for the pipeline sector to push out two security directives, the first of which required reporting of security incidents to CISA, the second of which required entities covered by the directive to undertake mandatory security controls.

We view this as a good model to drive the right level of security investment among the most critical entities in this country. We look forward to working with Congress and our partners across the interagency to ensure that we are rapidly raising the bar for cybersecurity across entities that provide national critical functions, wherever they may be.

Senator WHITEHOUSE. I thank you for that answer, and I would focus particularly on the words, "in the wake of."

Chair DURBIN. Thank you, Senator Whitehouse. Senator Sasse.

Senator SASSE. Thank you, Chairman. Thank you all for being here. How large is the universe of known ransomware gangs?

Mr. VORNDRAN. Senator, thank you for the question. The FBI is tracking more than 100 different variants. When I say variants, that would be a brand name, such as Sodinokibi, which also is known as Revil. That would be one. Please understand that there are similar actors that cross-cut multiple different variants. But to answer your question, there's more than 100 different variants is how many we track.

Senator SASSE. Can you—thank you for that. Can you size them a little bit for us, and I understand that some of them are duplicate brands, but kind of issue spot how big the biggest are, how big are the mediums, what's the barrier to entry below which people are not likely able to have competent technologists to be able to execute an attack?

Chair DURBIN. Senator, before he responds, would each of the witnesses pull the microphone a little closer?

Mr. VORNDRAN. Senator, the answer to your question is we have an entire interagency algorithm that essentially prioritizes from one to 101 the level of impact that each variant has had on the United States, its economy, and its other various equities. The largest one that we know of—we would estimate that their revenue from attacks exceeds \$200 million, to give you some type of scope on the value proposition.

Your last question about barriers to entry is a little bit of a difficult one to answer. What I would say is that we see affiliates using the ransomware variants that are going to be most effective at compromising potentially vulnerable infrastructure—information technology infrastructure. Certainly happy to follow-up on the barriers to entry conversation, but that would be the best answer I can give you today.

Senator SASSE. Who owns that data set? I see Senator Cornyn has just arrived. He and I are both active on this issue from the Intel Committee side, as well. If we wanted a briefing, who is the one person in the U.S. Government who is responsible for owning that data?

Mr. VORNDRAN. The roll-up of the data is owned by the FBI through the interagency, but the model was built by the interagency, and every interagency component has input into the model to finalize the prioritization of it.

Senator SASSE. Returning to Senator Graham's line of questioning, how many of those 100 are Russian-allied?

Mr. VORNDRAN. I don't know that answer. Certainly can respond at a later time with a more precise answer, but what I can say is that while the developers may be Russia-based, the affiliates that deploy the ransomware may or may not be Russia-based. It's a little bit of a complicated question, but if it's okay with you, sir, we can—we can get back to you with the precise number to answer your question properly.

Senator SASSE. We'd love it, and in addition to whatever print response you want to give us, I think there are a few of us that overlap between this Committee and CISE, who would love to have an actual briefing on it.

Senator Graham has left, but I'd like to pursue the question he asked you about deterrents, because the actual rate of growth is about 300 percent annually right now. Why do we think any of our deterrents is working? It's not a hostile question at any of you personally, but you all swung this as if there is some success here. It's pretty hard to see that from where we sit.

Mr. VORNDRAN. I can lead the conversation that—my answer from the FBI's perspective would be that we are doing as much as we can with what we have to deter. I can appreciate why from your perspective, Senator, that it's not having as significant an impact as you would want, but there are dedicated men and women in the FBI, all the partnerships here, that are devoting hundreds of hours a week to this problem set and helping.

If the question is are we having a large enough impact? I understand that question. Please understand, the answer to our question about why we're having an impact is because we have great men and women who are doing this work every day, doing prosecutions, infrastructure disruptions, you know, cryptocurrency seizures, and

not just within the FBI, but certainly in the agencies that sit here today and the international community—international community and the Intelligence Community, as well, sir.

Senator SASSE. So—go ahead.

Mr. DOWNING. If I may. Just to add to that, I think focusing on law enforcement deterrents is an important piece of this puzzle, and I agree with you that, though, it alone is not going to be enough. That's why I think we all need to focus on a whole-of-Government response. That is, that we have our colleagues in the Treasury Department looking at how to enhance our position on the cryptocurrency front. We have our friends in CISA building cyber hygiene to slow down the threat. We have our friends in the State Department who are building international consensus against it and putting pressure on Russia.

Yes, investigation and prosecution is an important piece of this, but it cannot be the only piece, I think, if we are going to succeed against this threat.

Senator SASSE. Strongly agree that Putin's cronies who moonlight outside not just the official intel services, but across the oligarchs like little rent an intel service on the side, clearly, they don't fear us, and that deterrent problem is well above your pay grade. Nobody's faulting you here for that. Sir, I recognize you're obviously right that there are a lot of hardworking patriots inside the organization, but that's a different question than whether or not we have the right national strategy. Thank you.

Chair DURBIN. Thank you, Senator Sasse. Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much, Mister Chair. Thank you all for the work you're doing. When I think back to my early confrontations with this issue as a prosecutor, I always remember a case we had. It was a child porn case, but it involved computers, and it was a little suburb. The police went to the scene, and they had not been trained. They pushed some buttons on the computer, and all our evidence disappeared.

Now, let me bring this to our current situation that we're in. It is so much worse and so much bigger. It is workforce as well as all these other challenges that my colleagues have laid out. Maybe the numbers I have: An estimated 3.5 million cybersecurity jobs will be available but unfilled by—in 2021. Approximately one in three cybersecurity jobs in the Federal level going unfilled. Talk to me about how we're going to get people from the private sector, perhaps—Senator Thune and I had a bill on this—to come here so we are as sophisticated as the bad guys trying to ransom and do all kinds of bad stuff to disrupt our critical infrastructure. How are going to get the people in and what should we do to help?

Mr. SHERIDAN. Senator, thank you for that question. I'll turn it over to Mr. Goldstein to partner on this answer. I do want to address your opening statement, though, related to State and local capabilities. As has been stated multiple times, this is whole-of-Government approach. The Secret Service has the National Computer Forensics Institute that has trained and equipped more than 16,000 State, local, Territorial, Tribal officers as well as judges and prosecutors. We train more than 3,000 a year and these really are the first line of defense. I think this goes to Senator Feinstein's questions about what people can do to be more resilient.

My colleague, Mr. Vorndran has mentioned relationships. This is where the relationship forms with those that you know in your community, your constituents, to have that level of trust, that level of communication, to be the first responder in these types of incidents.

That institution, as you may be aware, is due to sunset in 2022. We'd greatly appreciate Congress' support for allowing us to train as many as we have, but we need to seek reauthorization as well as growth, not only domestically, but internationally for that facility to, as you said, make sure we're better prepared on the State and local level.

Senator KLOBUCHAR. Okay. Then if we could get the question of the unfilled jobs and how we're going to get people into this area. Young people and the like with a call to service, I hope. Mr. Goldstein.

Mr. GOLDSTEIN. Absolutely. Senator, thank you for calling out this critical question. There is no bigger challenge facing the future of our Nation's cybersecurity than building a deep and diverse workforce to meet the threats we are facing now and facing tomorrow.

At CISA, we're looking at this as really having three components. The first is how do we build cybersecurity and STEM education into our K12 students today? At CISA, we have a grant program where we provide cybersecurity curriculum and training to K12 teachers across the country. Obviously, that is a large population. We need to scale and do more. The first question is how do we ensure that across elementary, middle, and high schools across this country our students are learning first and foremost the importance of cybersecurity, and then the basic skills to pursue this as an avocation from a very young age. That will require some very fundamental changes how we think about educating our children in this country.

The second is how do we resource those leaving secondary education going to 2-year institutions, HBCUs, trade schools, all the way to 4-year universities, ensuring that those universities have the programs where they're turning out graduates that are able to take jobs at the leading cybersecurity entities in our country, whether Secret Service, CISA, or the FBI, or the private sector. Because, frankly, we are all in the same fight here. Here at CISA again provides curriculum and training to a select group of entities, largely serving underserved communities. We need to do more there.

The third piece is how do we make it easier to enter public service as a cybersecurity practitioner. The cybersecurity market today is extraordinarily competitive, and we need an urgent call to action to make sure that the best and brightest are joining our agencies to help defend our country against these threats.

Senator KLOBUCHAR. Got it. I think some of our model is people stay forever in the Government, and we may have a situation where we have a call to action to come to our Government for a while. Maybe they go somewhere else after that, but we're just going to fall behind if we can't get people to do it. Did you want to add anything, Mr. Vorndran?

Mr. VORNDRAN. Senator, very briefly, just rough numbers. A computer scientist graduating college with a 4-year bachelor's degree can earn about \$100,000. The entry position, certainly within the Department of Justice, is about \$63,000. We can't incentivize that year over year right now, so just to highlight the focus of your concern and the recruiting retention problem. It is a significant barrier.

Senator KLOBUCHAR. Senator Thune and I had a bill a few years ago that would allow people to go into certain areas. You have all kinds of issues, especially with the FBI with then classified, private sector people coming in. I think we should revisit that for certain positions, it is—but we've got to figure this out, so we get the people.

I have some other questions—I'm out of time—about small businesses with the 51 percent not being able to have any resources to cybersecurity themselves, and how we're going to build that up. I can ask that on the record, or maybe my colleagues will. Thank you.

Chair DURBIN. Thanks, Senator Klobuchar. Senator Tillis.

Senator TILLIS. Thank you, Mr. Chairman. Gentlemen, thank you for being here. Mr. Sheridan, wanted to give you an opportunity to respond to Senator Graham's question. You were talking about authorities and other resources that you need, so, if you would hit that quickly.

Mr. SHERIDAN. Thank you very much, Senator. Regards to authorities, as I mentioned, our National Computer Forensics Institute reauthorization is extremely important, not just for us, but for the whole-of-Government approach. As well, our authorities within the Secret Service related to investigations, specifically for statutory authority on money laundering, structured payments, and unlicensed money transmitters would be very beneficial for us to strengthen our investigative mission. Thank you, sir.

Senator TILLIS. Thank you. Mr. Goldstein, in my office, I was a part of a practice that did ethical hack testing at Pricewaterhouse back in the late 1990's and early 2000's and followed this pretty closely. In my office, I have a Hacking for Dummies, which is a great book, and every business should read it and understand how vulnerable they are. I believe that businesses—a part of what we're doing here is to provide you all with better tools to seek out bad actors and hold them accountable, but businesses have benefited mightily from the internet and electronic systems. They need to harden their systems the way that they harden their physical presences, with alarm systems, burglar bars, whatever it takes to secure a physical premise.

I think one thing we have to do is make it very clear to business that we alone, the Federal Government, or the whole-of-Government, are not responsible for securing their business enterprise. We're there when somebody breaks in to bring them to justice.

Is it still the case that the vast majority of these hacks are attributed to human error? That there's a click on a link? Is that still the case in your research that we've got to better educate people, that they're the weak link in most of these successful hack events?

Mr. GOLDSTEIN. Thank you, Senator, for that question. It is certainly still the case that particularly with ransomware intrusions,

most of the events that we are seeing are attributable to known security weaknesses. It might be the case that an employee clicks on a phishing link. It might also be the case, as has been reported publicly with Colonial Pipeline, that the adversary exploited a legacy remote access device that was using a known password. Certainly, this is why we are so focused on driving adoption of these basic practices because we know that these can demonstrably reduce the likelihood that a business will be exploited by a ransomware intruder.

Senator TILLIS. Why shouldn't we—I fall short of mandating what the private sector does and to provide them best practices, but why shouldn't we as a matter of Federal policy require everyone who does business with the Federal Government to adopt and implement these practices as a price of admission for doing business with the Federal Government?

Mr. GOLDSTEIN. That's a great question, sir. President Biden's cybersecurity executive order, issued earlier this year, required CISA to work with our partners in Government to do exactly that, to prescribe new contract clauses that will be adopted into Federal acquisition law and will provide a floor for the kinds of security controls that we expect to see from Federal vendors.

Senator TILLIS. The administration already has that authority? Congress doesn't need to do anything more to push the point?

Mr. GOLDSTEIN. My understanding, sir, is that today we can do what we need to do in that space. That's correct.

Senator TILLIS. Mr. Vorndran, what about the concept of—I think maybe Senator Whitehouse and Daines have introduced the concept of a hackback to basically allow private sector to go after those who are holding them or requesting ransom. What's the—what's the Department's opinion about really encouraging businesses to go back after these people? Hackback.

Mr. VORNDRAN. You want me to? Senator, do you mind if I defer that question to Department?

Senator TILLIS. Yes.

Mr. VORNDRAN. Thank you.

Mr. DOWNING. Sir, on the Hackback question, the Department has long held the position that it is ill-advised to encourage or permit private sector people to hackback. Couple of reasons: First, there's a real risk to innocent users. Very often, the infrastructure that's involved is not the offenders that they're going after, but instead innocent third parties. Second, there is a real problem with the interference with ongoing criminal or intelligence investigations when you have private sector people monkeying around in these groups and these organizations. Third, very often at the early stages of an investigation, we don't know who's behind it, and so, if you happen to be hacking back from, let's say, a film company that is invaded, and it turns out later that it's North Korea, as has happened, that's a particularly sensitive situation where you want to make sure that the government actors are the ones in charge of how we are going to take those steps and not have it be done by private sector people who are not in a position to understand the full picture or the geopolitical situation.

Our long-standing position has been that that is not a helpful road to go down. Instead, report to us, report to the FBI. We can

take steps. We have authorities to have an effect and an impact, and that's the better approach.

Senator TILLIS. Thank you all. Thank you, Mister—

Chair DURBIN. Thank you, Senator Tillis. Senator Hirono.

Senator HIRONO. Thank you, Mister Chairman. I think the panel of all—you all agreed that there is a causal relationship between the growth in cryptocurrencies helping to drive the increase in ransomware attacks. I think that you generally agreed yes. We're not quite sure what to do about it, but aside from things like considering the U.S. banning cryptocurrencies, what about should we make ransomware payments illegal? Anybody want to answer that?

Mr. VORNDRAN. Senator, thank you for the question. It's our opinion that banning ransomware payments is not the road to go down, and there's really a prime reason for that. Right now, what was shared in the opening remarks is that ransomware has a single extortion model. Essentially, we would hold your data ransom until you pay for that data. In the very recent past, actors have moved to a double extortion model. First, they exfil data and threaten to leak it on a tour site for sensitive information. The second prong of the extortion is the ransom for the encrypted data.

It would be our opinion that if we ban ransom payments, now you're putting U.S. companies in a position to face yet another extortion, which is being blackmailed for paying the ransom and not sharing that with authorities. It's a really complicated conversation, but it's our position that banning ransom payments is not the road to go down.

Mr. SHERIDAN. If I could add, ma'am, as well—

Senator HIRONO. Yes.

Mr. SHERIDAN. Reporting is one of our biggest challenges related to this.

Senator HIRONO. I'm sorry, what is?

Mr. SHERIDAN. Reporting.

Senator HIRONO. Yes.

Mr. SHERIDAN. As was stated by several of my colleagues. Banning the payments would further push any reporting to law enforcement into obscurity and make it virtually impossible for us to have that relationship.

Senator HIRONO. This is quite the conundrum for all of us, and I note that we're going to need a workforce that is very attuned to the need for—to have an understanding of cybersecurity issues and sim backgrounds. You noted, I think it's Mr. Downing, that we need a whole-of-Government response. That means that we should be across departments. Does that include the Department of Education? Because I note that Mr. Goldstein said that we need to really have curriculum in our elementary schools that focuses on STEM and that provides an understanding of cybersecurity. Is the Department of Education involved in this whole-of-Government approach that you all talked about?

Mr. GOLDSTEIN. Thank you, ma'am, yes, absolutely. CISA works very closely with our colleagues at Education, as well as at the National Science Foundation and other agencies to make sure that all partners in Government with a role in promoting a curriculum that meets the challenges of today and tomorrow are onboard. This is really a whole-of-Government effort. Our goal is to make sure that

those individuals in school today are prepared to take on the jobs that we'll need them to face this challenge going forward.

Senator HIRONO. Is this kind of curriculum already in our elementary public schools?

Mr. GOLDSTEIN. That's correct in some cases. Certainly, it is not ubiquitous across the country yet, but this is part of, of course, a broad focus on STEM education. Part of ensuring that—that children in school in this country are focusing on STEM education is the cybersecurity aspect of that challenge. Making sure that we are encouraging both STEM as a basic focus and then cybersecurity as an aspect thereof will be critical going forward.

Senator HIRONO. I actually would like to see an actual curriculum in our elementary schools that focuses on STEM. What about engaging with our allies because it's not just the U.S. Government, whole-of-Government, but we really need to engage with our allies in how to prevent these kinds of crimes from occurring, so how are we doing on that score?

Mr. GOLDSTEIN. Sure. I'll offer a first thought and then I'll hand off to my colleagues. From our perspective at CISA, we work very closely with international computer emergency response teams, or CERTs, who are the network defenders globally to protect their countries' private and public networks, and we share information with them continuously on new ransomware threats that we can then share to help protect businesses and government networks in our country.

Senator HIRONO. Is the—

Mr. DOWNING. If the—

Senator HIRONO. Go ahead.

Mr. DOWNING. If I may, there are a number—you're exactly right that international collaboration is critical to what we do, and there are a number of factors that are in play here. We strongly support, for example, the Convention on Cybercrime, to encourage appropriate laws around the world, and that's been building over the years.

Partnerships with foreign law enforcement agencies are critical. The Secret Service and the FBI have personnel stationed in foreign countries, and we work extremely well with international agencies like Europol, with some very effective results.

Third, for the Department of Justice, we have a program called the ICHIPs, the International Computer Hacking and Intellectual Property coordinators stationed in various countries. We find that having prosecutors in foreign countries also helps to build those relationships which have proven to be so effective when we've done takedowns like that NetWalker and Emotet ones that I mentioned earlier.

It's that international collaboration that is key to many of the successes that we've had.

Senator HIRONO. Thank you. Thank you, Mr. Chairman.

Chair DURBIN. Senator Cornyn.

Senator CORNYN. Thank you, Mr. Chairman for holding this very important hearing. I think we're suffering from many of the same silos we—we identified on 9/11. We find that there's a number of different parts of the Federal Government that are dealing with the same problem in different ways, and we're depending on the ex-

ecutive branch depending on—from administration to administration to come up with a coherent strategy which uses the all of government approach that Mr. Downing and others have advocated.

Let me start with a basic—very basic question. When somebody gets hacked, should they be required to notify the Federal Government? Mr. Goldstein, perhaps CISA? Or the FBI?

Mr. GOLDSTEIN. Certainly. Our view is that any efforts to increase the volume of incident reporting to CISA and, to be sure, with our partners in Federal law enforcement, is absolutely essential. Absent this reporting, we are unable to offer assistance, we are unable to address many of the questions that you and your colleagues have raised today to understand the breadth and scope of the problem, and we're unable to develop information that we can share effectively to prevent other intrusions. Certainly, steps taken to increase reporting across the country will be highly beneficial. We look forward to working with Congress toward that important goal.

Senator CORNYN. Mr. Vorndran.

Mr. VORNDRAN. Senator, thank you for the question. If I can just amplify Mr. Goldstein's remarks. As is memorialized in Mr. Downing's statement for the record and my statement for the record, we are very significant advocates for mandatory breach reporting. There's really three reasons for that.

Right. We need sufficient information about tactical information, ransom requested, where to pay the ransom, how to contact the actors. The information must be shared promptly so that we can respond accordingly, and then there needs to be a requirement to immediately share across the interagency. Admittedly, sir, that already happens today, but anything we can collectively do to increase reporting is going to be very helpful in this problem area.

Our estimates are that between 25 and 30 percent of incidents get reported to Federal law enforcement at this time.

Senator CORNYN. I know there are at least two bills that are currently out there. One from the Homeland Security and Governmental Affairs Committee, a bipartisan bill. Senator Portman, Senator Peters. Then there's also an Intel Committee bill that Senator Warner and a number of us are working on to require that because it seems like in the past we've relied on the business community, for example, to make a report and perhaps they feel like because reputational considerations or some others, they may just want to not report it, and because once it gets into the public domain, then maybe people don't feel comfortable doing business with them. Or maybe they go to a competitor or the like.

It strikes me as absolutely critical, and I'm glad to hear your answer that we get the universe—universal picture, and then to give you and other authorities the opportunity to deal with it.

There ought to be some sort of confidential means to do that, and one that perhaps provides some liability protection, much as we've done in the past with some of the programs through the National Security Agency when it comes to collecting information from phone companies and the like.

How big a problem is attribution? Mr. Vorndran.

Mr. VORNDRAN. Senator, that's an excellent question. The response to your question is that it's very challenging, especially in

the criminal cyber element, moved away sometimes from the Nation's State cyber element. In the criminal cyber element, it is extremely challenging to gain attribution down to a keyboard or an actor behind a keyboard. I would estimate that about half of our cases don't have accurate attribution because of the complexity involved.

Senator CORNYN. That's part of the tradecraft of the cyber offender, correct? Hiding their identity?

Mr. VORNDRAN. Yes, sir. I mean, it's very easy to masquerade as a Mandarin keyboard in Brazil that would potentially probe a network. The person behind that keyboard is probably not in Brazil, and they may or may not speak Mandarin.

Senator CORNYN. I agree with you and Mr. Downing that the law enforcement—law enforcement model is an important component, but only a component of what our response should be. Indeed, after the 2016 Russian interference and cyberattacks on the DNC server and leaking that, General Nakasone and the folks out at Cyber Command and NSA undertook a way to try to protect our voting systems in 2018, and we had remarkably improved protection of our voting systems.

We know that we have the capability to do it, we just need to figure out how to come up with a strategy. Perhaps something like we did on Congress past 5G and beyond, which basically mandated that the executive branch come up with a comprehensive strategy, working with Congress because frankly, we're so—as I mentioned at the beginning—siloed here.

We've got different Committees of different jurisdiction and different levels of information about these issues and different perspectives depending on if you're the Judiciary Committee, focusing on law enforcement, as opposed to maybe the Intel Committee looking at the espionage threat. Or the Governmental Affairs Committee looking at some other aspect of it.

Having a plan I think is really important because right now, notwithstanding our outstanding capabilities, I think we're getting our lunch eaten on a regular basis, and we've got to up our game. That's not a comment on what you do or the people that work with you. I think it's up to Congress and the policymakers to come up with a policy that you can then implement to do the job that you're trained to do, and that you're trying to do every day. Thank you.

Chair DURBIN. Thanks, Senator Cornyn. Senator Blumenthal.

Senator BLUMENTHAL. Thanks, Mr. Chairman, and I want to join in thanking you and the Ranking Member for this hearing and thank you all the law enforcement members of this panel. You have definitely upped your game. There's no question about your recent record, and I'm sure it reflects long-standing work on putting together the infrastructure that's necessary to do that law enforcement, and the skills, and the equipment, and so forth.

As has been mentioned, Senators Whitehouse, Graham, Tillis, and I have a measure that we've introduced, the International Cybercrime Prevent Act, which is intended to provide you with more tools. Maybe mandatory reporting ought to be one of them.

A number of our colleagues have asked for liability protections in connection with that reporting, and I would welcome the opportunity to consult with you as to ways there may be to protect the

confidentiality of information that is provided in the course of reporting because I think that's one of the concerns that may discourage more reporting.

We've just—some of us come from a hearing in the Commerce Committee, where I asked the head of TSA about reporting, and he testified that there is reluctance because of the fear of publicity. That is a common thread in law enforcement, as you well know, that prevents reporting of rape, it prevents reporting by seniors about financial crimes, it prevents all kinds of reporting. We need to overcome that obstacle.

I want to ask about the harboring of these cybercriminals in Russia and China. I was very impressed and appreciated President Biden raising this issue in his meeting with Vladimir Putin. The Russian government's hacking and its providing safe haven to criminal elements that, in turn, have attacked us. He was very dramatic in his telling Russia, according to the readout of the recent Biden call with Putin this month, that we will take quote "any action necessary to defend our people and our critical infrastructure."

Have you seen any change in the amount or severity of cybercrime from Russia in this last month?

Mr. DOWNING. Perhaps I could take that one, Senator. I don't believe there has been a measurable drop. No, I don't think that is a change.

Senator BLUMENTHAL. Essentially, there's no evidence that Putin is heeding this warning as yet, correct?

Mr. DOWNING. I think that's fair, yes.

Senator BLUMENTHAL. How about on the part of China? Is it getting the message?

Mr. DOWNING. With respect to China, that's a complex situation. We continue to press on that issue from the Department of Justice's perspective in investigating and prosecuting those crimes aggressively.

Senator BLUMENTHAL. Let me be somewhat simplistic. What I'm hearing is that Russia and China essentially are taking no real action in cracking down on these criminal gangs or the malicious cyberattacks that make us the target, correct?

Mr. GOLDSTEIN. Senator, I would just add that, as my colleague noted, we believe that only about a quarter of ransomware intrusions are actually reported. The question of are we seeing a change in trend is a very hard one to answer. It certainly could be the case that some ransomware actors have changed behavior for a variety of reasons. We simply don't have the data to be able to answer the question with any level of authority.

Senator BLUMENTHAL. Okay, but we have to act on the basis of what we know, not what we don't know. From what we know, and you have the best knowledge in the business, there has been no perceptible change in behavior on the part of either China or Russia in cracking down on these criminal actors.

Mr. GOLDSTEIN. Based upon available data, we have not seen a change in a trendline of intrusions overall.

Senator BLUMENTHAL. The available data that you'd need would be more reporting of these attacks?

Mr. GOLDSTEIN. That's correct, sir.

Senator BLUMENTHAL. Do you have a way of knowing about these attacks without their being reported?

Mr. GOLDSTEIN. We do not, sir, not reliably.

Senator BLUMENTHAL. Is there conceivably a way technologically to know?

Mr. GOLDSTEIN. I defer to my colleagues in law enforcement if they have any methods. To reference from our point of view, hearing from the victims will be the most authoritative way to understand the breadth of these intrusions.

Senator BLUMENTHAL. Only a quarter of them are telling you when they are victims.

Mr. GOLDSTEIN. Again, sir, that's a rough estimate since we don't know the incidents that we are not hearing about.

Senator BLUMENTHAL. You don't know what you don't know, but I guess what I'm taking away from what I've heard from you and what I've heard in the Commerce Committee—the companies of America, our corporate sector really is failing in its responsibility to protect our national security by refusing to report these instances of cyberattack. Am I overstating it?

Mr. GOLDSTEIN. In this case, sir, it truly needs to be a whole-of-Nation effort, with Government and industry working together around this shared challenge, and the more the companies report their intrusions to the Government, the better job we can do in managing this risk.

Senator BLUMENTHAL. I interpret that as a yes. Thank you. Thanks, Mr. Chairman.

Chair DURBIN. Thank you, Senator Blumenthal. Senator Cruz.

Senator CRUZ. Thank you, Mister Chairman. Ransomware attacks have become more and more common, and more and more dangerous. In May of this year, hackers based in Russia shut down Colonial Pipeline, a pipeline that carries gasoline to the southeastern United States. What did the Biden administration do? Next to nothing. The administration sat around as gas lines formed up and down the eastern seaboard and the White House deputy national security advisor tried to absolve the Biden administration, tried to absolve the President from any responsibility whatsoever, saying quote, "Colonial is a private company, and we'll defer information regarding their decision on paying a ransom to them."

Later, after Colonial paid a \$4.4 million ransom, President Biden decided to reward Russia for allowing this hack. He greenlighted the Nord Stream 2 pipeline, a natural-gas pipeline from Russia to Germany that will put billions of dollars in the pockets of Vladimir Putin, and then he sat down with Putin and told him that only certain parts of America's critical infrastructure should be off limits. He specified 16 parts that were off limits. Call me crazy, but I think all of our critical infrastructure should be off limits to Russian hacking. And when the President enumerates 16 that matter, that is an invitation to hack every other part of our infrastructure.

Mr. Downing, does paying ransom encourage more ransomware attacks?

Mr. DOWNING. I think it's fair to say that when criminals profit, they draw more criminals into that space and so, the paying of ransoms is certainly one thing that fuels the increase of ransomware attacks that we've seen.

Senator CRUZ. Does telling Putin that only certain parts of our infrastructure are off limits—does that have the potential to encourage more attacks like the Colonial Pipeline attack?

Mr. DOWNING. I would have to say that the President's communications with Putin are outside of my purview. However, I can assure you that we are continuing to press for results, and we are not waiting around, from a law enforcement perspective, to see what would happen there. We are pursuing the cases and the investigations and the activities that we would in order to do the very best that we can to drive deterrents and to arrest and disrupt these operations.

Senator CRUZ. Mr. Goldstein, is attacking a pipeline a new concept or have we seen this before?

Mr. GOLDSTEIN. Senator, this—the attack of Colonial Pipeline is the first incidence that we have certainly seen in this country of an intrusion causing a disruption to pipeline infrastructure.

Senator CRUZ. Your organization just recently issued a release stating that between 2011 and 2013, Chinese state-sponsored actors targeted 23 U.S. natural-gas pipeline operators. Is that right?

Mr. GOLDSTEIN. That's correct, sir. That refers to targeting rather than an intrusion resulting in an actual disruption.

Senator CRUZ. The idea that malevolent actors would go after infrastructure like pipelines, that is a threat we've been aware of for some time.

Mr. GOLDSTEIN. That's correct, Senator.

Senator CRUZ. China has repeatedly used ransomware and cyberattacks to harm America. Not only has it attacked pipelines in an effort to cause physical damage, but just this year, hackers affiliated with the Chinese—Chinese government attacked tens of thousands of computers across tens of thousands of organizations, including a significant number of small businesses, towns, cities, and local governments.

Once again, unfortunately, the Biden administration responded to extreme threats with extreme weakness. The Biden administration has not imposed any sanctions on China. Instead, the administration announced that is dropping criminal cases against five Chinese scientists who, with the help of consular officials, hid their affiliations with China's military in order to infiltrate our Nation.

Mr. Downing, why is this administration refusing to prosecute Chinese scientists who lied about their ties to the Chinese military in order to come to this country and gain access to information?

Mr. DOWNING. Senator, thank you for the question. I would have to say that, from my position in the Criminal Division, I am not responsible for those decisions. However, it is something that I'd be happy to take back and get you an answer for.

Senator CRUZ. Let me ask anyone on the panel. Do you have an answer as to why the administration has not sanctioned China for repeated cyberattacks over and over and over again against the United States?

I think that's a question that administration should answer. Showing weakness to China and weakness to Russia only invites more aggression and more cyberattacks attacking our Nation. Thank you.

Chair DURBIN. Senator Ossoff.

Senator OSSOFF. Thank you, Mr. Chairman. Thank you to our panelists. One of the benefits of bringing a whole-of-Government approach to a national security issue such as this is that it can bring the full force of the U.S. Government. One of the risks is jurisdictional ambiguity, a lack of a clear chain of command, and organization responsibility. What I'd like to ask first is for each of you—and forgive me, I can't see how you're arrayed beneath the dais. Beginning with you, Mr. Downing, and then proceeding sequentially, to identify what it is that your agency, your component has lead responsibility for in preventing and responding to ransomware attacks that none of the other components or agencies represented here has lead responsibility for. What are you uniquely responsible for ensuring happens and gets done to protect our cybersecurity?

Mr. DOWNING. Thank you very much for the question, Senator. At the Department of Justice, we have two Divisions that are responsible in part for responding to the ransomware attacks. My Division, the Criminal Division, is responsible to—for those attacks that are identified as being from criminal actors. We have taken the lead on a very large number of the recent ransomware attacks.

We bring charges, we make charging decisions, we work on the legal side to make sure that the law enforcement agencies are able to obtain the evidence that they need, and we pursue extraditions through our Office of International Affairs in order to get them back to the United States.

My colleagues in the National Security Division support that work through a lot of different means related to national security authorities. However, when the actors responsible are nation-states, or proxies for nation-states, then they would have the key role in all of the same ways that I mentioned, gathering evidence, bringing charges, and seeing those charges through to court.

Senator OSSOFF. Thank you. Mr. Vorndran, please.

Mr. VORNDRAN. Thank you for the question, Senator. In response to your question, we would reference Presidential policy directive 41 from 2016. That was the first ever national policy on this topic and sought to define a significant cyber incident. In answer to your exact question, who's in charge? Instead of naming a single agency, it recognized shared responsibility across U.S. Government, and it defined threat response as involving investigation, attribution, and threat pursuit, and named the Department of Justice acting through the FBI and the National Cyber Investigative Joint Task Force as the lead agency for this line of effort during a significant incident. I'll certainly let Mr. Goldstein reference CISA's role. ODNI has a role in PPD 41, but I think another key—

Senator OSSOFF. I appreciate there's a broad spectrum of responsibilities here. My question is: what is FBI's role that is distinct from every other agency represented here today. What do you do, and your personnel do that nobody else does?

Mr. VORNDRAN. In PPD 41, investigate, attribute, threat pursuit for a ransomware incident.

Senator OSSOFF. Thank you, Mr. Vorndran. Mr. Goldstein, please.

Mr. GOLDSTEIN. Thank you, Senator. CISA is uniquely focused on the cyber-defense mission. In the context of incident response, we

are focused exclusively on mitigating impacts to the victim and deriving network defense information that we can share with others.

We also focused significantly on what we would call left of boom, focusing on sharing information and providing services to reduce the prevalence and impact of cybersecurity intrusions before they occur for critical infrastructure, small, medium businesses, and SLTT partners across the country.

Senator OSSOFF. Understand. Is it fair to say that prevention and adaptation? Is that what you're suggesting is your unique institutional role at CISA?

Mr. GOLDSTEIN. I would frame it, Senator, as prevention, resilience, and then, in the context of an incident, mitigation.

Senator OSSOFF. Mr. Sheridan.

Mr. SHERIDAN. Thank you, Senator. The Secret Service is focused on protecting the Nation's financial infrastructure and financial payment systems.

Senator OSSOFF. You all have some responsibility for protecting those aspects of critical infrastructure, correct? My question is what does the U.S. Secret Service lead on, or what operations do you conduct, what mission do you execute that is distinct from the other missions represented by your colleagues at other agencies?

Mr. SHERIDAN. Our distinction is that our statutory authority is focused on financial payment systems, the Nation's financial infrastructure, and I think the distinction of trying to make singular entities is diluting the concept about this being a team sport.

There is necessary overlap to provide defense in-depth, to ensure there's not a single point of failure that the adversary can exploit. We do have some overlapping authorities. The Secret Service focuses on financial payment systems and the Nation's financial infrastructure, which does have some shared responsibility, but we are the leading agency related to those investigations.

Senator OSSOFF. Thank you, Mr. Sheridan. No doubt, collaboration is important—is clarity of purpose. In the aftermath of recent significant cybersecurity failures, what I'm trying to establish is where there is sufficient clarity. Mr. Goldstein, would you please comment on how various sectors across the U.S., private and public sectors—so, for example, the defense industrial base, the financial services industry, local governmental entities, the energy sector that's represented, for example, by the recent Colonial Pipeline breach—how would you rank or contrast their respective levels of appropriate investment, preparation, and whether they engage in the kind of prudent, and vigilant, and disciplined, and well-resourced cybersecurity efforts necessary to protect their networks?

Mr. GOLDSTEIN. Thank you, Senator. I'll start by just noting that, apart from the agencies participating here today, there are a variety of other agencies across the Federal Government called sector risk management agencies that have unique expertise in promoting prudent risk management, both cyber and otherwise, across sectors of the U.S. economy that do play a critical role in this team sport, as Mr. Sheridan noted.

Across sectors, there is certainly significant divergence in cybersecurity maturity, both across sectors, but also within sectors. Certainly, we have seen significant investment in cybersecurity measures and best practices in the financial sector, the defense indus-

trial base, and the energy sector. That is not to say, of course, that every entity in those sectors is equally or even appropriately secure.

We certainly need to focus on each sector, and really shift our focus, as well, on national critical functions. Because we know that a function upon which Americans depend—so just keeping the lights on, that relies not only on the energy utilities, but also the cross-sector entities upon which they depend.

By looking at a functional approach, we can begin to ensure that the services that we all rely on remain resilient and secure against cyber intrusions.

Senator OSSOFF. Thank you, Mr. Goldstein. Thank you, Mr. Chairman.

Chair DURBIN. Thank you, Senator Ossoff. Senator, you're now recognized.

Senator BLACKBURN. Thank you, Mr. Chairman. Thank you to each of you. You know, it's been so interesting. We're having a pipeline cybersecurity hearing in Commerce this morning, so this is our focus today.

Director Sheridan, I'd like to come to you. We hear all this information, conflicting things between cryptocurrencies and cyberattacks. Some people say cryptocurrency is used because it's less traceable. Others say, well, it always leaves a digital trail, but that law enforcement is not using blockchain or other technologies that would work through this. We've recently started a financial innovation caucus. I'd love to hear from you on this. With cryptocurrency, does it make it harder for tracing ransomware attacks?

Mr. SHERIDAN. The interesting contradiction is that it actually makes it somewhat easier because, as you said, there is a digital trail. There are privacy coins and anonymizing techniques, such as chain swapping, chain hopping, peel chain methodologies and various technological approaches that can add layers to that digital trail.

In that sense, it makes it more difficult. If I handed you a \$5 bill and asked you where it's been, it would be almost impossible to tell. If I handed you a Bitcoin wallet address, we would be able to tell what's gone in and what's gone out because of the digital evidence.

It is possible to trace. To your point, we do need to expand our resources related to that. We have a very strong workforce, a very technically capable workforce, of computer scientists, watching analysts, crypto tracers, but we need more of them. We need to get better equipped, better trained, and expand our presence domestically and internationally related to those capabilities.

Senator BLACKBURN. Do you have a timeline for moving forward with having—being able to set some standards? Have you all looked at what this would take? What will it take as far as man hours, personnel, training?

Mr. SHERIDAN. We do have a very detailed projection in terms of timeline, resources, and budget for our ransomware approach as it relates to cryptocurrency and other digital monies. I—

Senator BLACKBURN. Is that information you could share with us, with the Committee?

Mr. SHERIDAN. Yes, ma'am, I would be happy to.

Senator BLACKBURN. I think that would be helpful.

Director Vorndran, let me ask you. Has the FBI looked into using new technologies and blockchain to track and remediate some of the ransomware attacks and transactions?

Mr. VORNDRAN. Thank you for the question, Senator. To amplify what Jeremy Sheridan said, we use the blockchain daily—

Senator BLACKBURN. Okay.

Mr. VORNDRAN [continuing]. Across the organization to track—trace Bitcoin, and I think Mr. Sheridan's comments are spot on, that in certain cases, it actually makes the tracing easier. In certain cases, it makes it more challenging. His reference to a \$5 bill and understanding its traceability is a very good analogy.

We have many FBI agents, FBI analysts, data operation specialists, and other types of personnel in the organization that use the blockchain on a daily basis.

Senator BLACKBURN. General Downing, let me come to you with this. Bulletproof hosters. Hearing about these and the data centers, and the companies that allow ransomware to be transacted on their servers. Of course, this is something that is troubling. That they're setting up overseas and largely outside of U.S. law.

Are there more steps that you all can take to better track and shut down these bulletproof hosting operations, at least domestically?

Mr. DOWNING. Thank you for the question. You've put your finger on it. In order for us to have an effective response to the ransomware problem, we need to look at all parts of the ecosystem. Bulletproof hosting is a particularly—is one of those parts. We have at times brought criminal prosecutions against the owners of these kinds of bulletproof hosters, where we can show that they are well aware that they are contributing to criminal activity, but it is, like many parts of this problem, made more difficult by the international side of it.

These actors are very often overseas, and so, we have to take steps to build our international partnerships in order to arrest them. Those are things we are focused on, though, and we will continue to be as part of the overall response to the ransomware threat.

Senator BLACKBURN. Thank you. Thank you, Mr. Chairman.

Chair DURBIN. Thanks, Senator. Senator Cotton.

Senator COTTON. Thank you, Mister Chairman. Mr. Vorndran. Thank you. Both Russia and China have tried to undermine multiple American industries through sabotage, intellectual property theft. American agriculture is no exception. In just the last few years, we've seen several hyperbolic examples of this.

In 2016, Chinese researchers were sentenced to Federal prison for attempting to steal patented corn seeds and trade secrets from American farms. In 2018, Chinese researchers were sentenced to Federal prison for trying to steal trade secrets from the USDA Dale Bumpers National Rice Research Center, and from American Biotech Company. In 2019, a Chinese national was indicted on economic espionage charges when he stole a copy of a proprietary algorithm for optimizing agricultural productivity for farmers.

This has happened in my home State. There's open indictments against Chinese nationals for trying to steal rice-related intellectual property. I assume they have absconded back to mainland China by now. The efforts aren't limited to espionage. Just a few weeks ago, a Russian-linked group launched cyberattacks against JBS, one of the largest meatpackers in the United States. The ransomware attack temporarily shut down JBS's cattle slaughtering and resulted in JBS paying a Bitcoin ransom of almost \$11 million.

These type of attacks and espionage against agriculture don't just threaten the livelihoods of American farmers and companies. They also threaten our food supply chain. Do you think—do you agree that American agriculture is a target for foreign cyber actors who are looking for opportunities to attack?

Mr. VORNDRAN. Senator, thanks for the question. The answer to your question is yes, we believe they are a target. We believe everybody is a target. Whoever has a vulnerability, there is an adversary out there that will try to exploit it for any number of reasons. Number 1 reason: financial gain.

Senator COTTON. Thank you. Mr. Goldstein, do you agree that American agriculture is a target for attack?

Mr. GOLDSTEIN. As my colleague noted, absolutely, but for the same reasons as noted. Organizations that are vulnerable and can be exploited for profit are certainly a target for these adversaries.

Senator COTTON. Mr. Downing, I wasn't going to ask this question, but you committed the cardinal sin of a witness, clearly nodding your head. Directing fire in your way—

Mr. DOWNING. All right.

Senator COTTON [continuing]. Now, I'll say do you agree, as well?

Mr. DOWNING. Yes, no, I think that's exactly right. My—the section I supervise were part of some of those prosecutions, and we have had some successes in bringing Chinese actors to justice in the United States courts.

Senator COTTON. Since I'm with you, Mr. Downing, then, would you agree that it would improve the security of American agriculture if the industry and the regulators in Government had better and faster information about the threats that they might face from foreign cyber actors?

Mr. DOWNING. Yes, as we've said repeatedly today, reporting from victims is critical. We strongly support the idea that Congress take up this issue and to pass legislation that would require reporting of a variety of different kinds of attack, particularly ransomware, of course, the subject of this issue. Also attacks on our critical infrastructures and other high-risk attacks that would affect especially a wider circle other than just the victim.

Senator COTTON. I'm glad to hear you say that you think Congress should take up legislation because I have a bill that will do just that. My Agricultural Intelligence Measures Act would ensure the USDA has streamlined access to threat information relevant to key players in American agriculture. I think it's time that we step up and protect America's farmers and ranchers from the foreign threats that seek to destroy our food supply chain.

Let me turn to a topic in my time left that I know that Senator Klobuchar raised, which is cyber talent recruiting. I think, Mr.

Vorndran, I'll address this to you, as well. You have two types of positions at the FBI is my understanding, computer scientists and forensic examiners, that are especially important for responding to cyberattacks and investigating the hunt—to hunt for cybercriminals who committed them. Cyber threats are constantly evolving, of course, and therefore our response to those threats also requires to have tech talent that is on the cutting edge, is that right?

Mr. VORNDRAN. Yes, Senator, that is accurate.

Senator COTTON. You have to compete for those folks with some pretty big companies that can pay pretty generous salaries, like Google, Apple, Amazon, Microsoft, Oracle, Facebook, and innumerable startups. That's not even mentioning other top cybersecurity companies. Do you find that the high demand for the country's best graduates in science, technology, engineering, math, and related fields makes it harder to recruit and retain some of the best cyber experts?

Mr. VORNDRAN. Senator, we have an amazing workforce, and I can't underscore that enough. People dedicated to the mission and protection of this country. To your question, yes, sir, it is hard to recruit the number of people that we need with those skill sets.

Senator COTTON. My office has been in touch with the FBI on this issue, and I do respect greatly the workforce you have. I do think there are some things that we could do to provide the FBI more tools to get the very best talent in our country, and to retain them, as well.

I would liken some of the challenges that you might face to stuff I've heard on Armed Services Committee from Air Force pilots, who leave the Air Force, not only because they can make more pay in the private sector, but because they're not getting to do enough of what they joined the Air Force to do, to fly high-performance aircraft to focus on bad guys. The Government's never going to be able to pay as much as the airlines pay, and I suspect the Department of Justice is never going to be able to pay as much as Silicon Valley pays, but we want to give you every tool possible in the toolkit to make sure that we have the very best people working on this problem, and that they are fulfilled and rewarded in their job, and want to make it a long-term proposition, not a career. My time's expired.

Chair DURBIN. Thank you, Senator Cotton. Thanks to the witnesses for joining us today. While we cannot stop ransomware attacks completely, we can certainly be better prepared. We learned today that preventative measures are more cost-effective and have greater impact on stemming the rise of these attacks than in just increased enforcement alone.

We also learned how critical information sharing is between private and public sectors across Government agencies. What struck me about this hearing was there was a general bipartisan consensus on this side of the table. I like that. I think that's a positive thing, and I hope it leads—I think it will—to specific legislation to deal with this.

There was one dissenting voice who blamed the Biden administration for the problems of Colonial Pipeline and such. I think fairness requires us to be candid about other aspects of previous administrations, such as Solarwinds, which was a massive breach

that affected thousands of companies and the U.S. Government. It was discovered not by the U.S. Cyber Command, but by another private entity, I understand, named FireEye. It's an indication that we can and should strive to do better.

It also is important to note that it wasn't until this administration in April made the public declaration connecting the Russians to Solarwinds, that that statement became accepted. I think that's an indication of the intent of this administration, I hope every administration, to keep America safe.

We need to view this problem with a sense of urgency. I think that the legislation which you propose, Mr. Downing, is a beginning of a conversation with the administration on doing this, and as you notice from Senator Whitehouse, Graham, Tillis, and Blumenthal, they're anxious to move this forward. We want this Committee to facilitate that conversation.

The hearing record will remain open for 1 week for statements. Questions for the record may be submitted by 5 p.m. on Tuesday, August 3rd. I thank the witnesses again for being here. The hearing is adjourned.

[Whereupon, at 11:58 a.m., the hearing was adjourned.]

[Additional material submitted for the record follows.]



Department of Justice

STATEMENT OF

RICHARD W. DOWNING
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"AMERICA UNDER CYBER SIEGE:
PREVENTING AND RESPONDING TO RANSOMWARE ATTACKS"

PRESENTED

JULY 27, 2021

**STATEMENT OF
RICHARD W. DOWNING
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
UNITED STATES DEPARTMENT OF JUSTICE**

**BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE**

AT A HEARING ENTITLED

**“AMERICA UNDER CYBER SIEGE:
PREVENTING AND RESPONDING TO RANSOMWARE ATTACKS”**

**PRESENTED
JULY 27, 2020**

Good afternoon Chairman Durbin, Ranking Member Grassley, and distinguished members of the Senate Committee on the Judiciary. Thank you for the opportunity to testify on behalf of the Department of Justice regarding our efforts to combat ransomware and digital extortion.

I will cover three areas in my testimony today. First, I will describe the danger ransomware presents to our public safety and national and economic security. Second, I will discuss how the Department of Justice is responding to this threat, including recent actions taken by the Ransomware and Digital Extortion Task Force. Finally, I will address issues that Congress might consider to help the Department stop ransomware attacks. In that regard, I am pleased to announce the Administration’s support for national cyber breach legislation, along with some recommendations for how such legislation could help make the Department more effective in combatting cyber threats. Such legislation would assist our response to cyber attacks by helping the Department disrupt attacks and providing evidence critical to bringing offenders to justice. Ideally, it should provide the federal government with a more complete view of the cyber threat environment and the risk that cyber attacks pose to some of our nation’s most sensitive entities and information.

I. The Threat Posed by Ransomware Attacks

Ransomware is malicious software (“malware”) used by cyber actors to extort owners of computer systems. Typically, the malware encrypts files on the victim’s computer, rendering the files inaccessible, and leaves a ransom note demanding payment in exchange for a key to decrypt the files. To further coerce victims into paying, some actors steal sensitive information from victims and threaten to publish that information on the Internet if the ransom is not paid. Cyber actors typically demand payment in a virtual currency such as Bitcoin or Monero.

Ransomware is a serious threat to our public safety and national and economic security. It has been used to attack municipal governments, police departments, and critical infrastructure, such as suppliers of food and gasoline. Some cyber actors have specifically targeted health care facilities during the COVID-19 pandemic, taking advantage of the global crisis to extort victims who are especially vulnerable and cannot afford to lose access to data. The volume of ransomware attacks and the size of demands have skyrocketed as well. Reports of attacks to the FBI's Internet Crime Complaint Center increased dramatically year after year, with more than 200% increase in ransom amounts in 2020. Some individual ransom demands have exceeded \$50 million.

Compounding this problem, cyber actors continue to improve upon their ransomware tactics. Many actors now research their victims—identifying the victim's net worth, the cost of a business interruption, and even the value of their cyber insurance policy—to extort as much money as possible. To avoid detection by law enforcement, actors have migrated to the dark web, using the TOR network to host sites that they use to anonymously communicate with victims or to publish stolen victim data. Some actors also demand that ransoms be paid in virtual currencies with concealed blockchains—so-called “anonymity enhanced currencies”—which are specially designed to make it more difficult to trace or to attribute transactions.

The business model of ransomware has evolved as well. Many ransomware developers now offer ransomware-as-a-service (“RaaS”): an arrangement in which the developers license their ransomware to affiliates for a fee. Under a typical agreement, the developers manage the ransomware, the affiliates identify and attack victims, and these two parties split any ransom payments. The practical impact is that RaaS has lowered the barrier to entry for cybercrime because many criminals do not need to create their own ransomware. As a result, it is easier than ever for cyber actors to attack victims.

Federal agencies face significant obstacles in investigating ransomware attacks. First, ransomware is a transnational crime. Cyber actors take advantage of this fact by using infrastructure located around the world. A cyber actor may use a server in one country to disseminate ransomware; a server in a second country to hold stolen victim information; and an e-mail account in a third country to negotiate with victims. To obtain relevant information, law enforcement investigators often need to use numerous requests for assistance from foreign law enforcement agencies, a process that can be cumbersome and time-consuming.

Cyber actors also use sophisticated means to conceal their identities and criminal activities. Many ransomware groups host their websites on the dark web, which allows them to communicate anonymously with victims. And the advent of anonymity enhanced currencies means it is sometimes impossible for investigators to trace the flow of ransom payments. In addition, the profitability of ransomware has created an ecosystem of services dedicated to supporting it. For example, “bullet-proof” hosts refuse to cooperate with law enforcement authorities, allowing cyber actors to carry out criminal schemes without being identified or taken offline; “crypters” assist criminals by ensuring that their malware will not be detected by anti-virus software; and “mixers” help criminals hide illicit virtual currency payments.

Of course, some countries provide safe havens for actors to engage in cybercrime abroad, so long as they remain “on call” for those countries’ intelligence services. The Department of the Treasury announced new sanctions this year against the Federal Security Service (“FSB”), a Russian intelligence and law enforcement agency. According to the Treasury Department, the FSB used cyber means to target U.S. government personnel and citizens around the world. The FSB also bolstered its cyber operations by cultivating hackers, enabling them to conduct disruptive ransomware attacks. As we know, Russia has a long history of ignoring cybercrime within its borders so long as the criminals victimize non-Russians. And it has fought our efforts to extradite cybercriminals when they travel outside Russia. Indeed, in the past seven years, Russia has attempted to block lawful extradition requests that the U.S. has made on 14 occasions, successfully blocking extradition three times.

Additionally, in 2020, the Department of Justice unsealed charges against hackers in the People’s Republic of China who conducted ransomware attacks against international victims while simultaneously hacking targets on behalf of the China’s Ministry of State Security. Countries like Russia and China also refuse to bring cybercriminals to justice, thus providing a safe harbor for cybercrime.

Another difficulty our investigators face is that ransomware actors take advantage of web hosting services, e-mail accounts, online storage accounts, and other services offered by American companies, but those companies fail to meet their obligations when criminal investigators serve them with search warrants or preservation requests. Federal law requires companies to produce information when the government serves them with a search warrant. If the government obtains a warrant to search a house, agents must search that house within days of when the magistrate signs the warrant. But when the government serves a search warrant on a tech company, they often take weeks, if not months, to return data. And sometimes these companies do not produce any data because they failed to preserve the relevant account. These issues hinder our investigations significantly and are a major factor in criminals’ ability to escape detection and apprehension. We believe that in many cases, the cause of this problem is that providers think about complying with the law and protecting public safety only after they have developed a money-making product. Too often, we discover that providers have failed to prioritize responding to valid legal process: either they don’t hire enough staff to respond to legal process, or they equip that staff with outdated and slow tools, or both. While we have attempted to work with providers and have raised this issue repeatedly for years, too often solutions do not appear to be forthcoming.

Finally, investigations are hindered because many data breaches are not reported to federal authorities. This reluctance may be driven by a number of concerns, including a fear of regulatory action or reputational harm, or of an interruption to business operations. Whatever the cause, the U.S. government cannot act—it cannot warn, disrupt, prosecute, or take any other action—if it never learns about a cyber attack.

II. The Ransomware and Digital Extortion Task Force

The Department of Justice—through the Computer Crime and Intellectual Property Section (“CCIPS”), the U.S. Attorney community, the FBI, and other components—has been fighting ransomware and the related problem of mass-hacking by criminals since those threats first emerged. The Department devotes significant resources to identifying, extraditing, and prosecuting ransomware actors, dismantling their technical and financial infrastructure, seizing their virtual currency, and deterring others from committing offenses.

These efforts are assisted by the Department’s National Security Division, which has devoted significant resources to disrupting foreign nation-states’ use of cyber-enabled means to threaten our critical infrastructure, exert malign influence, and steal export-controlled technology, trade secrets, intellectual property, and personally identifying information. The National Security Division has carried out this mission by working with the U.S. Intelligence Community, the Department of Defense, the State Department, and other departments and agencies to implement a whole-of-government approach, including through prosecution, technical operations, economic sanctions, and diplomatic efforts. This expertise has proven invaluable as the Department uses an all-tools approach to address the threat of ransomware.

The Criminal Division also created the Cybersecurity Unit in CCIPS to channel the section’s prosecutorial and investigative expertise into the prevention of computer crimes, such as ransomware attacks. Through the Cybersecurity Unit, CCIPS has made resources available to help private sector organizations respond to ransomware threats and work more effectively with law enforcement in the aftermath of ransomware attacks. For instance, in 2018 the Cybersecurity Unit updated its white paper on *Best Practices for Victim Response and Reporting of Cyber Incidents* specifically to address handling ransomware incidents. The Cybersecurity Unit has also published white papers intended to help private organizations lawfully conduct activities like cyber intelligence gathering so they can avoid falling prey to ransomware.

But combating ransomware requires a whole-of-society response, including coordinated action by agencies across the federal government, collaboration with foreign partners, and assistance from victims and the private sector. Agencies across the federal government are focused on efforts to disrupt the criminal groups, trace and retrieve ransoms paid using virtual currency, improve the resilience of public and private computer networks, and closely coordinate our efforts with international partners. Recognizing the severity of this threat, the Office of the Deputy Attorney General created the Ransomware and Digital Extortion Task Force, which will ensure that the Department is using all its tools and authorities to protect our nation.

First, in an effort led by CCIPS, the Task Force will enhance the Department’s capability to disrupt, investigate, and prosecute ransomware attacks. This effort will include providing training and support to address the threat of ransomware; placing a greater emphasis on intelligence and lead-sharing across the Department; leveraging all sources of investigative leads, including human sources; and identifying links between criminal actors and nation-states. An

effective and long-lasting means of dealing with the ransomware threat uses law enforcement action, including prosecution and forfeiture of ill-gotten gains. The Department is focusing its resources on deterring cybercrime, including ransomware, through arrest, incarceration, infrastructure disruption, and forfeiture whenever possible.

Of course, ransomware does not exist in a vacuum. The Task Force will also aim to disrupt and dismantle the ecosystem that supports ransomware, as well as the means cyber actors use to monetize their extortion schemes. This will include the use of all available criminal, civil, and administrative actions for enforcement, ranging from takedowns of botnets (networks of infected victim computers) used to spread ransomware, to seizure of illicit profits where possible, and prosecution of the actors that help ransomware groups launder their ill-gotten gains. The Task Force will also ensure that the Department focuses on the services that allow these digital extortion schemes to persist, including online forums that advertise ransomware and hosting services that knowingly facilitate these attacks.

Because preventing ransomware attacks demands a whole-of-society approach, the Task Force will work with many of the Department's key federal partners: the Department of Homeland Security, including the U.S. Secret Service and the Cybersecurity and Infrastructure Security Agency ("CISA"); the Department of the Treasury, including the Office of Foreign Assets Control and the Financial Crimes Enforcement Network; the Department of Defense, including Cyber Command; the intelligence community, the Department of Commerce, the Department of State, and others. Coordination of these efforts will ensure that the whole of the U.S. government's resources may be brought to bear to address the threat of ransomware in a systematic and comprehensive way—including through the potential use of economic sanctions, virtual currency regulations, diplomatic pressure, intelligence operations, and military action.

Successfully protecting the nation also requires robust information sharing with the private sector. The Task Force will work to strengthen and enhance partnerships between the Department and industry across a wide range of sectors to address ransomware and digital extortion. To foster and encourage further information sharing, these efforts will build upon existing relationships between the Department and private sector companies, such as major online service providers, threat intelligence firms, and insurance firms whose clients are victimized by these schemes.

Finally, the Task Force will work to increase collaboration with our foreign partners to share information and coordinate efforts in combating ransomware. Because many of the actors responsible for these crimes and much of the infrastructure that facilitates these attacks are located overseas, close cooperation with our foreign partners has been and will continue to be crucial to successfully identify perpetrators, dismantle ransomware operations, and disrupt safe havens for malicious activity. Among other resources, the Task Force will leverage the International Computer Hacking and Intellectual Property ("ICHIP") Global Law Enforcement Network ("GLEN"), which provides training and assistance to law enforcement, prosecutorial, and judicial partners around the world to stop cybercrime. The network has already stood up, trained, and begun mentoring two cryptocurrency working groups; one in southeast Asia, the other in Eastern

Europe. The Department, in conjunction with the State Department, intends to focus training efforts within the GLEN on ransomware and criminal use of cryptocurrency in the coming months. The Department will also continue to promote the Budapest Convention, which is the gold standard for fighting cybercrime and has been increasingly adopted by countries around the world.

I am pleased to report that in the short time since the Task Force was created, the Department has already had success in combating ransomware:

- In May 2021, the Colonial Pipeline Company was a victim of a ransomware attack by the group DarkSide. The attack had clear national security implications: Colonial Pipeline provides gasoline to the eastern seaboard of the United States. Because of the attack, the company paid a ransom of more than \$4 million. After Colonial Pipeline's quick notification to law enforcement, the Department used a federal warrant to seize most of the ransom payment from the offenders.
- The Department obtained the conviction of Oleg Koshkin and Pavel Tsurkan last month for operating a crypting service that concealed malware from anti-virus programs. Koshkin and Tsurkan's service enabled hackers to infect thousands of computers around the world, including with ransomware.

There are other recent Department operations I want to highlight as well:

- In February, the Department arrested a Latvian national for offenses relating to Trickbot, a malware that stole personal and financial information and disseminated ransomware. Trickbot caused extensive financial harm and inflicted significant damage to critical infrastructure in the United States. According to the indictment, the defendant wrote code related to the control, deployment, and payments of ransomware.
- In January 2021, the United States, Canada, and Bulgaria disrupted NetWalker, ransomware that was used to attack hospitals and emergency services during the pandemic. According to public documents, law enforcement authorities in the U.S. and Bulgaria disabled a website used by NetWalker affiliates to communicate with victims and seized more than \$450,000 worth of ransom payments. Canadian police also arrested a NetWalker distributor based on U.S. charges, and he is now incarcerated pending extradition proceedings. NetWalker ceased operation that day and has remained down ever since.
- Also in January 2021, the Department and several international partners disrupted the Emotet malware. According to an affidavit filed by the FBI, Emotet had infected approximately 1.6 million computers worldwide and caused hundreds of millions of dollars in damage. It was also used to send ransomware to infected computers. As part of the operation, authorities took over Emotet's command-and-control infrastructure, cut off communications between infected computers and the botnet's administrators, and shut down hundreds of servers worldwide that were being used to spread and control the botnet.

These successes demonstrate the broad reach of the U.S. government and send a strong message that the Department will use all the tools at its disposal to disrupt the ransomware ecosystem.

III. Legislative Solutions to Better Combat Ransomware

The explosion of ransomware incidents in the last year has brought into stark relief how several statutory changes would help the Department address this threat. Congress should consider whether changes are needed in three areas: (A) prompt reporting of specific computer intrusions as a means of preventing them elsewhere; (B) improving our ability to disrupt criminal activity; and (C) enhancing our ability to prosecute offenders and the effectiveness of such prosecutions.

A. Prompt Reporting of Specific Computer Intrusions as a Means of Preventing them Elsewhere

In the examples I discussed earlier, federal authorities were able to investigate and disrupt ransomware attacks because victims identified themselves and cooperated with the ensuing investigations. Unfortunately, studies show that most data breaches are not reported to the U.S. government. This reluctance may be driven by any number of concerns (including a fear of regulatory action or reputational harm, or of an interruption to business operations) but it presents a major challenge in America's response to the ransomware threat. This gap means that some crimes are never investigated, and that investigations into ransomware schemes are robbed of timely access to evidence that could prove critical to identifying and prosecuting offenders. And law enforcement cannot effectively warn, disrupt, prosecute, or take any other action without fully understanding the threat environment, which requires cooperation from victims.

Recently, the bipartisan Cyberspace Solarium Commission recognized this problem and called for national data breach legislation that would "establish requirements for critical infrastructure entities to report cyber incidents to the federal government."¹ The Administration strongly supports Congressional action to require victim companies to report significant breaches, including ransomware attacks.

In particular, such legislation should require covered entities to notify the federal government about ransomware attacks, cyber incidents that affect critical infrastructure entities, and other breaches that implicate heightened risks to the government, the public, or third parties. In terms of statutory reporting thresholds, we would recommend breaches that implicate heightened risks include supply-chain breaches that are reasonably likely to provide outsiders with access to critical infrastructure or government systems; breaches involving high-value trade secrets that pertain to goods or services primarily sold to critical infrastructure or government entities;

¹ CYBERSPACE SOLARIUM COMM'N, Final Report (Mar. 2020), at 104 (available at <https://www.solarium.gov/>).

ransomware attacks above a certain threshold. We would also consider other statutory reporting thresholds, if appropriate.

We recommend that covered entities should be required to promptly notify the government within a defined period of time after learning they have been impacted by ransomware, another heightened-risk breach. Of particular significance, entities should be required to report any ransom demand; the date, time, and amount of ransom payments; and addresses where payments were requested to be sent. And importantly, victims who assist the government should not be worse off for having done so, so they should maintain whatever privileges they had prior to sharing the information to protect others.

Another significant question that should be answered in drafting such legislation is where companies should report breaches. We recommend there should be a streamlined entry point for victims to use to report incidents, with full and immediate sharing with all relevant federal agencies.

Such legislation would provide the federal government with a more complete view of the cyber threat environment and the collective risk that cyber threats pose to some of our nation's most sensitive entities and information. For example, it would help authorities become better aware of when actors target critical infrastructure, export-controlled information, and key biological research such as that involving COVID-19. Mandatory incident reporting would also assist federal efforts to defend the nation against cyber threats and to pursue the actors responsible for them.

B. Strengthening the Department's Ability to Disrupt Ransomware and Mass Hacking

For years, criminals have engaged in the mass hacking of Americans. Hackers are using state-of-the-art techniques to infect hundreds of thousands—sometimes millions—of computers, all while becoming increasingly difficult to detect. Using techniques such as phishing or web browser exploitation, they have sought to install their own malicious software on as many computers as they can. They have chained these computers into massive networks, called botnets, which they have used to enable other crime, including sending spam or stealing online banking credentials. Ransomware is another escalation in this trend. While some ransomware actors specifically target certain victims, others are exploiting the fruits of massive illegal hacking.

The Department of Justice works to stop these crimes before they happen. We call this disruption. Arresting criminals is the strongest form of disruption, but not the only one. Using a combination of online operations and court orders, the Department seeks to gain control of criminal infrastructure and shut it down, or at least render it harmless. We did this, for example, in January, when we took over and shut down the Emotet botnet that had been used to spread ransomware.

One powerful tool the Department has used to disrupt botnets and free victim computers from malware is the civil injunction process. Current law gives federal courts the authority to issue injunctions to stop the ongoing commission of certain crimes by authorizing actions that

prevent a continuing and substantial injury. This authority played a critical role in the Department's successful disruption of the Coreflood botnet in 2011 and of the Gameover Zeus botnet and related Cryptolocker ransomware in 2014. (The Gameover Zeus botnet, which infected computers worldwide, inflicted more than \$100 million in losses on American victims alone.) Because the criminals behind these particular botnets used them to commit fraud against banks and bank customers, existing law allowed the Department to obtain court authority to disrupt the botnets by taking actions such as disabling communications between infected computers and the command-and-control servers.

The problem is that current law permits courts to consider injunctions only for certain crimes, including certain frauds and illegal wiretapping. Botnets, however, can be used for many different types of illegal activity, such as denial-of-service attacks or to install ransomware. Depending on the facts of any given case, these crimes may not constitute fraud or illegal wiretapping. In such instances, courts may lack the statutory authority to enjoin botnets in the same way that injunctions were used to incapacitate the Coreflood and Gameover Zeus botnets. The Administration has therefore proposed legislation to address this problem by granting courts the authority to enjoin a greater range of botnets and other cybercrime involving damage to 100 or more computers. (See Appendix A)

In addition, the statutes that prohibit the creation and use of botnets also have shortcomings because they do not clearly prohibit the *sale* or *renting* of a botnet. In one case, for example, undercover officers discovered that a criminal was offering to sell a botnet consisting of thousands of victim computers. The officers "bought" the botnet from the criminal and notified victims that their computers were infected. The operation, however, did not result in a prosecutable U.S. offense, because there was no evidence that the seller himself had created the botnet in question.

We believe that it should be illegal to sell or rent surreptitious control over infected computers to another person, just like it is already illegal to sell or transfer computer passwords. That is why the proposed legislation would prohibit the sale or transfer not only of "password[s] and similar information" (the wording of the existing statute) but also of "means of access," which would include the ability to access computers that were previously hacked and are now part of a botnet. (See Appendix A)

C. Enhancing our Ability to Prosecute

Finally, we support additional changes to the Computer Fraud and Abuse Act ("CFAA") that would make the statute more effective in the fight against ransomware. Key amongst these proposals is an amendment to Section 1030 to bring the forfeiture provisions of the CFAA in line with other federal statutes. This would provide concrete procedures for the forfeiture of property used to commit or facilitate a violation of the CFAA, as well as the proceeds of such violation. (See Appendix A)

In addition, the Administration has proposed an amendment that would update the CFAA to add penalties for the crime of conspiracy. Although the CFAA currently prohibits conspiracies to commit computer fraud, it does not clearly set forth penalties for that crime. As a result, there has been some reluctance to charge conspiracy under the CFAA because there is uncertainty over

the penalties that would apply. Consistent with other federal criminal statutes and with the structure of the CFAA, a charge of conspiracy or attempt will receive the same penalty as the corresponding substantive offense under Section 1030. (See Appendix B)

IV. Conclusion

I want to thank the Committee again for providing me the opportunity to discuss these important issues on behalf of the Department of Justice. We look forward to continuing to work with Congress to improve the government's ability to counter ransomware and digital extortion attacks. I am happy to answer any questions you may have.

APPENDIX A

Cybercrime Mitigation Act

Section 1: Short Title.

This Act may be cited as the “Cybercrime Mitigation Act.”

Section 2: Injunctions to Stop Damage to 100 or More Computers.

(a) AMENDMENT.—Section 1345 of title 18, United States Code, is amended—

(1) in the heading, by inserting “and abuse” after “fraud”;

(2) in subsection (a)—

(A) in paragraph (1)—

(i) in subparagraph (B), by striking “or” at the end;

(ii) in subparagraph (C), by inserting “or” after the semicolon; and

(iii) by inserting after subparagraph (C) the following:

“(D) violating or about to violate section 1030(a)(5) of this title where such conduct has caused or would cause damage (as defined in section 1030) without authorization to 100 or more protected computers (as defined in section 1030) during any 1-year period, including by—

“(i) impairing the availability or integrity of the protected computers without authorization; or

“(ii) installing or maintaining control over malicious software on the protected computers that, without authorization, has caused or would cause damage to the protected computers;” and

(B) in paragraph (2), in the matter preceding subparagraph (A), by inserting “, a violation described in subsection (a)(1)(D),” before “or a Federal”; and

(3) by adding at the end the following:

“(c) A restraining order, prohibition, or other action described in subsection (b), if issued in circumstances described in subsection (a)(1)(D), may, upon application of the Attorney General—

“(1) specify that no cause of action shall lie in any court against a person for complying with the restraining order, prohibition, or other action; and

“(2) provide that the United States shall pay to such person a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in complying with the restraining order, prohibition, or other action.”

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 63 of title 18, United States Code, is amended by striking the item relating to section 1345 and inserting the following: “1345. Injunctions against fraud and abuse.”.

Section 3: Stopping Dealing in Botnets; Forfeiture

(a) IN GENERAL.—Section 1030 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (7), by adding “or” at the end; and

(B) by inserting after paragraph (7) the following:

“(8) intentionally deals in the means of access to a protected computer, if—

“(A) the dealer knows or has reason to know the protected computer has been damaged in a manner prohibited by this section; and

“(B) the promise or agreement to pay for the means of access is made by, or on behalf of, a person the dealer knows or has reason to know intends to use the means of access to—

“(i) damage a protected computer in a manner prohibited by this section;
or

“(ii) violate section 1037 or 1343;”;

(2) in subsection (c)(3)—

(A) in subparagraph (A), by striking “(a)(4) or (a)(7)” and inserting “(a)(4), (a)(7), or (a)(8)”; and

(B) in subparagraph (B), by striking “(a)(4), or (a)(7)” and inserting “(a)(4), (a)(7), or (a)(8)”; and

(3) in subsection (e)—

(A) in paragraph (13), by striking “and” at the end;

(B) in paragraph (14), by striking the period at the end and inserting “; and”;
and

(C) by adding at the end the following:

“(15) the term “deal” means transfer, or otherwise dispose of, to another as consideration for the receipt of, or as consideration for a promise or agreement to pay, anything of pecuniary value.”;

(4) in subsection (g), in the first sentence, by inserting “, except for a violation of subsection (a)(8),” after “of this section”; and

(5) by striking subsections (i) and (j) and inserting the following:

“(i) CRIMINAL FORFEITURE.—

“(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

“(A) such person’s interest in any property, real or personal, that was used or intended to be used to commit or to facilitate the commission of such violation; and

“(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

“(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial proceeding, shall be governed by the provisions of section 413 of the Controlled Substances Act (21 U.S.C. 853), except subsection (d) of that section.

“(j) CIVIL FORFEITURE OF PROPERTY USED OR INTENDED TO BE USED IN THE COMMISSION OF AN OFFENSE.—

“(1) Any personal property that was used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section, shall be subject to forfeiture to the United States.

“(2) Seizures and forfeitures under this subsection shall be governed by the provisions of chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.”.

APPENDIX B

Act to Update Conspiracy in the Computer Fraud and Abuse Act

Section 1: Short Title.

This Act may be cited as the “Act to Update Conspiracy in the Computer Fraud and Abuse Act.”

Section 2: Penalties for Conspiracies to Violate Section 1030.

Section 1030 of title 18, United States Code, is amended in subsection (c)—

(A) in paragraph (1)—

- (i) in subparagraph (A), by inserting “or a conspiracy” before “to commit an offense punishable under this subparagraph”; and
- (ii) in subparagraph (B), by inserting “or a conspiracy” before “to commit an offense punishable under this subparagraph”;

(B) in paragraph (2)—

- (i) in subparagraph (A), by inserting “or a conspiracy” before “to commit an offense punishable under this subparagraph”;
- (ii) in subparagraph (B), by inserting “or a conspiracy” before “to commit an offense punishable under this subparagraph”; and
- (iii) in subparagraph (C), by inserting “or a conspiracy” before “to commit an offense punishable under this subparagraph”;

(C) in paragraph (3)—

- (i) in subparagraph (A), by inserting “or a conspiracy” before “to commit an offense punishable under this subparagraph”; and
- (ii) in subparagraph (B), by inserting “or a conspiracy” before “to commit an offense punishable under this subparagraph”;

(D) in paragraph (4)—

- (i) in subparagraph (A)—
 - (1) in subparagraph (i), by striking “attempted” and inserting “attempt or a conspiracy to commit an” before “offense, would, if completed, have caused”; and

(2) in subparagraph (ii), by inserting “or a conspiracy” before “to commit an offense punishable under this subparagraph”;

(ii) in subparagraph (B)—

(1) in subparagraph (i), by striking “attempted” and inserting “attempt or a conspiracy to commit an” before “offense, would, if completed, have caused”; and

(2) in subparagraph (ii), by inserting “or a conspiracy” before “to commit an offense punishable under this subparagraph”;

(iii) in subparagraph (C)—

(1) in subparagraph (i), by striking “an offense or an attempt to commit an offense under” and inserting “an offense, or an attempt or a conspiracy to commit an offense, under” before “subparagraphs (A) or (B)”; and

(2) in subparagraph (ii), by inserting “or a conspiracy” before “to commit an offense punishable under this subparagraph”;

(iv) in subparagraph (D)—

(1) in subparagraph (i), by striking “an offense or an attempt to commit an offense under” and inserting “an offense, or an attempt or a conspiracy to commit an offense, under” before “subsection (a)(5)(C)”; and

(2) in subparagraph (ii), by inserting “or a conspiracy” before “to commit an offense punishable under this subparagraph”;

(v) in subparagraph (E), by inserting “, conspires to cause, ” before “or knowingly or recklessly causes death”;

(vi) in subparagraph (F), by inserting “, conspires to cause, ” before “or knowingly or recklessly causes death”;

(vii) in subparagraph (G)—

(1) in subparagraph (ii), by inserting “or a conspiracy” before “to commit an offense punishable under this subparagraph”.



Testimony

Eric Goldstein

**Executive Assistant Director for Cybersecurity
Cybersecurity and Infrastructure Security Agency**

U.S. Department of Homeland Security

FOR A HEARING

BEFORE THE UNITED STATES SENATE

Committee on the Judiciary

America Under Cyber Siege: Preventing and Responding to Ransomware Attacks

July 27, 2021

Washington, D.C.

Chairman Durbin, Ranking Member Grassley, and members of the Committee, thank you for the opportunity to testify today on behalf of the Cybersecurity and Infrastructure Security Agency (CISA) regarding ransomware and the federal response to combat this growing threat.

Given the surge of debilitating ransomware attacks against private sector businesses and our critical infrastructure, as well as recent cybersecurity incidents impacting the federal government, this hearing provides a timely opportunity to review how CISA works with federal agencies and private sector entities to manage cybersecurity incidents in light of the urgent ransomware challenge. I also look forward to discussing lessons learned from recent cybersecurity incidents and sharing some perspective on how we can apply those lessons to improve our collective cybersecurity.

CISA's Mission and Role in Cybersecurity

CISA leads national efforts to advance the cybersecurity, physical security, and resilience of our critical infrastructure. In particular, CISA is a focal point to exchange cyber defense information and enable defensive operational collaboration among the Federal Government, and state, local, tribal and territorial (SLTT) governments, the private sector, and international partners.

One of CISA's primary missions is to enhance the security of federal networks. To accomplish this mission, CISA leads a collaborative effort with its partners throughout the Department of Homeland Security (DHS), the Office of Management and Budget and the broader interagency to identify and drive reduction of the most significant cyber risks, which includes providing tools, services, training, guidance and direction that helps enable timely identification of, protection against, and response to cybersecurity risks. We *Defend Today* through collective defense against threats and vulnerabilities and *Secure Tomorrow* by providing effective strategies and approaches to long-term risk management and cyber resilience. Our vision is a secure and resilient cyber enterprise that enables the federal government to provide critical services to the American people under all conditions.

We have an equally important mission to lead efforts to secure the nation's critical infrastructure, including SLTT government networks, against cybersecurity risks that could result in disruption to National Critical Functions upon which the American people depend. Federal civilian agencies, private sector businesses of all sizes, and critical infrastructure owners are facing urgent cybersecurity risks, including from nation-states and criminal groups such as ransomware gangs. To address these risks, CISA focuses on gaining visibility, improving operational coordination, and driving remediation.

First, CISA is focused on gaining visibility into cybersecurity risks that will allow us to more effectively help victims and provide timely information to help prevent future incidents. We work to achieve this goal by providing sensors and other capabilities, such as remote scanning and threat hunting to identify suspicious, malicious, or potentially risky activity across federal civilian networks.

Second, CISA is uniquely positioned to receive and analyze data from multiple sources, including the intelligence community, the private sector, SLTT governments, and other partners, to understand how seemingly unrelated activity may indicate a significant intrusion or even a widespread campaign. CISA also works to prioritize identified risks by leveraging the capabilities of our National Risk Management Center (NRMC) to understand relative criticality of critical infrastructure assets – such as our oil and gas pipeline and electric-grid infrastructure – and working with our partners across government to understand our adversaries’ intent and capabilities to exploit existing and emerging vulnerabilities.

Third, CISA drives remediation actions by providing incident response support and by coordinating with government and private sector partners for joint cyber defense operations that bring together capabilities from both sectors. Additionally, CISA further drives remediation by issuing binding directives for federal agencies to carry out, and a suite of recommendations through alerts and notices for the private sector’s use and implementation in their own networks and cybersecurity defenses.

Cyber intrusions over the past several months have further reflected the fact that our country is facing an immediate threat to our national security, economic prosperity, and public health and safety. Nation-state actors and criminal groups continue to increase their sophistication and their willingness to target organizations across all sectors of the economy. The impacts of these attacks continue to increase, including impacts to the provision of National Critical Functions from healthcare to energy to agriculture.

Ransomware: CISA Actions to Combat a Growing Threat

Ransomware is an ever-evolving form of malware that encrypts files on a device, rendering the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption, and often threaten to sell or leak the victim’s data if the ransom is not paid. Malicious actors continue to evolve their ransomware tactics over time, and CISA is urgently focused on reducing the risk of ransomware attacks that are targeting organizations across sectors.

Recently, ransomware attacks have surged among SLTT governments and critical infrastructure organizations. In fact, it is estimated that over 100 federal, state and municipal agencies, over 500 medical centers, and 1,680 educational institutions in the United States were hit by ransomware in 2020 and ransom demands exceeded \$1 billion dollars.¹ This epidemic is now affecting our nation’s most critical infrastructure: municipal governments, police departments, hospitals, schools, manufacturing facilities, and of course, pipelines.

While some recent incidents like the intrusion affecting Kaseya, an IT company providing remote management services for global customers including many Managed Service Providers, were more ambitious than usually observed from ransomware actors. Most

¹ Emsisoft, *The State of Ransomware in the US: Report and Statistics 2020*, <https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/>; Emsisoft, *The Cost of Ransomware in 2020: A Country-by-Country Analysis*, <https://blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/>.

ransomware attacks generally do not use zero-day vulnerabilities or exquisite tradecraft, but rather exploit known security weaknesses or a failure to adopt generally accepted best practices. Consequently, much of CISA's efforts to mitigate ransomware are focused on ensuring that all organizations in our country understand the risks of ransomware and providing proactive measures governments, organizations and businesses can take to prevent themselves from becoming a victim of a ransomware attack in the first place.

To that end, CISA and DHS have acted urgently to catalyze national action around this risk, and in January 2021, CISA unveiled the Reduce the Risk of Ransomware Campaign to raise awareness and blunt this ongoing and evolving threat. The campaign is a focused, coordinated and sustained effort to encourage public and private sector organizations to implement best practices, tools, and resources that mitigate ransomware risk. Additionally, in coordination with the Multi-State Information Sharing and Analysis Center (MS-ISAC), CISA released a joint Ransomware Guide that details industry best practices and a response checklist that can serve as a ransomware-specific addendum to state and local governments' cyber incident response plans.

Moreover, in February, during his first remarks dedicated to cybersecurity, Secretary Mayorkas issued a call for action to tackle ransomware more effectively, and to further drive a call to action, Secretary Mayorkas initiated a Ransomware Sprint in April 2021 that has included a series of high-profile national events intended to ensure that leaders across all sectors of the economy understand the criticality of this risk and take urgent action in response.

By implementing various best practices, governments and businesses can reduce their ransomware attack surface. For example, we encourage our partners to maintain offline and encrypted backups of data; conduct regular vulnerability scanning to identify and address vulnerabilities; regularly patch and update software and operating systems, including antivirus and anti-malware software; implement a cybersecurity user awareness and training program, including guidance on identifying and reporting suspicious activity; and implement an intrusion detection system (IDS) to detect command and control activity. These are among many other best practices contained in CISA's numerous guides and directives that organizations can access to help protect themselves from becoming the next ransomware victim. In addition, we urge all organizations impacted by a ransomware intrusion to immediately report their incident to law enforcement and to CISA so that the incident can be appropriately investigated. Upon receiving a report of a ransomware intrusion, CISA can offer technical guidance to help an organization effectively recover and develop alerts to help protect other possible victims.

To support our partners' cybersecurity posture, CISA provides a number of no-cost resources we encourage everyone to take advantage of. For example, we encourage SLTT governments to join the MS-ISAC, which is a free and voluntary center enabling bi-directional sharing of best-practices and network defense information regarding cybersecurity trends, including ransomware and malware that is a precursor to ransomware. Similarly, the Nationwide Cybersecurity Review is a no-cost, anonymous, annual self-assessment designed to measure gaps and capabilities of SLTT governments' cybersecurity programs. The Cybersecurity Review is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and is sponsored by DHS and the MS-ISAC.

Additionally, CISA provides assessments to help organizations understand how they can improve their defenses to avoid ransomware infection along with cyber exercises to evaluate and develop a cyber incident response plan in the context of a ransomware incident scenario. Moreover, CISA recently launched a new Ransomware Readiness Assessment to help all organizations evaluate their maturity in preparing for and responding to ransomware attacks. CISA also offers several services such as vulnerability scanning and remote penetration testing to assess, identify and reduce organizations' exposure to cybersecurity threats, including ransomware, at no cost. By requesting these services, organizations of any size can reduce their risk to ransomware attacks and other cyber threats. Finally, CISA has Cyber Security Advisors (CSAs) deployed across the country to advise on best practices and to connect governments and businesses with additional CISA resources.

Most recently, building on earlier ransomware campaigns, on July 15, 2021 DHS spearheaded a new inter-agency website – *StopRansomware.gov*, a collaborative initiative to make it easier for organizations across the country to access the information they need to prepare for and respond to ransomware intrusions. *StopRansomware.gov* is the new ransomware homepage for federal government agencies, including CISA, the FBI, U.S. Department of Health and Human Services, U.S. Secret Service, and the National Institute of Standards and Technology (NIST), to pool resources that can give businesses and organizations of all sizes a one-stop-shop to learn how to reduce their ransomware risk and provide them the opportunity to better protect their networks. The website will also highlight the latest ransomware-related alerts from these agencies.

Ransomware is a critical challenge and the risks posed to our nation are severe. But the challenge is not insurmountable. By investing in improved cybersecurity as recommended in CISA guidance, organizations can reduce the risk of a ransomware intrusion and limit its potential impacts.

Mitigating Future Risks

The recent high-profile ransomware attacks the country has faced – from the intrusions into the Colonial Pipeline Company and JBS Foods to the Kaseya supply-chain compromise – must serve as an urgent call to action to address our nation's cybersecurity risks. We must collectively and with great urgency strengthen our nation's cyber defenses, invest in new capabilities, and change how we think about cybersecurity, recognizing that all organizations are at risk, and we must focus on ensuring the resilience of essential services. To that end, CISA is acting with the utmost resolve to drive reduction of cyber risk to federal networks, SLTT governments, the private sector, and across the National Critical Functions. Achieving the progress we seek will require consideration of several key areas.

First, CISA is currently investing in and growing capabilities to increase visibility into cybersecurity risks across federal agencies and across non-federal entities. To accomplish this, we must enhance our ability to conduct persistent hunts for threat activity, ingest and analyze security data at all levels of the network, and conduct rapid analysis to identify and act upon known threats. At the same time, CISA is driving adoption of defensible network architectures, including implementation of zero-trust environments in which the perimeter is presumed

compromised and security must focus on protecting the most critical accounts and data. President Biden's Executive Order on *Improving the Nation's Cybersecurity* will drive critical progress in advancing cybersecurity across the federal government. Going forward, we must take lessons learned from our investments in federal cybersecurity to support organizations across sectors in driving similar change.

Second, CISA must work with all possible partners to gain increased visibility into national risks. With increased visibility, we can better identify adversary activity across sectors, which allows us to produce more targeted guidance, understand the degree to which adversary activity across sectors is increasing risk, and identify particular incidents requiring a specialized CISA response team. Our partnership with TSA to develop two Security Directives requiring reporting of cybersecurity incidents to CISA is an important step and an example of such collaboration. We look forward to working with Congress to further encourage reporting of cybersecurity incidents to the federal government in order to further enable this essential visibility.

Third, incidents such as the Colonial Pipeline Company ransomware attack reinforces the need for CISA to continue to invest in and mature our partnerships with critical infrastructure entities across industries. For example, our Cyber Information Sharing and Collaboration Program (CISCP) serves as a bi-directional forum in which CISA and private industry are collaborating on significant risks, developing sector-specific threat-focused products, and providing briefings on new trends, threats, and capabilities across the sectors. With information sharing protections available through the Cybersecurity Information Sharing Act of 2015 and the Protected Critical Infrastructure Information Act, the program enables trusted sharing between CISA and a network of high impact companies, Information Sharing and Analysis Centers (ISACs), and service providers.

Within CISCP, the Mutual Interest Initiative brings together cyber threat companies and Internet service providers to work with CISA and the broader government community to exchange analysis and collaboratively work on threat actor focused products. Furthermore, CISCP enables CISA to work in close coordination with software vendors and endpoint detection companies to both assess the impact of and mitigate the risk of critical vulnerabilities. From a technical standpoint, these partnerships with industry enable us to better understand the nature of vulnerabilities pre-and post-disclosure and in turn provided timely and thorough mitigation guidance to government agencies and critical infrastructure.

Going forward, CISA is establishing a Joint Cyber Planning Office (JCPO), as required by the Fiscal Year 2021 National Defense Authorization Act, to further mature our capabilities to plan, exercise, and coordinate cyber defense operations with partners across the government and private sectors. The JCPO will develop a comprehensive ransomware campaign plan that will unify efforts, synchronize activities, and identify strategic objectives to increase resilience and reduce the likelihood of a ransomware attack. Further, the JCPO will design and implement joint cyber defense plans to thwart efforts by malicious cyber actors to disrupt critical infrastructure through a whole-of-nation approach to cyber defense operations.

Lastly, recognizing that we cannot prevent all intrusions, we must drive a focus on resilience and functional continuity even as we drive improvements in security. We must advance business continuity exercises even as we catalyze adoption of cybersecurity best practices; we must ensure that operational technologies are segmented from and can run independently from business networks even as we advance our ability to detect threats in both environments; and, we must reduce single points of failure across our National Critical Functions as we identify and harden identified nodes of systemic risk.

Conclusion

Our nation is facing unprecedented risk from cyber attacks undertaken by both nation-state adversaries and criminals. The list of significant incidents in recent months is long and growing. Now is the time to act – and CISA is helping to lead our national call to action. We will deepen our partnerships with critical infrastructure partners, enhance our visibility into national cybersecurity, and drive targeted action to reduce vulnerabilities and detect our adversaries. In collaboration with our government partners, critical infrastructure entities, our international allies, and with the support of Congress, we will make progress in addressing this risk and maintain the availability of critical services to the American people under all conditions.

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



**Jeremy Sheridan
Assistant Director
Office of Investigations
United States Secret Service**

U.S. Department of Homeland Security

**Prepared Testimony
Before the
United States Senate
Committee on Judiciary**

July 27, 2021

Good morning Chairman Durbin, Ranking Member Grassley, and members of this Committee: Thank you for inviting me to testify before you on the threat of ransomware and the risks it poses to the American people. My testimony today will seek to highlight how the ransomware environment has evolved in recent years, with attacks becoming more frequent, more hazardous, and more costly over time, and what the U.S. Secret Service and our partners across the Federal Government, and around the world, are doing to hold criminal actors accountable.

My name is Jeremy Sheridan and I am the Assistant Director of the Office of Investigations. In this role, I lead more than 160 Secret Service field offices and direct our network of Cyber Fraud Task Forces (CFTFs) in their investigations of sophisticated computer and financial crimes. I work to ensure our global network of field offices and task forces effectively detect and arrest those who are engaging in the criminal violations we are authorized to investigate,¹ while fully supporting our diverse protective requirements across the world.

Year-over-year, the U.S. Secret Service has observed a marked uptick in the frequency, sophistication, and destructiveness of ransomware attacks against the American people. While this surge is due to a number of complex and interrelated factors, we believe the principal forces driving it are 1) the swelling profitability of these attacks, in part as a result of the growth of cryptocurrencies as a form of extortion payment; 2) the lack of adequate defenses on the part of many U.S.-based organizations; and 3) perhaps most importantly, the maturation of a cybercriminal ecosystem that has grown more sophisticated and destructive over the decades, perpetrating increasingly brazen attacks.

There is no silver bullet for any of these contributing factors. We must recognize that ransomware will be with us for some time to come. But there is still much that we can do to improve the current situation.

- First, we must reduce the profitability of ransomware campaigns by scaling up law enforcement efforts to detect and interdict the proceeds of these extortion schemes.
- Second, we must work with private sector, state and local governments, and other vulnerable organizations to improve their own network defenses.
- Third, we must dramatically intensify national and international efforts to investigate, arrest, and prosecute those engaged in ransomware and other transnational cybercrimes.

Absent these combined efforts, I foresee an increase in both the severity and frequency of highly disruptive ransomware attacks. So long as greedy individuals lacking moral scruples can access the Internet, cybercrime will be with us. Even still, we can substantially reduce these harms by improving our collective defenses and by making cybercrime both less profitable and more risky to the criminals. I'm proud to say that the U.S. Secret Service stands ready to play our part in this effort.

The U.S. Secret Service Approach

The Secret Service has been at the forefront of combatting ransomware and related cybercrimes from their earliest iterations, and we continue this work today. Building upon our more than 150 years of experience fighting financial crimes, our approach has been, and continues to be, to “follow the money.”

¹ See 18 U.S.C. §§ 1028-1030, and 3056(b).

We have investigated and arrested some of the world's most notorious cybercriminals, including many of whom were thought to be beyond the reach of law enforcement.²

Together with our partners, we have successfully investigated and ultimately shut down a number of illicit digital money providers and exchanges³ that actively facilitated the laundering of transnational cybercriminal proceeds, including proceeds from ransomware. These include Liberty Reserve⁴ in 2013 and BTC-e⁵ in 2017, both of which have been accused of serving as key platforms for cybercriminals to transfer and launder proceeds through digital money.

With respect to ransomware specifically, the Secret Service has been investigating cases since at least 2013, when the ransomware variant known as CryptoLocker, the first known ransomware strain to leverage bitcoin as its extortion payment method, emerged on the cybercrime scene. At the time, ransomware attacks constituted only a small fraction of the overall cybercrime market. Ransom demands for CryptoLocker were typically low – often less than \$300.⁶

Today, the situation has radically changed for the worse, as we all recognize. The average ransom demand has skyrocketed, according to industry estimates. Some ransomware groups are reportedly demanding as much as \$10 million to \$20 million to free their locked computer systems.⁷ Ransomware actors are targeting not just big businesses with deep pockets, but also schools, city governments, and most tellingly, hospitals, even in the midst of a global pandemic.

The Secret Service has responded to ransomware attacks against a wide array of organizations, including municipalities and police departments. Our law enforcement partners around the nation share similar experiences. As the attacks on the Colonial Pipeline Company, JBS Foods, and Kaseya from this past year clearly reveal, these criminals will go to any length in their relentless pursuit of profit.

² See, “Russian Cyber-Criminal Sentenced to 27 Years in Prison for Hacking and Credit Card Fraud Scheme,” available at, <https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-27-years-prison-hacking-and-credit-card-fraud-scheme>; “Russian National Admits Role in Largest Known Data Breach Conspiracy Ever Prosecuted,” <https://www.justice.gov/opa/pr/russian-national-admits-role-largest-known-data-breach-conspiracy-ever-prosecuted>; “Russian National Pleads Guilty to Running Online Criminal Marketplace,” <https://www.justice.gov/usao-edva/page/file/1238961/download>; “Ukrainian Citizen Sentenced To 41 Months In Prison For Using Army Of 13,000 Infected Computers To Loot Log-In Credentials, Payment Card Data,” <https://www.justice.gov/usao-ni/pr/ukrainian-citizen-sentenced-41-months-prison-using-army-13000-infected-computers-loot-log>; “Ukrainian National Who Co-founded Cybercrime Marketplace Sentenced to 18 Years in Prison,” <https://www.justice.gov/opa/pr/ukrainian-national-who-co-founded-cybercrime-marketplace-sentenced-18-years-prison>.

³ Exchanges are businesses that allow for the trade of digital currencies for other assets, such as conventional fiat money, such as US dollars, or other digital currencies.

⁴ See Manhattan District Attorney, “DA Vance Testimony on Digital Currency before the Department of Financial Services,” <https://www.manhattanda.org/da-vance-testimony-on-digital-currency-before-the-department-of-financial-services/>.

⁵ See, “Russian National and Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox,” <https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged>.

⁶ See, “CryptoLocker Ransomware,” available at <https://www.secureworks.com/research/cryptolocker-ransomware>.

⁷ See, “Ransomware Threat Assessments: A Companion to the 2021 Unit 42 Ransomware Threat Report,” available at <https://unit42.paloaltonetworks.com/ransomware-threat-assessments/>.

Ransomware as an Evolution of Cybercrime

The evolution of ransomware from a relatively minor nuisance to a substantial threat to our homeland has been a gradual but steady process. Ransomware is just the latest and most pernicious trend to emerge out of a cybercriminal ecosystem that has been building in size and sophistication for decades.

The origins of ransomware can be traced back to the 1990s and early 2000s, when the vast majority of financially-motivated cybercrime – or “electronic crime,” as the Secret Service called it at the time – was focused on the theft and sale of credit card numbers and personally identifiable information (PII). Cybercriminals would hack into an organization to steal its customer account data, including credit card numbers and PII, which would later be used to make fraudulent purchases, or to sell to other criminals to further other criminal schemes. This cycle of theft, sale, and resale of credit card numbers and PII created a vast underground digital marketplace, in which stolen account information or even access to a victim’s computers could be bought and sold in a growing set of cybercriminal forums operating on the Internet.

As the marketplace matured, criminals began sharing best practices for hacking, laundering illicit proceeds, and avoiding detection by law enforcement. Cybercriminals who specialized in one particular area of cybercrime – such as network intrusion, malware development, or money laundering – began offering their products and services to others in exchange for a fee, or a percentage of the illicit proceeds of the scheme in which those products or services were to be used. Thus, the “crime-as-a-service” industry was born, an industry upon which much of today’s ransomware environment depends.

This maturation coincided with, and in certain respects was the result of, two key technological developments. The first was the arrival of bitcoin as the first widely accepted cryptocurrency in 2009. Bitcoin, which is based on public-key cryptography and ongoing decentralized computation to form a blockchain, offered cybercriminals a novel means of accepting and transferring value, one that does always comply with the oversight and controls placed on traditional banking and financial systems.

Around the same time, we witnessed the second key technological development: the adoption of EMV chips by major U.S. and global credit card providers.⁸ EMV chips, which require physical position of a card and an associated PIN number, made a variety of criminal schemes much more difficult to undertake. EMV adoption, while still ongoing to this day in the United States, served to dramatically reduce the profitability of credit card theft. It forced cybercriminals to look for alternative schemes. Many turned to ransomware, which, following the success of CryptoLocker in 2013, appeared to be the next “hot” criminal enterprise. And indeed it was.

Over the ensuing years, ransomware became increasingly sophisticated and professionalized. Today’s ransomware gangs employ a vast array of specialists, from malware developers to human resources departments to public relations teams. They meticulously gather information on victim organizations and set extortion prices based on the information they collect. Gangs even employ encrypted text-over-the-Internet chat services to facilitate communication between victims and ransomware operators, offer discounts for rapid payments, and charge penalties for payment delays by victims. Dozens of new ransomware strains have been developed and deployed against U.S. targets. These have been some of the

⁸ Sec., “The President’s BuySecure Initiative: Protecting Americans from Credit Card Fraud and Identity Theft,” <https://obamawhitehouse.archives.gov/blog/2014/10/17/president-s-buysecure-initiative-protecting-americans-credit-card-fraud-and-identity>.

most destructive cyber-attacks in recent memory, such as Petya in 2016, WannaCry in 2017, and Darkside in 2021. Many new ransomware strains built upon those that came before them, adding layers of encryption and obfuscation, making defense and mitigation efforts far more challenging.

Alarming, ransomware actors also began experimenting with adding additional extortion demands, often referred to as “double extortion.” Criminals now sometimes demand two separate ransom payments, the first to unlock a frozen computer network, and then a second to prevent the public disclosure of stolen information. Some are even extending this practice to “triple-extortion,” adding denial-of-service attacks to further pressure victims of these extortion schemes.

Addressing the Ransomware Challenge

There are no easy answers to the ransomware challenge we face today. But it is abundantly clear that this fight will require a whole-of-government, and indeed a whole-of-society, approach. Cooperation and collaboration are and will remain vital.

Information Sharing and Timely Incident Reporting

As a starting point, there is a clear need for enhanced coordination between the government and industry, particularly as it relates to information sharing and incident reporting. This is an area where there has been notable progress in recent years, in no small part due to the passage of the Cybersecurity Information Sharing Act of 2015 (CISA 2015), which offered certain liability protections to companies that share threat information with the U.S. Government.

But, CISA 2015 should be viewed as just a foundation. The U.S. Government needs access to timely, actionable information. If victim companies fail to report ransomware attacks early, or if they fail to report them at all, it hinders law enforcement’s ability to assist them with asset recovery or to prevent future incidents.

Accordingly, it remains worth considering whether there may be opportunities to establish additional incentives and/or requirements to strengthen this reporting process. Determining the exact contours of such programs will take time. However, the current status quo, in which firms have limited motivation to work with the government, may prove unsustainable in the long term.

Organizational Defenses, Cyber Hygiene, and Enterprise Network Security

But information sharing and reporting is just part of the puzzle. It is something we have been saying for years, but it is worth restating: every organization, big or small, public or private, must implement basic cybersecurity hygiene and best practices. Even simple steps – such as keeping operating systems, software, and applications up-to-date and patched, or making sure that anti-virus and anti-malware solutions automatically update and run regular scans can significantly raise an organization’s defensive posture. Organizations should be encouraged to configure their enterprise networks to defend against, or at least mitigate, some of the worst harms of these attacks.

While many larger organizations have been able to design their systems effectively in this regard, many smaller and less well-resourced organizations have not been so well prepared and have suffered as a result. I’d like to commend the Cybersecurity and Infrastructure Security Agency (CISA) and our partners throughout the Department of Homeland Security (DHS) for their efforts in this regard. Specifically, the

DHS “Ransomware Sprint”⁹ provided essential advocacy and support within DHS on these issues, and CISA’s “Stop Ransomware” campaign¹⁰ has been instrumental in providing guidance to industry to strengthen their own defenses and to effectively communicate with U.S. law enforcement. I believe more needs to be done along these lines to ensure that all U.S. organizations have the information needed to build resilient systems that can withstand a sophisticated ransomware attack.

Cyber Insurance

The insurance industry will likely play a key role in both enhancing incident reporting and raising organizational defenses. Cyber insurance is becoming a crucial element in response to a range of cybersecurity incidents, including ransomware attacks. The insurance sector and federal government can and must work collaboratively to encourage cyber insurance policyholders to improve security and avoid the hazard of financing the growth of transnational cybercrime.

Public and private sector stakeholders have a shared interest in a vibrant cyber insurance market that facilitates both cyber risk reduction and action to advance our Nation’s cybersecurity. Sharing timely incident information with the government is critically important, as it facilitates the availability of federal response support (including, as appropriate, cybersecurity and law enforcement resources) to the impacted entity. It also enables the government to issue warnings and indicators to other potential victims. We continue to examine how we can best engage with the cybersecurity insurance industry.

Domestic and International Partnerships

Catching cybercriminals is a team sport, and partnerships form the bedrock of all of the Secret Service’s investigative work. Specifically, within the Executive Branch, we work hand-in-hand with the Department of Justice (e.g., the Federal Bureau of Investigation, the Office of International Affairs, U.S. Attorney’s Offices, and the Computer Crime and Intellectual Property Section), the Department of State (e.g., the Bureau for International Narcotics and Law Enforcement Affairs), and the Department of Treasury (e.g., the Financial Crimes Enforcement Network and the Office of Foreign Assets Control). We coordinate and deconflict our ransomware cases through the National Cyber Investigations Joint Task Force (NCIJTF), where we lead the Criminal Mission Center.

Within our own Department of Homeland Security, we closely partner with CISA to share cybersecurity alerts and best practices, and conduct joint criminal investigations with Immigration and Customs Enforcement (ICE) - Homeland Security Investigations. We also work with State, Local, Tribal, and Territorial (SLTT) partners to assist them with their local investigations, in addition to a variety of private sector and non-government groups, such as the National Cyber-Forensics and Training Alliance (NCFATA) and Ransomware Task Force (RTF).

Our foreign partners perform critical roles in assisting U.S. law enforcement with conducting investigations, making arrests, and seizing criminal assets.

Fostering overseas partnerships helps to develop a shared understanding of risks, to ensure timely legal assistance, and to support effective international anti-money laundering (AML) regulatory and enforcement programs. The Secret Service has been highly successful at partnering with other countries

⁹ See, “Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience,” <https://www.dhs.gov/news/2021/03/31/secretary-mayorkas-outlines-his-vision-cybersecurity-resilience>.

¹⁰ See, “Stop Ransomware,” <https://www.cisa.gov/stopransomware>.

on these issues, working collaboratively to arrest transnational cyber criminals when they travel. We at the Secret Service continue to build the relationships necessary for effective enforcement operations.

Focusing on Financial Transactions

As noted above, cryptocurrency is often used to facilitate cybercrime, allowing for instant, pseudo-anonymous extortion payments and money laundering operations. But cryptocurrencies have their limitations. To be utilized within the mainstream economy – namely, to exchange them for most goods or services – cryptocurrencies must generally be converted into government-backed fiat currency, such as the U.S. dollar, European Euro, or Chinese Yuan. This conversion typically occurs through “exchanges,” financial services which allow for the purchase and sale of digital assets with fiat currency.

Exchanges have been particularly effective control points for governments to focus their efforts, both as on-ramps and off-ramps to the cryptocurrency economy. However, as the variety of digital assets increases, further attention is needed to address the risks of services that obscure digital transactions from law enforcement and regulatory oversight. Ransomware actors and those that support them persistently seek to avoid U.S. and foreign AML and know-your-customer (KYC) requirements by using exchanges that do not adhere to these laws or reporting requirements. Criminals are also increasingly exploiting over-the-counter (OTC) brokers, which facilitate transactions conducted directly between two parties through bilateral contracts.

Accordingly, it is vital that AML and KYC laws achieve their intended effects, regardless of the bad actor’s motivations for exploiting them. The enactment of the Anti-Money Laundering Act of 2020 (AML 2020) was an important step in this direction. However, enhanced data reporting, collection, retention, and accessibility requirements may strengthen criminal investigations and effective oversight.

Workforce Development

Finally, combatting ransomware requires highly skilled criminal investigators. Hiring, developing, retaining, and equipping our investigative workforce is absolutely essential, as are programs to train our domestic and foreign law enforcement partners to develop their own investigative capabilities. This can be achieved by strengthening law enforcement training and capacity building programs that equip Federal law enforcement, and our partners, with the technical skills and tools necessary to pursue the most sophisticated transnational criminals.

Conclusion

It does us no service to sugarcoat the reality of today’s situation: the cybercriminals are emboldened and getting stronger. Ransomware is menacing our economy and our institutions. Cybercriminals are using ransomware to make more money and do more harm ever before.

Progress is possible, as the success of the Secret Service and our partners has demonstrated, but it will take a continued commitment to make it clear that such purely criminal and destructive activities are unacceptable. I’m grateful for the support of Congress and our many partners, at home and abroad, for joining us in saying, “enough is enough.”

Thank you again for your continued support for the mission of the U.S. Secret Service, and your work on these important issues. I look forward to working closely with this Committee, and with other Members of Congress, on our shared priorities.



Department of Justice

STATEMENT OF

BRYAN A. VORNDRAN
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

“AMERICA UNDER CYBER SIEGE:
PREVENTING AND RESPONDING TO RANSOMWARE ATTACKS”

PRESENTED

JULY 27, 2021

**STATEMENT OF
BRYAN A. VORNDRAN
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE**

**BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE**

AT A HEARING ENTITLED

**“AMERICA UNDER CYBER SIEGE:
PREVENTING AND RESPONDING TO RANSOMWARE ATTACKS”**

**PRESENTED
JULY 27, 2021**

Chairman Durbin, Ranking Member Grassley, and Members of the Committee, thank you for the invitation to provide remarks on the FBI's role in our nation's fight against ransomware.

Ransomware is a growing threat to the health and safety of the American people and our national and economic security, with the Kaseya incident being the most recent example of ransomware's wide-ranging effects. I am honored to lead the men and women of the FBI's cyber program, where we are using our unique authorities to impose risk and consequences on the malicious cyber actors who are committing these crimes. But we cannot go at it alone, and as you will hear today, our strategy involves not only our partners in the federal government but also those in the private sector and abroad.

The individuals who conduct cyber intrusions and ransomware campaigns, and the officials who direct or harbor them, believe they can compromise U.S. networks, steal our financial and intellectual property, and hold our critical infrastructure hostage for ransom, all without incurring risk themselves.

The FBI sits at the convergence of U.S. government efforts to change this risk calculus. As a member of both the law enforcement and intelligence communities, with domestic and international reach, the FBI is focusing our unique authorities, and our ability to engage with international law enforcement, domestic victims, and key technology service providers, to identify and disrupt adversaries **before** they compromise U.S. networks, and hold them accountable when they do.

Key to the FBI's strategy is using the information and insight we develop through our investigations to support our full range of public and private sector partners. There are many countries, companies, and agencies who play roles in defending networks, sanctioning destabilizing behavior, collecting cyber threat intelligence, and conducting cyber effects

operations. We seek to work with all of them, in the belief that our collective actions to combat cyber threats are most impactful when they are planned jointly and sequenced for maximum impact.

In coordination with our partners, the FBI has successfully disrupted numerous cybercriminal enterprises, including those deploying ransomware, but lasting impact will require joint, sequenced operations with our U.S. counterparts and foreign allies as well as a removal of sense of impunity many of these actors currently feel.

What is Ransomware?

At its most basic, ransomware is a computer program created by malicious actors to 1) infect a computer or server, 2) encrypt its contents so they cannot be accessed or used, and 3) allow the malicious actors to demand that a ransom be paid in exchange for the decryption key. Victim organizations without effective backups are not able to operate until their data is restored. Ransomware can paralyze organizations, and the cost to rebuild an encrypted network can be catastrophic for small- and medium-sized businesses and municipalities.

The ransomware threat is not new, and it has been one of the FBI's top priorities for cybercriminal investigations for some time. In 2018, for example, we eliminated the threat from a highly impactful ransomware variant called SamSam that infected victims in nearly every U.S. state, including the city of Atlanta, the Port of San Diego, and multiple major healthcare companies. Our investigation led to a November 2018 indictment of the responsible Iranian cybercriminals and sanctions against two digital currency exchanges that enabled their operations; this ransomware variant has not been seen since.

In a trend not unique to cybercrime, as we expand our capability to disrupt ransomware actors, criminals have adapted to increase the scale, impact, and prevalence of ransomware attacks. The increasingly sophisticated and targeted nature of ransomware campaigns has significantly increased their impacts on U.S. businesses, and ransom demands are growing larger. Simultaneously, "ransomware-as-a-service" (RaaS), in which a developer sells or leases the ransomware tools to their criminal customers, has decreased the barrier to entry and technological savvy needed to carry out and benefit from these compromises and increased the number of criminals conducting ransomware campaigns. As this has happened, the number of ransomware variants has grown; today, we have investigations into more than 100 variants, many of which have been used in multiple ransomware campaigns. Recently, we have seen "double extortion" ransomware – where actors encrypt, steal, and threaten to leak or sell victims' data – emerge as a leading tactic for cybercriminals, raising the stakes for victims, which in turn has increased the likelihood of ransom payments being made. While cybercriminals remain opportunistic, they have also become more targeted in their campaigns, purposely aiming their malware at those institutions which can least afford downtime – specifically infrastructure critical to public safety, including hospitals and emergency services.

These ransom payments are typically requested in the form of a virtual currency, like Bitcoin. Virtual currency is not governed by a central authority, and regulation of the industry is still evolving globally, which can make it difficult to find out who is behind a transaction.

Cryptocurrency can be moved anywhere in the world, often more quickly than traditional currency, and these transactions frequently take place on the dark web, which presents its own set of problems. While these ransom demands often used to be just a few hundred dollars, we now see American businesses targeted with ransom demands in the millions, and in some cases tens of millions, of dollars. The statistics paint a stark picture: in 2020, the FBI's Internet Crime Complaint Center (IC3) statistics showed a 20 percent increase in reported ransomware incidents and a 225 percent increase in ransom amounts. Unfortunately, what is reported is only a fraction of the incidents out there.¹

We have also seen both nation-state adversaries and cybercriminals targeting managed service providers (MSPs), where by infecting one system, they can access the networks of hundreds of potential victims – as we saw in the recent Kaseya incident. But we are working to bring awareness to this method of compromise. Last month, our partners at the U.S. Secret Service (USSS) put together a cyber incident response simulation for companies that use MSPs, and it was my pleasure to join the Secret Service and give a unified federal message on the importance of hardening their systems and engaging with law enforcement before they are victims of an attack.

Ransomware has become one of the most costly and destructive threats to businesses and governments. On top of this, throughout the COVID-19 pandemic, we saw callous opportunism by criminal groups who put public safety at risk by attacking health care providers during a global pandemic. These groups demonstrate no morality; they will target entities big and small, public and private, and show little care for how their actions affect vulnerable populations.

How the FBI's Cyber Strategy Counters the Ransomware Threat

Because this criminal activity has become more lucrative and enticing, it is our job to make it harder and more painful for hackers to do what they are doing. That is why we announced a new FBI cyber strategy last year, using our role as the lead federal agency with law enforcement and intelligence responsibilities to not only pursue our own actions, but to work seamlessly with our domestic and international partners to defend their networks, attribute malicious activity, sanction bad behavior, and take the fight to our adversaries overseas. We must impose risk and consequences on cyber adversaries and use our unique law enforcement and intelligence capabilities and authorities to do so through joint operations sequenced appropriately for maximum impact. We have to target the entire criminal ecosystem – including malware developers, money launderers, and shady infrastructure providers – and work with agencies like the Cybersecurity and Infrastructure Security Agency (CISA), victims, and cybersecurity firms. All the while, we must continue to team with the Department of State to ensure our foreign partners are able and willing to cooperate in our efforts to bring the perpetrators of cybercrime to justice.

¹ In 2019, the IC3 received 2,047 ransomware complaints with adjusted losses of more than \$8.9 million, though that is likely a small fraction of the true scope of the threat because it captures only those who individually reported to the IC3. These numbers represent a nearly 40 percent increase in ransomware complaints to the IC3, and more than double the adjusted losses reported in 2018. In 2020, the IC3 received 2,474 complaints identified as ransomware with adjusted losses of over \$29.1 million.

More specifically, and in conjunction with the Department of Justice's recently-formed Ransomware and Digital Extortion Task Force, our strategy for countering ransomware and other complex cybercriminal schemes is focused on pursuing and disrupting 1) the actors, 2) their infrastructure, and 3) their money – all while providing help to victims and actionable intelligence to warn potential future victims. When pursuing these actors, we work with like-minded countries to identify those responsible for damaging ransomware schemes, arrest them, and extradite them to the United States to face justice whenever possible. At the same time, taking down cybercriminals' technical infrastructure adds to the impact, as it raises their costs, disrupts their operations, prevents new victims, and often gives us new intelligence on their operations. Lastly, since virtual currencies are so central to ransomware, we have developed our ability to trace these transactions and have been able to seize funds and shut down illicit currency exchanges in some instances. We were recently able to accomplish this objective in the Colonial Pipeline case, when the victim and our federal partners worked quickly and closely with us to recover a substantial portion of the cryptocurrency paid as ransom.

We do all this with victims at the center of our efforts. At the FBI, we aim to inform, support, and assist victims in navigating the aftermath of crime and the criminal justice process with dignity and resilience. We want to empower all victims of cyber intrusions, just as we do for victims of other crimes. In some instances, we have done this by developing or acquiring a ransomware's decryption key to help victims recover without paying the ransom. We have also, on occasion, been able to give advance warning to vulnerable or targeted entities. While the FBI is not a remediation service, the work we do to investigate and respond to cybercrime enables us to collect information, which we share to prevent future attacks and use to assist victims if they have already been hit.

As I mentioned, we have certain unique investigative authorities. Using our authorities, through our investigations, we are able to collect information that enables disruptions, which are most impactful when they include coordinated actions by us, our domestic partners like the Department of the Treasury and U.S. Cyber Command, and our foreign partners. As an example, the FBI is leading a whole-of-government counter-ransomware campaign coordinated through the National Cyber Investigative Joint Task Force (NCIJTF), which includes the U.S. Intelligence Community (USIC) and law enforcement partners from across the federal government. As an initial step in the campaign, the FBI partnered with the National Cyber Forensics and Training Alliance (NCFTA) to host its first annual ransomware summit in September 2019, which brought together the USIC, federal law enforcement agencies, and private sector partners with expertise in ransomware, cybersecurity, and cyber incident response to work on possible solutions to the ransomware problem.

Our strategy has enabled us to land some major blows against the threat actors behind ransomware and its delivery mechanisms. In addition to imposing these consequences against our adversaries, we shared the information from our investigations, intelligence collection, and incident response with foreign partners, others in the USIC, and agencies with a role in cybersecurity. And we worked especially closely with CISA to share information with critical infrastructure owners and operators via FBI reports and joint advisories. The ransomware threat

is not going away, so we must carry this strategy and its momentum forward through the rest of 2021 and into 2022.

Addressing Ransomware's Global Footprint

As I mentioned earlier, without strong foreign partnerships, our cyber strategy cannot be fully implemented and we cannot successfully counter the ransomware threat.

We know our most significant threats come from foreign actors using global infrastructure to compromise U.S. networks. By working with friendly foreign law enforcement agencies and intelligence partners, we make it harder for these actors to conceal their activities and their whereabouts.

Not every foreign nation helps us in this fight. While we seek to disrupt entire cybercriminal enterprises, the most impactful consequence we can impose on a malicious cyber actor is an arrest as part of comprehensive disruption. If an actor is in a country like Russia or China, an arrest is currently not a viable option. Even when an indicted cybercriminal is in another country, Russia in particular takes actions to interfere with our extraditions. To make things more difficult, the lines between nation-states and cybercriminal actors are blurred, and even though a foreign nation may not be directing a ransomware campaign, it may still be complicit by providing a safe haven to those malicious actors who are doing harm to the United States, our citizens, and our businesses.

But our allies outnumber our foes, and in just the past few months, our work with foreign partners – supported by our legal attaches overseas – has led to impactful consequences against cybercriminals and sent a strong message that the reach of the U.S. government extends beyond its borders.

In January 2021, the FBI and others at the Department of Justice (DOJ) partnered with law enforcement and judicial authorities in the Netherlands, Germany, the United Kingdom, France, Lithuania, Canada, and Ukraine, with international activity coordinated by Europol and Eurojust, to disrupt the infrastructure of a highly destructive malware known as Emotet. Among other things, Emotet could also be used as a way to spread ransomware. This was one of the longest-standing professional cybercrime tools and had enabled criminals to cause hundreds of millions of dollars in damage to government, educational, and corporate networks. In this case, we used sophisticated techniques and our unique legal authorities, but it could never have happened without our international partners.

Also this January, we worked with international partners in Canada and Bulgaria to disrupt NetWalker, a ransomware variant that affected numerous victims, including companies, municipalities, hospitals, law enforcement, emergency services, school districts, colleges, and universities. In this case, we obtained federal charges, and a subject was arrested in Canada pending extradition proceedings. In addition, we seized more than \$450,000 in cryptocurrency.

Last month, through coordination with law enforcement and judicial authorities in The Netherlands, Germany, the United Kingdom, Canada, Sweden, Italy, Bulgaria, and Switzerland, we seized the web domains and server infrastructure of DoubleVPN, a virtual private network

that allowed ransomware actors to attack their victims and hide their tracks. Thanks to this international operation, this service, which was heavily advertised on both Russian and English-speaking cybercrime forums, is no longer available to cybercriminals.

How Victims and Potential Victims Can Help Themselves and Others

We have the strategy to take action against our cyber adversaries. But the strategy will fail if we do not know about suspicious activity or that a compromise has occurred. And because of the nature of U.S. laws and network infrastructure, we will never know about most malicious activity if it is not reported to us by the private sector.

We know ransomware victims, particularly large enterprises, risk negative publicity if they disclose being impacted by ransomware. As a result, ransomware incidents are often addressed by the victim directly and are never reported to the public or law enforcement. Ransomware incidents targeting public entities, such as state or local municipalities, often receive high levels of publicity. In addition to the losses reported to the IC3 I mentioned earlier, these groups face costs associated with business disruption and remediation, which can eclipse the ransom demand itself. For example, these costs were \$17 million and \$18.2 million, respectively, in ransomware campaigns against Atlanta and Baltimore.

I would like to spend a moment on the decision of whether or not to make a ransom payment. The FBI discourages ransomware victims from paying ransom for a variety of reasons. Even if a ransom is paid, there is no guarantee the business or individual will regain access to their data. On top of this, paying a ransom does not always keep data from ultimately being leaked. Additionally, paying a ransom incentivizes future ransomware attacks and emboldens criminal actors to continue their illicit work. However, **regardless of whether or not a victim chooses to pay, the FBI strongly encourages victims to report ransomware incidents to the FBI.** Our goal is to identify, pursue, and impose consequences on criminal actors, not their victims.

We are pushing important threat information to network defenders, and we are making it as easy as possible for the private sector to share information with us. For example, we are emphasizing to the private sector how we keep our presence unobtrusive in the wake of a breach, how we protect information that companies and universities share with us and commit to providing useful feedback, and how we coordinate with our government partners so we speak with one voice. A call to one federal agency is a call to all federal agencies, and I hope we are sending that message by sitting as a unified front here today.

At the same time, we need the private sector to do its part. We need to be warned – quickly – when they see malicious cyber activity. We also need companies to work with us when we warn them they are being targeted. The recent examples of significant cyber incidents – SolarWinds, Microsoft Exchange, Colonial Pipeline, JBS, and Kaseya – only emphasize what Director Wray has been saying for a long time: The government cannot protect against cyber threats on its own. We need a whole-of-society approach that matches the scope of the danger. There is really no other option for defending a country where nearly all of our critical infrastructure, personal data, intellectual property, and network infrastructure sit in private hands.

So what specific steps can companies take to follow our guidance, protect themselves and our nation, and help themselves if ransomware strikes?

First, the public, cybersecurity professionals and system administrators, and business leaders can use threat information shared by the FBI and the rest of the federal government to strengthen their network defenses and guard against ransomware and other malicious cyber activity. Our reports, which are coordinated with our federal partners, are shared directly with critical infrastructure owners and operators, and when possible are posted to our IC3 website to warn the public about the trends we are seeing and the specific threats out there. In addition to these threat advisories, CISA's website and the new interagency site www.StopRansomware.gov have resources on how people and businesses can protect themselves. Some of the general cybersecurity practices we encourage include creating and securing offline backups of critical data, installing patches as soon as they become available, updating anti-virus software, connecting only to secure networks, employing multi-factor authentication, and ensuring the validity of all emails and the links they contain before clicking them.

Second, if you are an organization, create an incident response plan. If you are compromised, you need to know what to do. All of your leaders and security professionals need to be on the same page, and you must be able to make decisions quickly. Having worked with victims who had incident response plans versus those who did not, the difference is stark. Victims with incident response plans are often able to respond faster and more efficiently and can significantly limit the damage caused by a ransomware incident.

Third, organizations should build relationships with their local FBI field offices. Whether you are a small organization or a large corporation, our local offices welcome making connections before anything has gone wrong. If you see us speaking at an event in your area, show up, and talk to us after – we would be thrilled to meet your CEO, chief information security officer (CISO), general counsel, or anyone who has a role in keeping your networks secure and incident response. But it cannot stop there. Continue to share information with us after that meeting, and you have my word we will do the same back to you.

Fourth, if you are compromised, or if you think you may have been, report it to us as quickly as you can. You can report these incidents via the Internet Crime Complaint Center at www.IC3.gov or by contacting your local FBI field office – hopefully to the FBI agent you already know. We will take it from there and make sure the wheels of the entire federal government incident response team are set into motion so you can focus on remediation.

If an incident occurs, it may not be too late, but time is of the essence. The difference between seeking help on day one and day five is real – it can be the difference between a company reconstituting its network or declaring bankruptcy. We will always use our full range of national security authorities and criminal legal processes to investigate ransomware incidents, but many of those techniques require probable cause and prior court authorization, so there is no substitute for quick, voluntary action by private owners of U.S. networks and infrastructure in helping us act rapidly against a threat. Swift action from the private sector is an enormous public service, and we truly appreciate private sector cooperation whenever we can get it. In the

Colonial Pipeline and Kaseya incidents, for example, swift reporting and response contained the impact of what could have been significantly worse events.

Mandatory Reporting of Ransomware and Other Cyber Incidents

Because far too many ransomware incidents go unreported, and because silence benefits ransomware actors the most, we wholeheartedly believe a federal standard is needed to mandate the reporting of certain cyber incidents, including most ransomware incidents. Unlike other types of cybercrimes, the victim will almost always know when a ransomware incident has occurred. The scope and severity of this threat has reached the point where we can no longer rely on voluntary reports alone to learn about incidents. We support a nationwide standard that establishes which ransomware incidents must be disclosed, when and to whom they must be reported, and what those reports must include.

Mandatory ransomware incident reporting alone will not defeat the ransomware threat. However, it is a crucial step on that path for a number of reasons, and there are five in particular I would like to highlight. First, it will enhance the federal government's view of the threat and allow us to understand the full extent of ransomware activity nationwide. Second, this level of visibility will enhance cybersecurity efforts by informing cybersecurity advisories used to warn the public about incident trends and ransomware actors' specific tactics, techniques, and procedures. This in turn helps the public take appropriate steps to defend their networks. Having a better grasp of these trends and the specifics about individual incidents behind them will help the FBI organize strategic engagement with entities and industries that are experiencing the greatest harm. Third, it will assist incident response efforts so federal incident response agencies can provide support to a greater number of victims and collect evidence to open and advance cases. Fourth, having greater transparency into nationwide ransomware activity will help the FBI connect seemingly unrelated incidents to common actors so we can investigate the full extent of their activity and work to hold them accountable for all of their crimes. Fifth, reporting of ransom demands, payments, and details about those payments allows the FBI to "follow the money" to investigate where these payments are going and to whom, with the ultimate goal of seizing those funds.

One of the most important things Congress can do to assist the U.S. government's fight against ransomware is to pass a national cyber incident reporting standard. We believe the status quo is untenable, and to make significant progress against this threat, we need transparency into the full scope of the threat and the damage it is causing. Cybersecurity is national security. Simply put, if ransomware victims do not report these incidents, we cannot have cybersecurity, and we cannot have national security. Mandatory reporting legislation would take us a giant step toward protecting both.

The Resource Demands of Malicious Cyber Activity

When we do learn of a ransomware incident, our agents are in direct contact with victims and with private industry partners to share threat indicators—such as malicious IP addresses—and gather evidence that helps us identify who is compromised and who else is vulnerable. Our technically trained incident response assets throughout the country, collectively known as our

Cyber Action Team (CAT), assist affected entities. Our field offices with experience in complex national security and cyber investigations are our hubs for triaging the data we acquire through legal process, from partners, and through other lawful means. And our digital forensics and intelligence personnel exploit that information for indicators and intelligence that will help us to attribute the malicious activity to those responsible.

With the growing frequency and scale of recent significant cyber incidents – in some cases involving tens of thousands of victims – we are increasingly faced with hard choices that carry risk, include moving personnel away from long-term investigations or other significant incidents so we can surge toward the immediate need. In our SolarWinds investigation alone, a single FBI field office collected more than 170 terabytes of data – about 17 times the content of the entire Library of Congress. The FBI continues to exploit and analyze intelligence and technical data to uncover adversary tactics, share our findings, and pursue actions that will prevent those responsible from striking again.

Recent ransomware campaigns have shown us the investments in time, money, and talent cybercriminals are willing to make to compromise our networks. Accordingly, it requires a teams-based approach among various departments and agencies to understand, defend against, and counter these malicious cyber actors. Congress can help us by providing the resources requested in the President's 2022 Budget request to ensure the FBI and our partners are resourced to play our respective parts as we defend the nation together.

Conclusion

Even more than the other criminal violations we investigate, the FBI depends on our partners – public and private, foreign and domestic – to help us keep Americans safe from the many threats posed by ransomware. As part of our strategy, we have been putting a lot of energy and resources into cultivating these partnerships. As Director Wray has put it, cyber is the ultimate team sport, and I truly believe our partners are seeing the benefits of having FBI Cyber on their team.

Chairman Durbin, Ranking Member Grassley, and members of the Committee, thank you for the opportunity to testify today. I am happy to answer any questions you might have and to work together with you in the nation's fight against ransomware so the FBI can help achieve our collective cyber mission – to give the American people safety, security, and confidence in our digitally connected world.

**Questions for the Record from Senator Charles E. Grassley
Hearing on “America Under Cyber Siege: Preventing and Responding to Ransomware
Attacks”
July 27, 2021**

Bryan A. Vorndran
Assistant Director, Cyber Division
Federal Bureau of Investigation
Washington, D.C.

1. What do you see as our options to best deter and punish state-affiliated ransomware attacks?
2. What are the biggest challenges you face in investigating ransomware as a service providers?
3. In the hearing you mentioned that the FBI had no interest in investigating or prosecuting victims of ransomware. I appreciate your clarity. Do you know whether the FBI, DOJ, or any other government body intends to issue any formal guidance on this issue?
4. How would an extorted business or government go about finding a qualified ransomware negotiator? What value do such individuals bring to ransomware events?
5. Has the FBI considered a public education campaign to warn potential victims of the dangers of paying ransomware, including “double extortion”?
6. How do FBI, USSS, and CISA coordinate among agencies to ensure efforts are not duplicated?
7. If victims of ransomware contact either the FBI or USSS, are they given the same or similar guidance? Has federal law enforcement coordinated how reported incidents are investigated? What is the procedure that FBI and USSS use to de-conflict cases?

Questions for the Record from Senator Ben Sasse
SJC Hearing: “America Under Cyber Siege: Preventing and Responding to Ransomware
Attacks.”
July 27, 2021

Questions for All Witnesses: Richard Downing (DOJ), Bryan Vorndran (FBI), Eric Goldstein (CISA), and Jeremy Sheridan (USSS)

1. Given the growing frequency of high-profile ransomware attacks and given that the main prohibition on ransomware payments only relates to payments made to OFAC designated entities, why are we not seeing more sanctions on these variants?
 - a) To what extent have each of your agencies observed a change in the character, makeup, and activity of any ransomware variants that have previously been designated by OFAC?
 - b) Should public attribution inherently lead to OFAC designations?
 - c) Please describe the law enforcement challenges associated with bringing these variants to justice without sanctions.
2. How do each of your respective agencies think about deterring actors in this space?
 - a) What have you found to be the most valuable tools to deter average cybercriminals and ransomware variants from launching attacks?
 - b) Where are the most prominent limits to deterrence theory in practice?
3. How would you describe the role of the ransomware insurance market in combatting the growing ransomware issue? Is the insurance market more helpful or harmful to the ultimate goal of reducing ransomware attacks?
 - a) Are companies with ransomware insurance more likely to pay a ransom than those without insurance?
 - b) Is there any evidence to suggest that hackers are more likely to target companies that have ransomware insurance?
4. According to the blockchain research firm Chainalysis, ransomware payments reached a total of \$412 million during 2020, representing a 341 percent increase over the prior year. How is the ransomware insurance market responding to this growing number of attacks?
 - a) Are insurance companies requiring their customers to maintain any baseline security or preventative measures in order to qualify for coverage?
 - b) Outside of advising on “best practices,” is there anything else the government can, or should, be doing to fortify our resilience against ransom attacks through the insurance industry?
5. Who is currently responsible for regulations relating to the ransomware insurance industry?
 - a) At present, are insurance companies required to report to the government ransom attacks against their customers for whom they make payments? If not, is there any reason why they should not be required to do so?

Questions for the Record from Senator Ben Sasse
SJC Hearing: “America Under Cyber Siege: Preventing and Responding to Ransomware
Attacks.”
July 27, 2021

Questions for All Witnesses: Richard Downing (DOJ), Bryan Vorndran (FBI), Eric Goldstein (CISA), and Jeremy Sheridan (USSS)

1. Given the growing frequency of high-profile ransomware attacks and given that the main prohibition on ransomware payments only relates to payments made to OFAC designated entities, why are we not seeing more sanctions on these variants?
 - a) To what extent have each of your agencies observed a change in the character, makeup, and activity of any ransomware variants that have previously been designated by OFAC?
 - b) Should public attribution inherently lead to OFAC designations?
 - c) Please describe the law enforcement challenges associated with bringing these variants to justice without sanctions.

2. How do each of your respective agencies think about deterring actors in this space?
 - a) What have you found to be the most valuable tools to deter average cybercriminals and ransomware variants from launching attacks?
 - b) Where are the most prominent limits to deterrence theory in practice?

3. How would you describe the role of the ransomware insurance market in combatting the growing ransomware issue? Is the insurance market more helpful or harmful to the ultimate goal of reducing ransomware attacks?
 - a) Are companies with ransomware insurance more likely to pay a ransom than those without insurance?
 - b) Is there any evidence to suggest that hackers are more likely to target companies that have ransomware insurance?

4. According to the blockchain research firm Chainalysis, ransomware payments reached a total of \$412 million during 2020, representing a 341 percent increase over the prior year. How is the ransomware insurance market responding to this growing number of attacks?
 - a) Are insurance companies requiring their customers to maintain any baseline security or preventative measures in order to qualify for coverage?
 - b) Outside of advising on “best practices,” is there anything else the government can, or should, be doing to fortify our resilience against ransom attacks through the insurance industry?

5. Who is currently responsible for regulations relating to the ransomware insurance industry?
 - a) At present, are insurance companies required to report to the government ransom attacks against their customers for whom they make payments? If not, is there any reason why they should not be required to do so?

Questions for the Record from Senator Ben Sasse
SJC Hearing: “America Under Cyber Siege: Preventing and Responding to Ransomware
Attacks.”
July 27, 2021

Questions for All Witnesses: Richard Downing (DOJ), Bryan Vorndran (FBI), Eric Goldstein (CISA), and Jeremy Sheridan (USSS)

1. Given the growing frequency of high-profile ransomware attacks and given that the main prohibition on ransomware payments only relates to payments made to OFAC designated entities, why are we not seeing more sanctions on these variants?
 - a) To what extent have each of your agencies observed a change in the character, makeup, and activity of any ransomware variants that have previously been designated by OFAC?
 - b) Should public attribution inherently lead to OFAC designations?
 - c) Please describe the law enforcement challenges associated with bringing these variants to justice without sanctions.

2. How do each of your respective agencies think about deterring actors in this space?
 - a) What have you found to be the most valuable tools to deter average cybercriminals and ransomware variants from launching attacks?
 - b) Where are the most prominent limits to deterrence theory in practice?

3. How would you describe the role of the ransomware insurance market in combatting the growing ransomware issue? Is the insurance market more helpful or harmful to the ultimate goal of reducing ransomware attacks?
 - a) Are companies with ransomware insurance more likely to pay a ransom than those without insurance?
 - b) Is there any evidence to suggest that hackers are more likely to target companies that have ransomware insurance?

4. According to the blockchain research firm Chainalysis, ransomware payments reached a total of \$412 million during 2020, representing a 341 percent increase over the prior year. How is the ransomware insurance market responding to this growing number of attacks?
 - a) Are insurance companies requiring their customers to maintain any baseline security or preventative measures in order to qualify for coverage?
 - b) Outside of advising on “best practices,” is there anything else the government can, or should, be doing to fortify our resilience against ransom attacks through the insurance industry?

5. Who is currently responsible for regulations relating to the ransomware insurance industry?
 - a) At present, are insurance companies required to report to the government ransom attacks against their customers for whom they make payments? If not, is there any reason why they should not be required to do so?

Questions for the Record from Senator Ben Sasse
SJC Hearing: “America Under Cyber Siege: Preventing and Responding to Ransomware
Attacks.”
July 27, 2021

Questions for Bryan A. Vorndran, Assistant Director, Cyber Division, Federal Bureau of Investigation and Richard Downing, Deputy Assistant Attorney General of the Criminal Division, Department of Justice

1. In written testimony the FBI noted that it is currently investigating more than 100 ransomware variants. Does this number represent the entirety of the known universe of ransomware variants today?
 - a) If not, what percentage does it represent?
 - b) What metrics do we use to judge each of these variants’ alignments with nation state actors?
 - c) How many variants are aligned with the Russian Federation, People’s Republic of China, Islamic Republic of Iran, and the Democratic People’s Republic of Korea? How many operate independent of these hostile nation states?
 - d) Please describe the challenges of effectively responding to ransomware attacks when ransomware variants are receiving de facto safe harbor in foreign jurisdictions.
2. Is there a substantive difference in types of assistance the FBI can offer to companies that have fallen victim to a ransomware attack depending on their practice of good cyber hygiene?
 - a) Are there certain practices, beyond prompt reporting, that position the FBI and DOJ to more effectively act to reclaim paid ransoms?

Questions for All Witnesses: Richard Downing (DOJ), Bryan Vorndran (FBI), Eric Goldstein (CISA), and Jeremy Sheridan (USSS)

1. Given the growing frequency of high-profile ransomware attacks and given that the main prohibition on ransomware payments only relates to payments made to OFAC designated entities, why are we not seeing more sanctions on these variants?
 - a) To what extent have each of your agencies observed a change in the character, makeup, and activity of any ransomware variants that have previously been designated by OFAC?
 - b) Should public attribution inherently lead to OFAC designations?
 - c) Please describe the law enforcement challenges associated with bringing these variants to justice without sanctions.
2. How do each of your respective agencies think about deterring actors in this space?
 - a) What have you found to be the most valuable tools to deter average cybercriminals and ransomware variants from launching attacks?
 - b) Where are the most prominent limits to deterrence theory in practice?

3. How would you describe the role of the ransomware insurance market in combatting the growing ransomware issue? Is the insurance market more helpful or harmful to the ultimate goal of reducing ransomware attacks?
 - a) Are companies with ransomware insurance more likely to pay a ransom than those without insurance?
 - b) Is there any evidence to suggest that hackers are more likely to target companies that have ransomware insurance?

4. According to the blockchain research firm Chainalysis, ransomware payments reached a total of \$412 million during 2020, representing a 341 percent increase over the prior year. How is the ransomware insurance market responding to this growing number of attacks?
 - a) Are insurance companies requiring their customers to maintain any baseline security or preventative measures in order to qualify for coverage?
 - b) Outside of advising on “best practices,” is there anything else the government can, or should, be doing to fortify our resilience against ransom attacks through the insurance industry?

5. Who is currently responsible for regulations relating to the ransomware insurance industry?
 - a) At present, are insurance companies required to report to the government ransom attacks against their customers for whom they make payments? If not, is there any reason why they should not be required to do so?

RICHARD W. DOWNING
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
U.S. DEPARTMENT OF JUSTICE
QUESTIONS FOR THE RECORD
FROM A HEARING ENTITLED
“AMERICA UNDER CYBER SIEGE:
PREVENTING AND RESPONDING TO RANSOMWARE ATTACKS”
BEFORE THE
SENATE COMMITTEE ON THE JUDICIARY
JULY 27, 2021

Questions from Senator Tillis:

- 1. Your written testimony annexed proposed language for a draft “Cybercrime Mitigation Act.” It tracks two sections of the International Cybercrime Prevention Act, S.2139, a bipartisan bill that I co-sponsored with Senators Whitehouse, Graham, and Blumenthal. However, certain provisions were omitted. For example, the proposed Cybercrime Mitigation Act does not create increased penalties for those who damage critical infrastructure computers and does not connect felonious computer fraud and abuse to racketeering activities. Please explain why provisions that were part of the Cybercrime Prevention Act were not included in the proposal, and specifically address why provisions specifically addressing critical infrastructure would not be helpful.**

RESPONSE: The Department of Justice supports the efforts to update the Racketeering Influenced and Corrupt Organizations Act (“RICO”) by making Computer Fraud and Abuse Act (“CFAA”) offenses and certain Wiretap Act offenses subject to RICO. As computer technology has evolved, it has become a key tool of organized crime. And just as RICO has proven to be an effective tool to prosecute traditional organized crime, it should also be a tool to fight criminal organizations that use computer intrusions and other CFAA violations to further their schemes. These changes, as proposed in the International Cybercrime Prevention Act (“ICPA”), would make clear that all types of CFAA violations should be considered criminal predicates under the RICO statute, with the associated heavy penalties.

The Department of Justice also supports the efforts in ICPA to strengthen the criminal code to better protect our critical infrastructure, by enhancing the penalties that apply to intrusions and attacks affecting the computers that run our critical infrastructure. In light of the grave risk posed by those offenses, the Department believes that enhanced penalties not only appropriately punish offenders, but also will more effectively deter others who would engage in misconduct that puts public safety and national security at risk.

2. **We have heard that combatting ransomware threats requires a whole-of-government and whole-of-society approach. What must be done to improve coordination among the many actors that play a role in combatting ransomware attacks, stopping future attacks, and bringing the bad actors to justice, and what should Congress do to help?**

RESPONSE: The White House is leading the nation’s response to combatting ransomware, ensuring the whole-of-government uses the best tools each department and agency has to improve prevention, detection, disruption, and resiliency. The Department of Justice’s key federal partners are the Department of Homeland Security, including the U.S. Secret Service and the Cybersecurity and Infrastructure Security Agency (“CISA”); the Department of the Treasury, including the Office of Foreign Assets Control and the Financial Crimes Enforcement Network; the Department of Defense, including Cyber Command; the intelligence community; the Department of Commerce, and the Department of State. Our collaborative approach ensures that all of the U.S. government’s resources may be brought to bear to address the threat of ransomware in a systematic and comprehensive way—including through the potential use of economic sanctions, virtual currency regulations, diplomatic pressure, intelligence operations, and military action.

The Department is also increasing collaboration with our foreign partners to share information and coordinate efforts in combating ransomware. Because many of the actors responsible for these crimes and much of the infrastructure that facilitates these attacks are located overseas, close cooperation with our foreign partners has been and will continue to be crucial to successfully identify perpetrators, dismantle ransomware operations, and disrupt safe havens for malicious activity.

Congress should consider whether changes are needed in a few areas, including improving our ability to disrupt criminal activity and enhancing our ability to prosecute offenders and the effectiveness of such prosecution.

A. The Department of Justice uses the civil injunction process as a powerful tool to disrupt botnets and free victim computers from malware. The current law permits courts to consider injunctions only for certain crimes, including certain frauds and illegal wiretapping. Botnets, however, can be used for many different types of illegal activity, such as denial-of-service attacks or to install ransomware. Depending on the facts of any given case, these crimes may not constitute fraud or illegal wiretapping. The Department supports legislation to address this problem by granting courts the authority to enjoin a greater range of botnets and other cybercrime involving damage to 100 or more computers.

In addition, the statutes that prohibit the creation and use of botnets also have shortcomings because they do not clearly prohibit the sale or renting of a botnet. It should be illegal to sell or rent surreptitious control over infected computers to another person, just like it is already illegal to sell or transfer computer passwords. That is why the proposed legislation would prohibit the sale or transfer not only of “password[s] and similar information” (the wording of the existing statute) but also of “means of access,” which would include the ability to access computers that were previously hacked and are now part of a botnet.

B. Additionally, the Department of Justice recommends additional changes to the CFAA that would make the statute more effective in the fight against ransomware. Key amongst these proposals is an amendment to Section 1030 to bring the forfeiture provisions of the CFAA in line with other federal statutes. This would provide concrete authorities for the forfeiture of property used to commit or facilitate a violation of the CFAA.

In addition, the Department supports an amendment to the CFAA to add explicit language on penalties for the crime of conspiracy. Consistent with other federal criminal statutes and with the structure of the CFAA, a charge of conspiracy or attempt should explicitly specify the same penalty as the corresponding substantive offense under Section 1030.

- 3. Your written testimony notes that the reluctance to report ransomware incidents and payments made may be driven concerns “including a fear of regulatory action or reputational harm, or of an interruption to business operations.” What other reasons are there for the failure to voluntarily report? In recommending a mandatory reporting scheme, what assurances are you prepared to give those who report incidents to address these concerns, including harm to reputation, regulatory retaliation, or harms to intellectual property? How will the government safeguard data provided by companies to combat ransomware?**

RESPONSE: The reluctance of businesses to report ransomware and other cybersecurity incidents may be driven by multiple concerns. These include concerns that disclosure may lead to adverse regulatory action or civil liability; that disclosing information to the government may waive privilege or other legal protections in that information; that the government will be required to disclose proprietary or other sensitive information to the public under public disclosure laws; and that reporting may lead to reputational harms. These fears are often overstated, but businesses operating under a voluntary disclosure regime may default to taking a no-report approach. That unfortunately presents a major challenge to America’s ability to respond to ransomware and other cyber incidents. And the harm caused by businesses not disclosing incidents is borne not just by those businesses, but by future victims and others affected by an incident. The government can act only if it knows about an incident. The failure to report these crimes may mean that they never get investigated or that the government may lose valuable time and evidence critical both to identifying and warning other potential victims before more incidents occur, and to identifying, disrupting, and prosecuting the malicious actors responsible for these crimes.

- 4. In light of the recent hack of Cellebrite by Signal, and given that the DOJ depends significantly on Cellebrite tools for their investigations, we are very concerned that recent events have compromised the integrity of digital evidence and negatively impacted the chain of custody of current cases and investigations by the Department. Please provide us an update as to the current state of play regarding the impact of the hack and developments resulting from the hack and with any and all information regarding the steps the Department is taking to address this situation.**

RESPONSE: On April 21, 2021, the CEO of the Signal messaging service posted on Signal’s blog about alleged vulnerabilities in Cellebrite’s software. That post claimed that:

[I]t’s possible to execute arbitrary code on a Cellebrite machine simply by including a specially formatted but otherwise innocuous file in any app on a device that is subsequently plugged into Cellebrite and scanned. There are virtually no limits on the code that can be executed.

For example, by including a specially formatted but otherwise innocuous file in an app on a device that is then scanned by Cellebrite, it’s possible to execute code that modifies not just the Cellebrite report being created in that scan, but also all previous and future generated Cellebrite reports from all previously scanned devices and all future scanned devices in any arbitrary way (inserting or removing text, email, photos, contacts, files, or any other data), with no detectable timestamp changes or checksum failures. This could even be done at random, and would seriously call the data integrity of Cellebrite’s reports into question.

The blog post concluded with the claim that, entirely by coincidence, upcoming versions of Signal would be randomly inserting “aesthetically pleasing” files into some users’ installed Signal app, implying that Signal would deploy malware to exploit these alleged vulnerabilities.

The Department of Justice is aware of no evidence that Signal has in fact created and deployed such malware or that any Cellebrite reports have been corrupted. Some media outlets reported that Cellebrite pushed a software security update to its customers shortly after Signal’s blog post, but neither Cellebrite nor anyone else has confirmed that this alleged update had any connection to Signal’s claims.

Moreover, even if the alleged exploit exists, Signal’s only claim is that it can rewrite reports generated about a device examination, not that it can corrupt extracted data *per se*. It is standard procedure in forensics to do forensic work only on a copy of the extracted data image. Thus, even if Cellebrite reports were found to be unreliable—again, there is no factual basis for believing this to be true—that is irrelevant to the reliability of the files and other data extracted from a given device. Forensic agents can still validate data from the extracted data image.

We have confirmation of only one federal criminal case in which the defendant has moved for a new trial or to suppress evidence on the basis of Signal’s claims. See *United States v. Childress*, 2021 WL 2972868 (W.D. Va. July 14, 2021). In that case, the district court denied the defendant’s motion to suppress, finding that the defendant’s “general allegations regarding Cellebrite are lacking adequate support.” *Id.* at *4 n.3. As a result, Signal’s allegations have had no material impact on the Department’s ability to carry out its investigative and prosecutorial duties.

Owing to media reports published shortly after Signal’s blog post, we are also aware of one state defendant who moved for a new trial in West Virginia on the basis of Cellebrite’s alleged unreliability. See, e.g., “Lawyer seeks new trial based on alleged cybersecurity flaws in phone-cracking product,” <https://www.abajournal.com/news/article/lawyer-seeks-new-trial-based-on-alleged-cybersecurity-flaws-in-phone-cracking-product> (May 7, 2021). These reports identified

the defense attorney involved, but the case number and defendant's name were redacted. After a diligent search using the limited information available, the Department has found no judicial decisions addressing the motion or subsequent press reports on the case. A Twitter account purporting to belong to the defense lawyer in question tweeted about the initial filing on April 26 (<https://twitter.com/mtmdlwyer/status/1386733853298069505>), but does not appear to have issued any more recent statements about the motion.

5. What changes need to be made to the federal government or your Department's hiring practices to attract and retain top cybersecurity professionals?

RESPONSE: The Federal Government Cyber Mission resides in numerous federal agencies, to include the Department of Justice (DOJ). Therefore, DOJ needs to make use of streamlined hiring processes, without any unnecessary steps for candidates, to ensure recruitment of quality and skilled cyber-focused personnel. In addition, current and prospective DOJ cyber professionals, including policy and legal cyber specialists, need to receive competitive salaries and incentives based on their skills, expertise, and performance that are crucial for DOJ cyber mission delivery.

6. What percentage of data is encrypted at rest on federal and commercial systems? How can we incentivize system owners to further adopt secure storage solutions?

RESPONSE: The Department of Justice defers to CISA, the National Security Agency, and the Office of Management and Budget.

Questions from Senator Grassley:**1. What do you see as our options to best deter and punish state-affiliated ransomware attacks?**

RESPONSE: The United States has several options to disrupt and deter state-affiliated ransomware attacks, including through prosecution, technical operations, economic sanctions, and diplomatic efforts. A whole-of-government approach must be used, with careful consideration as to the response—or responses—most appropriate for each particular threat. For its part, the Department’s National Security Division (“NSD”) has worked with the U.S. Intelligence Community, the Department of Defense, the Department of Homeland Security, the Department of the Treasury, and the State Department to address state-sponsored cybercrime. NSD does so through a variety of means, including by bringing indictments against those responsible, by providing our partners with evidence and other threat intelligence gleaned from its investigations, providing legal and policy support, and through concurrent technical and other law enforcement operations.

2. Aside from mandating a national breach law, are there ways to incentivize more reporting?

RESPONSE: Though there are steps that could be taken to increase incentives to voluntarily report ransomware and other cyber incidents, we believe that experience has shown that mandatory reporting is warranted. Businesses have a range of reasons they cite for their reluctance to report incidents, including concerns over regulatory action or civil liability, potential loss of legal protections or privileges, and concerns over reputational harms or business disruptions. These fears are often overstated, but businesses operating under a voluntary disclosure regime will too often default to not reporting incidents as a way to avoid even minimal or hypothetical risk. This, unfortunately, presents a major challenge under a purely voluntary reporting system, and the lack of reporting will continue to harm America’s ability to respond to ransomware and other cyber threats. The failure to report these crimes means they may never get investigated or that the government’s investigation will lose valuable time and evidence often critical to identifying and warning other potential victims before more attacks occur, and critical to identifying, disrupting, and prosecuting the malicious actors behind these attacks.

3. The Administration has recommended mandatory breach notification. What is the recommended punishment, if any, for noncompliance, and why?

RESPONSE: For a reporting requirement to be effective, there must be real consequences from failing to timely file a mandated report. To accomplish this, differing types and levels of penalties tailored and appropriate to the particular facts and circumstances of the violation should be available. But to be a sufficient inducement for some entities to meet the requirements—given competing incentives and uncertainty whether the government will discover a failure to report an incident that is not otherwise disclosed—the penalties available need to include the authority to

impose fines based on, for example, a willful or knowing violation and repeated failures to comply with reporting requirements. These penalties should be administered under regulations and procedures that define the standards and processes that will be used, including the consideration of aggravating and mitigating circumstances, to determine the amount of any fine or other penalty appropriate for a violation.

3. Are sanctions against China a possible response to the Microsoft Exchange hack?

RESPONSE: On July 19, 2021, the United States government, alongside our allies and partners, formally confirmed that cyber actors affiliated with the Chinese Ministry of State Security (“MSS”) exploited vulnerabilities in Microsoft Exchange Server in a massive cyber espionage operation that indiscriminately compromised thousands of computers and networks, mostly belonging to private-sector victims.

As evidenced by the indictment of three MSS officers and one of their contract hackers, which was unsealed by the Department of Justice on the same day the public attribution was made, the United States will impose consequences on malicious cyber actors for their irresponsible behavior in cyberspace.

The United States is working with our partners and allies to promote responsible state behavior in cyberspace, counter cybercrime, and oppose digital authoritarianism. We are also providing support to countries that are committed to building their capacity to protect their digital networks, investigate and impose consequences on malicious cyber actors, and participate in international conversations on cyber policy. These efforts will enhance global security and stability in cyberspace.

Any decision on whether to sanction China for its pattern of irresponsible, disruptive, and destabilizing behavior in cyberspace will not be a decision for the Department of Justice, but rather a decision by the Department of the Treasury with interagency input.

4. How could we encourage American tech companies to comply more speedily with valid process from lawful authorities?

RESPONSE: Investigations are increasingly reliant on electronic evidence held by U.S. businesses, especially customer records held by technology companies. Unfortunately, these same companies routinely fail to comply with legal process within a reasonable time period, and the companies often disregard court-ordered deadlines. Their delays hinder investigations of all types and in many instances impair the government’s ability to identify criminals and interdict criminal activity. The Department has sought to address these problems through dialogue with companies and, when necessary, court intervention. These approaches are sometimes productive but impractical at scale, and the government’s efforts are hampered by the lack of clear remedies. This problem is likely to continue until companies face clear consequences for disregarding their

obligation to timely comply with legal process. Congress may wish to consider whether additional legislation would provide an appropriate mechanism to ensure timely compliance.

5. Can you please let me know definitively if the China Initiative still exists or not?

RESPONSE: The Department remains fully committed to enforcing the criminal laws that protect the intellectual property, critical and emerging technology, and other national assets essential to our nation's security and prosperity. We continue to place a very high priority on countering the threat posed to American research security and academic integrity by the PRC government's agenda and policies. On November 1, 2021, Matthew G. Olsen was sworn in as Assistant Attorney General for National Security. The Attorney General has asked AAG Olsen to review all of the activities of the National Security Division and determine whether any changes are appropriate. The Criminal Division and other components involved in the China Initiative will consult on that activity.

6. In your testimony, you referenced an attempted ransomware attack on hospitals and emergency services during the pandemic. Because attacks on the health care sector are becoming increasingly common and this sector may not be adequately prepared to respond, what other steps (beyond the prompt reporting that you recommended in your testimony) might Congress take to ensure that the health care sector can defend itself adequately against ransomware attacks? For example:

a. To what extent is it necessary or advisable to encourage the practice of "coordinated vulnerability disclosure"?

RESPONSE: The Department of Justice has been generally supportive of coordinated vulnerability disclosure policies and programs. When properly managed, they can be an effective mechanism for encouraging the discovery and community-wide reporting of security vulnerabilities. For this reason, the Department's Criminal Division published a framework in 2017 outlining the elements of a vulnerability disclosure program. U.S. Department of Justice Criminal Division, Computer Crime & Intellectual Property Section, Cybersecurity Unit, *A Framework for a Vulnerability Disclosure Program for Online Systems*, Version 1.0 (July 2017), available at <https://www.justice.gov/criminal-ccips/page/file/983996/download>. This framework has been referenced by other departments and agencies, including in Cybersecurity and Infrastructure Agency Binding Operational Directive 20-01, "Develop and Publish a Vulnerability Disclosure Policy." The healthcare sector might benefit from the adoption of such policies, just like any other sector that relies on electronic devices and software that can harbor cybersecurity vulnerabilities.

b. Are we doing enough to prioritize federal research on health care cyberattacks, or should we encourage certain federal agencies to take additional steps to prioritize such research?

RESPONSE: Learning more about cyberattacks on healthcare facilities could be instructive; however, ensuring that such attacks are reported to the federal government so that federal cyber incident response agencies can mount the appropriate response would be even more consequential. For this reason, the Department of Justice has supported the enactment of federal cyber incident reporting legislation that would cover incidents that affect critical infrastructure.

- c. **In addition to reporting critical incidents, what other steps, if any, do you recommend that Congress or the executive branch take to facilitate the contingency planning that is needed to address ransomware threats to the health care sector and reduce potential harm to patients?**

RESPONSE: This Administration has prioritized efforts to address the threat of ransomware. Those efforts have included improving contingency planning for ransomware incidents against all sectors of the critical infrastructure, such as the healthcare sector. It has also included improving the U.S. Government's cyber incident management and response policies and procedures. Questions about those efforts would best be answered by the National Security Council, the Office of the National Cyber Director, and by the Department of Health and Human Services, the Sector Risk Management Agency for the health and public health sector.

Questions from Senator Sasse:

1. **Given the growing frequency of high-profile ransomware attacks and given that the main prohibition on ransomware payments only relates to payments made to OFAC designated entities, why are we not seeing more sanctions on these variants?**

RESPONSE: The Department of Justice defers to the Department of the Treasury on questions related to its sanction's authority.

- a. **To what extent have each of your agencies observed a change in the character, makeup, and activity of any ransomware variants that have previously been designated by OFAC?**

RESPONSE: The Department of Justice does not comment on active investigations.

- b. **Should public attribution inherently lead to OFAC designations?**

RESPONSE: The Department of Justice defers to the Department of the Treasury on questions related to its sanction's authority.

- c. **Please describe the law enforcement challenges associated with bringing these variants to justice without sanctions.**

RESPONSE: Ransomware is a long-standing problem with unique challenges that pose a serious threat to our public safety and national and economic security. First, the Department of Justice needs to be aware when a significant breach, including a ransomware attack, has occurred. The Department strongly recommends that Congress consider enacting a law to require victims to report breaches to law enforcement.

Ransomware is a transnational crime. Cyber actors take advantage of this fact by using infrastructure located around the world. A cyber actor may use a server in one country to disseminate ransomware; a server in a second country to hold stolen victim information; and an email account in a third country to negotiate with victims. To obtain relevant information, law enforcement investigators often need to use numerous requests for assistance from foreign law enforcement agencies, a process that can be cumbersome and time-consuming.

Some countries also provide safe havens for actors to engage in cybercrime abroad. As we know, Russia has fought our efforts to extradite cybercriminals when they travel outside Russia. Countries like Russia and China also refuse to bring cybercriminals to justice, thus providing a safe harbor for cybercrime.

We also see cybercriminals rebrand under a new name after being sanctioned. In December 2019, the Department of the Treasury took action against Evil Corp, a Russian-based group responsible

for developing and distributing the Dridex banking trojan. In order to circumvent sanctions, Evil Corp members renamed their ransomware multiple times.

Additionally, cyber actors also use sophisticated means to conceal their identities and criminal activities. Technology itself has created places for criminal to hide their tracks with the wide availability of encryption, anonymous services, and untraceable payments. Many ransomware groups host their websites on the Tor Network, which allows them to communicate anonymously with victims. Furthermore, the advent of anonymity-enhanced cryptocurrencies (*e.g.*, “privacy coins”) and the use of identity-concealment technologies (*e.g.*, mixers and tumblers), creates difficulties for investigators to trace the flow of ransom payments. In addition, ransomware’s profitability has created an ecosystem of services dedicated to supporting these crimes, (*e.g.*, ransomware as a service (RaaS), a subscription-based model that enables affiliates to use already-developed ransomware tools to execute ransomware attacks).

Another difficulty our investigators face is that ransomware actors take advantage of web hosting services, e-mail accounts, online storage accounts, and other services offered by American companies that fail to meet their obligations when criminal investigators serve them with search warrants or preservation requests. Federal law requires companies to produce information when the government serves them with a search warrant. If the government obtains a warrant to search a house, agents must search that house within days of when the magistrate signs the warrant. But when the government serves a search warrant on tech companies, they often take weeks, if not months, to return data. And sometimes these companies do not produce any data because they failed to preserve the relevant account. These issues hinder our investigations significantly and are a major factor in criminals’ ability to escape detection and apprehension. We believe that in many cases, the cause of this problem is that providers think about complying with the law and protecting public safety only after they have developed a money-making product. Too often, we discover that providers have failed to prioritize responding to valid legal process: either they do not hire enough staff to respond to legal process, or they equip that staff with inadequate software tools, or both. While we have attempted to work with providers and have raised this issue repeatedly for years, too often solutions do not appear to be forthcoming.

2. How do each of your respective agencies think about deterring actors in this space?

a. What have you found to be the most valuable tools to deter average cybercriminals and ransomware variants from launching attacks?

RESPONSE: Consistent with the whole-of-government response to the ransomware threat, the Department of Justice is coordinating with partner agencies to utilize the capabilities of all departments and agencies to deter ransomware actors. The Department of Justice’s most valuable tools to deter cybercriminals and ransomware actors include arrest, infrastructure disruption, and forfeiture. The Department of Justice has been successful in arresting cybercriminals around the world, signaling to cybercriminals that the United States will hold them accountable for attacks against victims in the United States. When the Department of Justice arrests a cybercriminal, other

cybercriminals often perceive additional risk in continuing to associate with that person, or in entering the same illicit line of work. Similarly, disruption of cybercrime infrastructure dispels the myth of invincibility and highlights the risk that law enforcement will leverage cybercrime infrastructure to identify and apprehend associated cybercriminals. The use of forfeiture authorities to seize criminal proceeds diminishes expected returns of profit-motivated ransomware activity and thus renders cybercrime less attractive.

The January 2021 Netwalker coordinated action illustrated the deterrent effect of these tools in practice. After the United States and its international partners arrested a Netwalker affiliate, disrupted a hidden web resource used to communicate with Netwalker victims, and seized over \$450,000, the Netwalker ransomware gang's operations were severely impeded. See <https://www.justice.gov/opa/pr/departement-justice-launches-global-action-against-netwalker-ransomware>.

b. Where are the most prominent limits to deterrence theory in practice?

RESPONSE: For the Department of Justice, deterrence is impeded by the perception that perpetrators will not actually suffer arrest, prosecution, or other negative consequence for their criminal activity in certain jurisdictions. Perceived “safe haven” jurisdictions can limit the effects of deterrence, and the Department of Justice has pursued robust international cooperation to bring ransomware actors to justice, wherever they are located. These international partnerships include the U.S.-EU Ransomware Working group, the Ottawa 5 Ransomware Working Group, efforts to promote implementation of the Financial Action Task Force Standards for AML/CFT to virtual assets and virtual asset service providers; recent ransomware disruption initiatives; G7 ransomware engagement; and bilateral engagement with countries perceived to allow cybercriminals to target Americans without repercussions. The Departments of Justice and State also partner to manage the State-funded U.S. Transnational and High-Tech Crime Global Law Enforcement Network (GLEN), an initiative designed to deliver capacity building and strengthen international cooperation to combat cybercrime and intellectual property theft. The GLEN features DOJ International Computer Hacking and Intellectual Property Advisors (ICHIPs), DOJ Global Cyber Forensic Advisors and long-term federal agent mentors. The GLEN has escalated its efforts to deliver training specifically designed to combat criminal misuse of cryptocurrency, including through analysis training and establishment of regional working groups.

The Department has further sought to facilitate international cybercrime enforcement through its work on the Budapest Convention on Cybercrime, including the recently concluded negotiations on the Second Additional Protocol to the Budapest Convention, and through ongoing multilateral negotiations on a cybercrime treaty at the United Nations, and through delivery of capacity building to enable developing countries to enact legislation in line with the provisions of the Convention and, on the foundation of that framework, engage in the process of accession to that treaty. The Department's ongoing effort to negotiate CLOUD agreements with trusted foreign partners promises to expedite cybercrime investigations and more efficiently prosecute cybercriminals. Recent public messaging by Department leadership has further amplified the

deterrent message of recent law enforcement activity, including the disruption of ransomware infrastructure overseas and the indictments and arrest of overseas ransomware actors.

3. How would you describe the role of the ransomware insurance market in combatting the growing ransomware issue? Is the insurance market more helpful or harmful to the ultimate goal of reducing ransomware attacks?

a. Are companies with ransomware insurance more likely to pay a ransom than those without insurance?

RESPONSE: Ransomware insurance carries the possibility of producing helpful and harmful effects on the reduction of ransomware attacks. Payment of ransoms encourages ransomware groups to continue their efforts. However, if cyber insurance companies required the insured to maintain set standards of cyber security as a condition of reimbursement of a ransom payment, report ransomware attacks to law enforcement, and cooperate with law enforcement investigations, this could help reduce the number of successful ransomware attacks.

b. Is there any evidence to suggest that hackers are more likely to target companies that have ransomware insurance?

RESPONSE: The Department of Justice does not have statistics on whether that is the case.

4. According to the blockchain research firm Chainalysis, ransomware payments reached a total of \$412 million during 2020, representing a 341 percent increase over the prior year. How is the ransomware insurance market responding to this growing number of attacks?

a. Are insurance companies requiring their customers to maintain any baseline security or preventative measures in order to qualify for coverage?

RESPONSE: The Department of Justice does not have statistics on insurance policies.

b. Outside of advising on “best practices,” is there anything else the government can, or should, be doing to fortify our resilience against ransom attacks through the insurance industry?

RESPONSE: The insurance industry is one of the many private partners who can help strengthen cybersecurity and mitigate ransomware attacks. Recognizing that role, the Administration engaged with the insurance industry at the August 2021 White House Cybersecurity Summit. The Administration is continuing to study ways that the insurance industry can play a role in improving cyber resilience.

5. Who is currently responsible for regulations relating to the ransomware insurance industry?

- a. **At present, are insurance companies required to report to the government ransom attacks against their customers for whom they make payments? If not, is there any reason why they should not be required to do so?**

RESPONSE: The Department of Justice defers to the Department of the Treasury.

| | |
|-------------------|--|
| Question#: | 1 |
| Topic: | Expanding Services |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Question: Will CISA be expanding its services to businesses as the threat of ransomware grows? I understand stopransomware.gov to be a first step. What is the next step? Are you also looking into, for example, expanding phone support for small business and individuals, or providing cybersecurity products directly?

Response: The Cybersecurity and Infrastructure Security Agency (CISA) is focused on reducing the risk of ransomware attacks by working collaboratively with our federal, state, local and private sector partners to enhance infrastructure cybersecurity against today’s threats and shape the strategic environment over the long-term. CISA is engaged on multiple fronts to help address ransomware and is working to raise awareness and promote basic cyber hygiene across tens of thousands of businesses and within our own government agencies. In summer 2021, CISA led the interagency development and launch of “StopRansomware.gov,” the U.S. Government’s official repository for resources from across the interagency community to help public and private organizations tackle ransomware more effectively. Victims are encouraged to visit StopRansomware.gov to help determine if they have been hit by ransomware, learn more about what they can expect through the arc of the attack, and see what steps they can take to mitigate the impact and to recover.

CISA aims to give organizations the tools and guidance they need to increase their resilience and security. We continually develop and share a variety of resources – including extensive guidance and best practices – that can help at-risk entities reduce the chance of being successfully attacked and mitigate the impact if they are attacked. This includes technical indicators related to specific ransomware campaigns. Entities can utilize these resources to expand their awareness of ransomware and other cyber threats, assess their individual risk profile, and take positive action to protect themselves from a successful cyberattack. These resources are free and available through “StopRansomware.gov”.

CISA is also available to provide technical assistance, upon request, to critical infrastructure organizations during major cybersecurity incidents. CISA’s role is to help victims understand the extent of an intrusion, evict the adversary, adopt strong security practices to prevent future intrusions, and also to gather information to protect other potential victims from being attacked in the first place. CISA has cybersecurity advisors and coordinators deployed across the country who offer cybersecurity assistance on a voluntary, no-cost basis to critical infrastructure organizations, including state, local, tribal and territorial (SLTT) governments. The cybersecurity advisors and coordinators provide cyber preparedness, strategic messaging, working group support, partnership development, cyber assessments, threat information sharing and incident coordination and support. As an example, during a recent ransomware incident involving the food/agriculture sector, cybersecurity advisors partnered with CISA headquarters, private sector

| | |
|-------------------|--|
| Question#: | 1 |
| Topic: | Expanding Services |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

partners associated with the Joint Cyber Defense Collaborative, and the Federal Bureau of Investigation (FBI) to mitigate the ransomware attack and restore their systems to continue their business operations.

Additionally, CISA is building new, and strengthening existing, partnerships with key players to leverage its expansive information-sharing authorities to ensure early warning of threats and attacks.

| | |
|-------------------|--|
| Question#: | 2 |
| Topic: | Cyber Insurance |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Question: How useful is cyber insurance for large business and local governments? Is cyber insurance an essential expense for small businesses?

Does cyber insurance result in more ransoms being paid, which can have the unwanted effect of increased funding to criminal groups?

Response: Cyber insurance is a relatively new and specialized market that broadly includes forms of insurance that address losses resulting from cybersecurity or other computer-related issues, depending on the coverage. Although cyber insurance products have been on the market since the late 1990s, the market is still maturing and remains underdeveloped despite significant growth over the last two years. This relatively new form of insurance varies greatly from carrier to carrier in terms of coverage, as well as how carriers measure and assess risk.

SLTTs and private sector partners have availed themselves of cyber insurance for several years. Organizations participate in the cyber insurance market to transfer the risk of cyber threats. However, there are multiple issues limiting the potential of the cyber insurance market and the pace at which the market is evolving, namely the ability to assess risk accurately. To do so, insurance companies would need to mature underwriting guidelines, risk management processes, and robust and reliable pricing models that are continuously validated, especially given the dynamic nature of cyber risk.

| | |
|-------------------|--|
| Question#: | 3 |
| Topic: | Agriculture Ransomware |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Question: Agriculture is a target for ransomware. What are some of the unique challenges of protecting agriculture from these attacks?

Response: In addition to the negative impacts faced by other businesses, ransomware attacks targeting the agriculture sector can also impact the food supply chain, resulting in direct consequences for every American. The introduction of information technology to the industry brings cybersecurity requirements to large businesses, small farms, and producers that may not have considered these risks before now. Taking recommended steps to protect networks, systems, and data may be difficult to manage for small-scale operations that have limited resources and experience implementing and managing cybersecurity programs. Additionally, the geographically distributed nature of agriculture in the U.S. makes identifying, detecting, remediating, and recovering from cybersecurity-related issues particularly challenging. While small farms and producers may not be a primary target, these groups represent a significant part of the industry, increasing risk and the challenge of mitigating cybersecurity issues at scale. CISA's resources listed on "StopRansomware.gov" are designed to be accessible to businesses of different sizes and levels of cybersecurity experience, with many products specifically designed for small and medium businesses.

| | |
|-------------------|--|
| Question#: | 4 |
| Topic: | Unreported Incidents |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Question: During the hearing you noted that you believe that only about a quarter of ransomware incidents are reported.

Can you please confirm the percentage of ransomware incidents that are believed to be unreported to federal law enforcement? Please describe how you arrived at your estimate.

Why do you believe so many incidents are unreported? Are any of these incidents reported to state or local law enforcement but not federal law enforcement?

Response: The percentage of ransomware incidents potentially unreported to federal law enforcement or to CISA remains high. We know that private companies are performing incident response work with entities impacted by ransomware, and we know that the number of ransomware attacks targeting private companies is high. Today, CISA only receives information on a fraction of incidents and lacks a reliable way to understand the breadth of unreported incidents. This hampers our visibility and, thus, our ability to conduct critical analysis, spot adversary campaigns, release mitigation guidance, and provide timely response to critical infrastructure operators.

CISA must continue to invest in and mature our voluntary partnerships with critical infrastructure entities. Ensuring that partners are aware of information sharing protections available through the Cybersecurity Information Sharing Act of 2015 and the Protected Critical Infrastructure Information Act will help enhance trusted information sharing between CISA and the private sector. We further look forward to working with Congress in enacting mandatory incident reporting legislation.

| | |
|-------------------|--|
| Question#: | 5 |
| Topic: | Reporting Mandate |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Question: If Congress mandates reporting of ransomware incidents to federal law enforcement, what incentives or penalties does CISA recommend be included in the mandate to promote compliance?

If Congress mandates reporting of ransomware incidents, to what agencies does CISA recommend reporting to satisfy a mandate?

Response: CISA appreciates Congress’s leadership on this issue and applauds the recent passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (“CIRA”), which became law with the Fiscal Year 2022 Omnibus Appropriations bill. This legislation enables the visibility required for us to better see cybersecurity threats and to address the devastating effects of cyber-attacks.

The reality is that the private sector owns and operates the vast majority of our nation’s critical infrastructure, so they play a vital role in working with CISA to improve our nation’s cybersecurity. Mandatory incident notification is necessary for CISA and other federal agencies to identify significant incidents in their early stages and allow us the window needed to analyze the situation and then investigate, respond to the adversary, and help mitigate impacts. CISA supports broad cyber incident reporting requirements that would require the reporting of a range of cyber incidents, including ransomware and incidents that impact critical infrastructure and their supply chains.

Over the next 24 months, CISA will develop proposed rules for implementing mandatory cyber incident reporting for critical infrastructure owners and operators. The rulemaking process will be consultative with our government and industry partners and will ensure that we are striking the right balance between getting accurate information quickly and letting victims respond to an attack without imposing onerous requirements on them. Part of this rulemaking process will include the establishment of thresholds of impact to ensure that the information received is relevant and impactful.

CISA and its partners, such as the FBI, will use these reports to build a common understanding of how our adversaries are targeting U.S. networks and critical infrastructure. This information will fill critical information gaps and allow us to analyze incoming reporting across sectors to spot trends, deploy resources and render assistance to victims suffering attacks, and quickly share that information with network defenders to warn other potential victims. These reports will help identify significant incidents in their early stages and allow us to help mitigate impacts to critical infrastructure.

| | |
|-------------------|--|
| Question#: | 5 |
| Topic: | Reporting Mandate |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Without prompt notification to CISA, critical analysis, mitigation guidance, and information sharing is severely delayed, leaving critical infrastructure vulnerable. Timely information can be the difference between containing an incident and seeing its effects cascade across sectors and the economy. That is why rapid reporting of cyber incidents by private sector entities is crucial. CISA's goal is not to overwhelm companies or our own personnel, but to balance getting information in a timely manner with ensuring that information is meaningful and actionable. Any mandated reporting of cybersecurity incidents should include timely reporting to CISA, along with any other departments and agencies the Administration and legislation determines appropriate. .

| | |
|-------------------|--|
| Question#: | 6 |
| Topic: | Agency Coordination |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Question: How do FBI, USSS, and CISA coordinate among agencies to ensure efforts are not duplicated?

Response: Every incident is unique and requires a high degree of interaction with the affected entity to determine incident severity and impact, among other technical details necessary for incident response.

Under Presidential Policy Directive (PPD) 41, CISA serves as the lead for asset response during a significant cyber incident. As the lead for asset response, CISA is focused on helping victim organizations evict the adversary and restore to a secure state. CISA also aims to derive information from the intrusion to share quickly with government and private sector partners to understand the extent of the threat and recommend actions that will help prevent further similar intrusions. CISA collaborates with industry and government partners to help organizations understand and counter cybersecurity risks associated with the malicious activities of nation-state and non-state actors. FBI is the lead agency for threat response activities, focused on investigating an incident, attributing incidents to adversaries and contextualizing them within the broader threat intelligence picture, and working with federal and foreign partners to impose costs on the responsible actor. The United States Secret Service (USSS) provides critical investigatory capabilities under its unique authorities.

CISA also has cybersecurity advisors and coordinators deployed across the country who offer cybersecurity assistance on a voluntary, no-cost basis to critical infrastructure organizations, including SLTT governments. The field-based cybersecurity advisors and coordinators partner with their local FBI and USSS field offices to provide cyber preparedness, strategic messaging, working group support, partnership development, cyber assessments, threat information sharing, and incident coordination and support.

CISA's success in its mission relies on building strong partnerships to collectively address our shared risk. Cybersecurity requires a whole-of-government and whole-of-society approach. CISA is focused on working with its interagency partners to ensure accountability in managing, mitigating, and reducing risk to digital and critical infrastructure.

| | |
|-------------------|--|
| Question#: | 7 |
| Topic: | OFAC Designations |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Ben Sasse |
| Committee: | JUDICIARY (SENATE) |

Question: Given the growing frequency of high-profile ransomware attacks and given that the main prohibition on ransomware payments only relates to payments made to OFAC designated entities, why are we not seeing more sanctions on these variants?

Response: USSS works closely with the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury, and other relevant interagency partners, to consider the potential applications of sanctions under Executive Order 13694 and related authorities. OFAC publishes identifying information of individuals, groups, and entities that are specially designated for sanctions. Publicly identifying such foreign persons or entities has the potential of impeding law enforcement and other actions against them by causing them to go in to hiding or otherwise altering their operations so they can continue their criminal activity. Therefore, interagency consideration is essential to effectively and appropriately use sanctions designations to address malicious cyber activity.

Question: To what extent have each of your agencies observed a change in the character, makeup, and activity of any ransomware variants that have previously been designated by OFAC?

Response: The USSS has observed foreign persons designated for their malicious cyber activities continue to engage in similar transnational cyber criminal activity.

Question: Should public attribution inherently lead to OFAC designations?

Response: If the U.S. government has already publicly identified foreign persons engaging in malicious cyber activity, such as by unsealing an indictment, then OFAC also designating them likely presents little additional operational risk. However, further consideration may be warranted to determine if sanctions are appropriate and consistent with relevant laws, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*) (NEA), and/or section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)). To this end, the interagency deliberates and sequences whole-of-government campaigns including a range of cost-imposing consequences against adversaries. These decisions are made necessarily on a case-by-case basis in an effort to shape adversary behavior in light of what we know about adversary motivations through intelligence, diplomatic, law enforcement, economic, and CERT-to-CERT channels.

Question: Please describe the law enforcement challenges associated with bringing these variants to justice without sanctions.

| | |
|-------------------|--|
| Question#: | 7 |
| Topic: | OFAC Designations |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Ben Sasse |
| Committee: | JUDICIARY (SENATE) |

Response: Ransomware variants are easily created, therefore the USSS focuses on arresting and seizing the assets of those involved in criminal conspiracies and other violations of federal law. Often these individuals reside in foreign countries and it requires significant international law enforcement cooperation to locate and extradite them to face justice. In cases where ransomware actors are located in countries without an extradition treaty with the United States and poor mutual law enforcement assistance relationships, such as Russia, law enforcement often witnesses criminals enjoying “safe haven” wherein they can operate with relative impunity from local justice. Despite the challenges inherent in such operations, the USSS and our law enforcement partners have been successful in arresting such individuals. This includes those that are located in countries that do not have extradition treaties with the United States. Developing the investigative teams and international cooperation to scale these law enforcement efforts to curb the growing threat of ransomware is an important budgetary priority, which is challenging to execute under a continuing resolution and fiscal uncertainty. The FBI can provide additional insight on the range of challenges faced by law enforcement.

| | |
|-------------------|--|
| Question#: | 8 |
| Topic: | Deterrence |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Ben Sasse |
| Committee: | JUDICIARY (SENATE) |

Question: How do each of your respective agencies think about deterring actors in this space?

What have you found to be the most valuable tools to deter average cybercriminals and ransomware variants from launching attacks?

Where are the most prominent limits to deterrence theory in practice?

Response: CISA focuses on driving “deterrence through denial,” in which targeted organizations adopt strong security and resilience measures to make it difficult for cyber adversaries to achieve their goals. CISA develops and shares extensive guidance and best practices that can help at-risk entities reduce the chance of being successfully attacked and mitigate the impact if they are attacked, including technical indicators related to specific ransomware campaigns. “StopRansomware.gov” provides cyber incident preparedness resources, including checklists and training to help organizations reduce the likelihood of becoming a victim of a ransomware attack and guides on what to do if affected by ransomware, directing readers to a reporting mechanism to the FBI, CISA, and the USSS. Organizations should apply these best practices to the greatest extent possible based on the availability of organizational resources to help manage the risk posed by ransomware and support a coordinated and efficient response to a ransomware incident.

| | |
|-------------------|--|
| Question#: | 9 |
| Topic: | Ransomware Insurance I |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Ben Sasse |
| Committee: | JUDICIARY (SENATE) |

Question: How would you describe the role of the ransomware insurance market in combatting the growing ransomware issue? Is the insurance market more helpful or harmful to the ultimate goal of reducing ransomware attacks?

Are companies with ransomware insurance more likely to pay a ransom than those without insurance?

Is there any evidence to suggest that hackers are more likely to target companies that have ransomware insurance?

Response: Cyber insurance is a relatively new and specialized market that broadly includes forms of insurance that address losses resulting from cybersecurity or other computer-related issues, depending on the coverage. Although cyber insurance products have been on the market since the late 1990s, the market is still maturing and remains underdeveloped despite significant growth over the last two years. This relatively new form of insurance involves coverages that vary greatly from carrier to carrier, as well as how carriers measure and assess risk.

SLTTs and private sector partners have availed themselves of cyber insurance for several years. Organizations participate in the cyber insurance market to transfer the risk of cyber threats. However, there are multiple issues limiting the potential of the cyber insurance market and the pace at which the market is evolving, namely the ability to assess risk accurately. To do so, insurance companies would need to mature underwriting guidelines, risk management processes, and robust and reliable pricing models that are continuously validated, especially given the dynamic nature of cyber risk.

Similarly, the limited visibility into the full scope of different ransomware incidents limits the ability to determine if hackers target insured companies over the uninsured. Mandatory incident reporting legislation could provide insight allowing an answer to this question of targeting.

| | |
|-------------------|--|
| Question#: | 10 |
| Topic: | Ransomware Insurance II |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Ben Sasse |
| Committee: | JUDICIARY (SENATE) |

Question: According to the blockchain research firm Chainalysis, ransomware payments reached a total of \$412 million during 2020, representing a 341 percent increase over the prior year. How is the ransomware insurance market responding to this growing number of attacks?

Are insurance companies requiring their customers to maintain any baseline security or preventative measures in order to qualify for coverage?

Outside of advising on "best practices," is there anything else the government can, or should, be doing to fortify our resilience against ransom attacks through the insurance industry?

Response: Cyber insurance is a relatively new and specialized market that broadly includes forms of insurance that address losses resulting from cybersecurity or other computer-related issues, depending on the coverage. Although cyber insurance products have been on the market since the late 1990s, the market is still maturing and remains underdeveloped despite significant growth over the last two years. This relatively new form of insurance involves coverages that vary greatly from carrier to carrier, as well as how carriers measure and assess risk.

SLTTs and private sector partners have availed themselves of cyber insurance for several years. Organizations participate in the cyber insurance market to transfer the risk of cyber threats. However, there are multiple issues limiting the potential of the cyber insurance market and the pace at which the market is evolving, namely the ability to assess risk accurately. To do so, insurance companies would need to mature underwriting guidelines, risk management processes, and robust and reliable pricing models that are continuously validated, especially given the dynamic nature of cyber risk.

| | |
|-------------------|--|
| Question#: | 11 |
| Topic: | Ransomware Insurance Regulations |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Ben Sasse |
| Committee: | JUDICIARY (SENATE) |

Question: Who is currently responsible for regulations relating to the ransomware insurance industry?

At present, are insurance companies required to report to the government ransom attacks against their customers for whom they make payments? If not, is there any reason why they should not be required to do so?

Response: Insurance is regulated at the state level.

Although some sectors (*e.g.*, financial institutions and healthcare) are required under federal law to report to a federal regulator regarding incidents affecting their systems or information, there is currently no single mandatory federal requirement to report cyber incidents or ransomware payments (including payments that insurance companies make on behalf of other entities). Rather, entities must assess the complex disclosure requirements imposed by an array of agencies at the federal and state levels. Moreover, when a victim does seek to do the right thing and report an incident to the federal government, they may not know which agencies to contact, delaying their reporting during an emergency situation. Among the harms this may cause is a lag in availability of critical mitigation guidance to the operators who are positioned to take action. Without timely notification to CISA, critical analysis, mitigation guidance, and information sharing is severely delayed, leaving critical infrastructure vulnerable. Timely information can be the difference between containing an incident and seeing its effects cascade across sectors and the economy.

CISA appreciates the work of members of Congress in both the House and the Senate on cyber incident notification in the 117th Congress. The earlier that CISA, the federal lead for asset response, receives information about a cyber incident, the faster it can conduct urgent analysis and share information to protect other potential victims. Further, it would allow insight that could answer these questions on the value of cyber insurance.

| | |
|-------------------|--|
| Question#: | 12 |
| Topic: | Combatting Attacks |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | Senator Thom Tillis |
| Committee: | JUDICIARY (SENATE) |

Question: We have heard that combatting ransomware threats requires a whole-of-government and whole-of-society approach. What must be done to improve coordination among the many actors that play a role in combatting ransomware attacks, stopping future attacks, and bringing the bad actors to justice, and what should Congress do to help?

Response: One of CISA's top priorities is forging strong partnerships with critical infrastructure partners to enable robust operational collaboration, identify adversary activity across sectors, produce more targeted guidance, and ultimately reduce the frequency and impact of cyber incidents. We are leveraging these partnerships to increase operational collaboration through the newly established Joint Cyber Defense Collective (JCDC). The JCDC will leverage CISA's broad authorities to share information about threats and vulnerabilities to enable early warning and prevent other victims from being attacked, enabling us to transform information sharing into timely, relevant information action.

The JCDC brings together the authorities, capabilities, and talents of the federal government with the power of industry to enable shared situational awareness of the threat landscape, to plan and action against the most significant threats to the nation. The JCDC leads the development of the nation's cyber defense plans, which outline activities to prevent and reduce the impacts of cyber intrusions. Leveraging new authorities provided by the National Defense Authorization Act of 2021, the JCDC brings together public- and private sector entities to unify deliberative and crisis action planning while coordinating the integrated execution of these plans. The plans promote national resilience by coordinating actions to identify, protect against, and respond to malicious cyber activity targeting U.S. critical infrastructure or national interests.

| | |
|-------------------|--|
| Question#: | 13 |
| Topic: | Private Information Sharing |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | Senator Thom Tillis |
| Committee: | JUDICIARY (SENATE) |

Question: What reasons do private sector entities give as to why they may not readily share information with the federal government. What assurances are you prepared to give those who share information or report incidents to address concerns that sharing information with the government could lead to harm to reputation, regulatory retaliation, or harms to private sector intellectual property? How will the government safeguard data provided by companies as part of the effort to combat ransomware attacks?

Response: The private sector, which owns and operates most of the nation's critical infrastructure, plays a vital role in working with CISA to improve our nation's cybersecurity. Private sector organizations are not required to request assistance from the federal government but are strongly encouraged to consider requesting assistance from CISA when faced with a cyber intrusion. Incentivizing the private sector to work with the federal government is key to the voluntary collaboration upon which CISA has always relied. The private sector must see the benefit and the results through efforts such as CISA's assistance programs and threat information sharing programs as outweighing any risk in sharing. It is incumbent on CISA to provide that assurance to our partners. For example, ensuring that partners are aware of information sharing protections available under the Cybersecurity Information Sharing Act of 2015 and the Critical Infrastructure Information Act will enable enhanced trusted information sharing between CISA and the private sector. CISA has discovered that private sector entities are not always aware of the existence of these protections, which can result in less information being shared in a timely manner. In addition, private sector entities often point to European privacy regulations as a reason for why they cannot share cyber threat information with CISA.

Rapid reporting of cyber incidents by private sector entities can help identify significant incidents in their early stages and allow CISA to help mitigate impacts to critical infrastructure. CISA can help an organization determine the scope of the infection, ensure the adversary is out of the network, and advise on how to rebuild -- but only if we know about the incident. CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities. Irrespective of the type of incident or its reporting method, CISA works to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.

CISA views privacy as more than just compliance with privacy law and policy. Privacy at CISA is also about public trust and confidence, and how the government acts responsibly and transparently in the way it collects, maintains, and uses information provided by the public. CISA has a long history of receiving information from the private sector and has, throughout that history, effectively protected the data supplied to us by our partners consistent with the principles of the Privacy Act of 1974, the E-Government Act of 2002, and the Critical Infrastructure Act of

| | |
|-------------------|--|
| Question#: | 13 |
| Topic: | Private Information Sharing |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | Senator Thom Tillis |
| Committee: | JUDICIARY (SENATE) |

2002. CISA regularly works with the private industry and diligently protects the data and privacy of the entities we work with. We will continue this practice whether information is shared pursuant to voluntary cyber threat information sharing program or, if enacted, under a mandatory incident reporting law. Regardless of how incident information is reported, CISA remains committed to using that information in a way that protects the victim's identity and helps to protect future targets from compromise.

| | |
|-------------------|--|
| Question#: | 14 |
| Topic: | Retention |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | Senator Thom Tillis |
| Committee: | JUDICIARY (SENATE) |

Question: What changes need to be made to the federal government or your Department's hiring practices to attract and retain top cybersecurity professionals? How will the planned cybersecurity talent management system and other policy changes under consideration by your agency assist in combatting cybercrimes and ransomware attacks? When will such changes be implemented?

Response: Building the nation's cyber workforce is a major priority for CISA. Projections suggest a global cybersecurity workforce shortage of millions, with more than half a million of those positions in the U.S. alone. The United States has an estimated 500,000 vacant cybersecurity jobs, over 35,000 within the government. These are high-paying, professional jobs that need people of diverse backgrounds and experiences to fill them!

CISA offers a diverse set of career prospects, from ethical hackers, who are engaged in penetration testing or "red team" attacks, to malware analysts, who study the functionality and potential origins of malware samples, to a host of other positions. CISA strives to prioritize career growth for our workforce. Because the cybersecurity field is so diverse, there are many opportunities to move up, gain more experience, or transfer positions.

On November 15, 2021, DHS and CISA launched the Cybersecurity Talent Management System (CTMS), an innovative new personnel system designed to more effectively recruit, compensate, and retain our top cybersecurity professionals. Through CTMS, the DHS hiring process for cybersecurity positions can shift away from the standard hiring model, which is largely based on formal education requirements, to instead focus on a candidate's demonstrated skills and aptitude. CTMS candidates will be evaluated by a series of assessments and simulations.

CTMS will be used as an additional tool to attract the full spectrum of cyber talent from entry-level through senior executives, including technical subject-matter experts. CTMS will strengthen the cyber workforce by bringing in applicants from both outside as well as from within the federal government.

CTMS is unique as it completely reimagines the entire federal hiring process. Importantly, it is designed to be adaptable to meet mission and market demands. CTMS will help improve the ability to identify mission critical skills, build a better pipeline to help the best qualified candidates make the transition between the private sector and the government, and compensate team members using market-sensitive salaries based on their demonstrated expertise.

| | |
|-------------------|--|
| Question#: | 15 |
| Topic: | New Website |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | Senator Thom Tillis |
| Committee: | JUDICIARY (SENATE) |

Question: The new website StopRansomware.gov is designed to pool resources from several government agencies. What plans are there to ensure that this information is curated, maintained, and remains relevant and user-friendly? What efforts are made to ensure the public is aware of this resource?

Response: “StopRansomware.gov” is a whole-of-government website. As such, CISA works with partners across the federal government to update threat information and ensure it remains relevant. The site is discussed regularly at multiple stakeholder meetings and CISA works with agencies to add information as it becomes available. The website and its resources are also listed in speaking engagements, at conferences and events, and via social media. It is consistently in the top 10 pages visited on CISA.gov and, to date, has been visited more than 454 thousand times.

| | |
|-------------------|--|
| Question#: | 16 |
| Topic: | Resources Available |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | Senator Thom Tillis |
| Committee: | JUDICIARY (SENATE) |

Question: What resources are you making available to State and Local Governments in light of the ransomware crisis?

Response: CISA is urgently focused on reducing the risk of ransomware attacks by working collaboratively with all of our partners, including SLTT governments to enhance cybersecurity against today’s threats and shape the strategic environment over the long-term to a better protected one.

In January 2021, CISA kicked off a cybersecurity awareness and outreach campaign to encourage public- and private sector organizations and key stakeholders to take appropriate actions to “Reduce the Risk of Ransomware.” In coordination with the Multi-State Information Sharing and Analysis Center, CISA released a joint Ransomware Guide that details industry best practices and a response checklist that can serve as a ransomware-specific addendum to state and local governments’ cyber incident response plans. CISA supported DHS Secretary Mayorkas’ Ransomware Sprint, which ran through April and May 2021 and was designed to ensure that all sectors of the economy, including SLTTs, understand the criticality of this risk and take urgent action in response. CISA has already filled 37 of the Cybersecurity State Coordinator positions based in the 50 state capitals and will fill the remaining spots in the near future as authorized in the Fiscal Year 2021 National Defense Authorization Act. Duties of these state coordinators include: relationship building and advisement on governance structures for developing and maintaining secure and resilient infrastructure; serving as the federal cybersecurity risk advisor to support preparation, response, and remediation efforts; facilitating cyber threat information sharing; raising awareness of federal cybersecurity resources available to non-federal entities to increase resilience; supporting training and exercises, and planning for continuity of operations and expedited recovery; serving as a principal point-of-contact for non-federal entities to engage the federal government on cyber incidents; assisting non-federal entities in developing vulnerability disclosure programs; and assisting in the development of state cybersecurity plans. Augmenting the state coordinators, CISA also has cybersecurity advisors deployed in major cities across the country who offer cybersecurity assistance on a voluntary, no-cost basis to critical infrastructure organizations including SLTTs. These cybersecurity advisors and coordinators force multiply our already substantial regional efforts and the outreach to our SLTT partners will do nothing but increase in the future.

In July, CISA spearheaded the development and launch of the whole-of-government resource “StopRansomware.Gov” to make it easier for organizations across the country to find free and authoritative information, resources, and tools they need to prepare for and respond to ransomware intrusions. The launch of StopRansomware.gov is a reflection of how dangerous the threat of ransomware is – this is a coordinated effort across numerous federal agencies, who are

| | |
|-------------------|--|
| Question#: | 16 |
| Topic: | Resources Available |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | Senator Thom Tillis |
| Committee: | JUDICIARY (SENATE) |

pooling their resources to enable organizations to learn how to reduce their ransomware risk and better protect their networks, with the effect of discouraging malicious cyber actors from engaging in ransomware.

Further, CISA is developing a catalog of Bad Practices that are exceptionally risky to encourage organizations to implement an effective cybersecurity program to protect against cyber threats. Sector-specific guidance is also being developed and will be provided for all 16 critical infrastructure sectors vital to the nation. Disabling or destroying the 16 critical infrastructure sectors would cause great harm to security, economic welfare, public health, and safety.

Additionally, CISA has also made resources available through the Federal Virtual Training Environment, which provides free online cybersecurity training to federal employees, SLTT government employees, federal contractors, and US military veterans.

| | |
|-------------------|--|
| Question#: | 17 |
| Topic: | Secure Storage |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | Senator Thom Tillis |
| Committee: | JUDICIARY (SENATE) |

Question: What percentage of data is encrypted at rest on federal and commercial systems? How can we incentivize system owners to further adopt secure storage solutions?

Response: As directed by Section 3(c)(ii) of Executive Order 14028, “Improving the Nation’s Cybersecurity,” CISA is working across the federal civilian executive branch to understand government-wide progress in adopting multifactor authentication and encryption of data at rest and in transit.

Through the Executive Order, CISA will support agencies in driving adoption of multifactor authentication and encryption for data at-rest and in-transit and will also work with NIST to develop an initial list of secure software development lifecycle standards for software purchased by the Federal Government and minimum testing requirements for software source code. CISA will continue to analyze the reporting coming in from the interagency and take appropriate action to maximize the implementation of multifactor authentication and data encryption across the Federal Civilian Executive Branch.

To help with these changes, CISA recently developed a Zero Trust Maturity Model and Cloud Security Technical Reference Architecture to assist agencies as they implement data protection measures by leveraging ZTAs and greater use of the cloud. The Zero Trust Maturity Model will assist agencies in the development of their zero trust strategies and implementation plans. It also provides several ways in which CISA services can help support zero trust solutions. On the other hand, the Cloud Security Technical Reference Architecture was developed in coordination with federal government partners and is designed to guide agencies’ secure migration to the cloud by explaining considerations for things like shared services and cloud security posture management.

CISA is committed to the adoption of zero trust cybersecurity principles. As organizations migrate towards zero trust architecture, their mindsets must shift from a “location-centric” to a “data-centric” approach to cybersecurity. The zero trust model can be used as a way for organizations to secure their applications and data within the enterprise, as opposed to focusing on the traditional network perimeter model as the primary means of defense.

As outlined in CISA’s Zero Trust Maturity Model, data should be protected on devices, in applications, and networks, and organizations should inventory, categorize, and label data, protect data at-rest and in-transit, and deploy mechanisms for detection data exfiltration. Organizations are encouraged to begin adopting zero trust principles immediately, knowing that adopting a mature zero trust architecture can take several years. In the near term, organizations should transition from primarily storing data in on-premises data stores where they are

| | |
|-------------------|--|
| Question#: | 17 |
| Topic: | Secure Storage |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | Senator Thom Tillis |
| Committee: | JUDICIARY (SENATE) |

unencrypted at rest towards storing data in cloud or remote environments where they are encrypted at rest, with the ultimate goal of encrypting all data at rest.

| | |
|-------------------|--|
| Question#: | 1 |
| Topic: | State-Affiliated Attacks |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Question: What do you see as our options to best deter and punish state-affiliated ransomware attacks?

Response: Law enforcement agencies, like the United States Secret Service, perform a limited, but important role, in deterring and punishing activities of foreign states. Through our criminal investigations, and international law enforcement cooperation, we detect, investigate, arrest, and prosecute those engaged in transnational cyber crimes and seize their ill-gotten assets. Through these law enforcement actions we directly deter and punish those that engage in the use of ransomware, regardless of a potential affiliation with a state. Law enforcement also develops and shares actionable information that can be used to protect against and mitigate the impact of ransomware.

Law enforcement actions also help to illuminate the conduct of foreign states—for example, are they unwitting of transnational cyber criminals in their jurisdictions or knowingly tolerating such activities. Understanding such distinctions in foreign state conduct can be essential to diplomatic or other efforts to alter the conduct of a foreign state.

Because those responsible for ransomware attacks hide their true identities and physical locations in cyberspace, the State Department has partnered up with federal law enforcement agencies to offer rewards for information leading to the identification and location of key leaders of these transnational criminal organizations under the Transnational Organized Crime Rewards Program pursuant to 22 USC 2708(b)(6). Currently, there are two up to \$10 million reward offers for information leading to the identification or location of an individual who holds key leadership positions in the transnational organized crime groups: the [DarkSide Ransomware Group](#) and the [Sodinokibi Ransomware Group](#).

For these reasons, law enforcement is an essential component in addressing transnational criminal activity like ransomware.

| | |
|-------------------|--|
| Question#: | 2 |
| Topic: | Payment Mechanisms |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Question: During the hearing you noted that without cryptocurrency that ransomware attacks would still occur but that a different payment mechanism would be utilized. Please describe what other payments structures could or have been utilized by bad actors to facilitate ransomware payments. Are there other payment mechanisms we should focus on in addition to cryptocurrency if we want to disrupt the ability of these criminals to profit from their work?

Response: Cyber extortion schemes, like ransomware, have existed longer than cryptocurrency. For example, cyber extortionists have required payment by mailing a cashier's check (or similar payment order) to a post office box, use of various money transmission services, cash shipments and deliveries, and other payment methods. Such means continue to be utilized, in addition to the use of cryptocurrency. A technology neutral approach to strengthening US enforcement related to money laundering, regardless of the form of money used, could be effective and disrupting the ability of transnational cyber criminals to profit from ransomware and other illicit activity.

| | |
|-------------------|--|
| Question#: | 3 |
| Topic: | Ransomware Guidance |
| Hearing: | America Under Siege: Preventing and Responding to Ransomware Attacks |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Question: If victims of ransomware contact either the FBI or USSS, are they given the same or similar guidance? Has federal law enforcement coordinated how reported incidents are investigated? What is the procedure that FBI and USSS use to de-conflict cases?

Response: The Secret Service has closely coordinated with the Federal Bureau of Investigation (FBI), U.S. Department of Justice, the Cybersecurity and Infrastructure Security Agency (CISA), and other agencies in providing information on how organizations should respond to ransomware incidents. We all work closely together to provide consistent and appropriate guidance, to include through the information published on stopransomware.gov.

The Secret Service regularly works with other agencies, to include the FBI and CISA, on deconflicting and jointly investigating incidents as well as identifying tactics, techniques and procedures (TTPs) that can be shared across sectors to limit widespread exploitation. This occurs formally via detailees, joint task forces, and information systems amongst our headquarters offices, as well as directly between our respective field offices. This deconfliction occurs consistent with relevant agency policies, such as DHS Policy directive 045-04 and PPD-41.



Ransomware 2021

Critical Mid-Year Update

July 2021

Table of Contents

| | |
|---|----|
| Executive summary | 3 |
| Introduction | 4 |
| Ransomware in 2021 YTD | 6 |
| Sanctions risk in ransomware | 10 |
| Case study: Netwalker | 14 |
| Ransom sizes grow | 21 |
| Money laundering and ransomware | 28 |
| Russian-affiliated ransomware | 31 |
| United States ransomware regulatory updates | 33 |
| Conclusion | 40 |

Executive summary

Here's a summary of our key findings and takeaways on ransomware over the last two years:

- **Ransomware is a major growing cybersecurity issue for both the public and private sectors.** Known payments to ransomware attackers rose 344% from 2019 to 2020, when they reached over \$416 million worth of cryptocurrency. Attackers show no signs of slowing down in 2021, and have already taken in more than \$210 million from victims so far this year. It's important to keep in mind that these are low-end estimates, and that the true numbers are almost certainly higher.
- **Ransomware payments can create sanctions risk for victim organizations and companies that help them facilitate payments.** Chainalysis found that 15% of known ransomware payments in 2020 carried sanctions risk. So far, that number is up to 32% in 2021.
- **The average ransom payment has grown significantly.** In Q4 2019, the average ransomware payment we tracked was just \$12,000 worth of cryptocurrency. In Q1 2021, the average payment size was \$54,000. We believe this is due in part to ransomware attackers more effectively targeting larger organizations with the help of illicit, third-party vendors who sell them hacking tools, stolen data, and other assets to carry out more successful attacks.
- **More ransomware attacks appear to be carried out by cybercriminals in Russia and other Commonwealth of Independent States (CIS) countries.** We compared the top ten most prolific ransomware strains in 2020 and 2021, and found that the share of funds extorted by ransomware strains associated with cybercriminals based in Russia or other CIS countries has grown this year.
- **Ransomware money laundering activity is highly concentrated.** Our data shows that in 2020, 82% of cryptocurrency sent by ransomware addresses went to just five cryptocurrency services. That concentration is even more pronounced at the deposit address level. Just 199 deposit addresses received 80% of all funds sent by ransomware addresses in 2020, with an even smaller group of 25 addresses accounting for 46%.
- **The United States government's ransomware policies must continue to evolve.** U.S. government agencies and policymakers have taken positive steps to address the ransomware issue. We examine these steps and make further policy recommendations in this report.

Keep reading to learn about these developments and other key trends in ransomware.



Introduction

When we published our latest [Crypto Crime Report](#) a few months ago, we noted that ransomware was 2020's fastest-growing segment of cryptocurrency-related crime, with victim payments to attackers growing 311% to reach nearly \$350 million worth of cryptocurrency. Since then, Chainalysis joined the Institute for Security and Technology's [Ransomware Task Force](#), alongside other technology providers like Amazon, Cisco, FireEye, McAfee, and Microsoft and government agencies like CISA, FBI, and the Secret Service. Together, the task force put out [a report](#) sizing up the ransomware problem and making recommendations on how governments around the world can address it. We're proud of this work and believe it is a great start in defining the problem and putting solutions in place to tackle it.

However, ransomware has only become more serious in recent months. Since publishing the Crypto Crime Report, Chainalysis has identified more active ransomware addresses and revised our estimate for the total amount of ransomware payments in 2020 to over \$416 million. As we mentioned in our original report, this estimate is a lower bound of the true total, as this only includes payments our team has confirmed, and underreporting means we likely haven't categorized every victim payment in our datasets. Our data improves over time, and so we anticipate this estimate will continue to rise.

Further, ransomware attackers are becoming more sophisticated and more brazen in 2021, commanding larger ransoms from high-profile victims including:

- Airplane manufacturer Bombardier, attacked by [Clon](#)
- Computer maker Acer, attacked by [REvil](#)
- Washington D.C. Police Department, attacked by [Babuk](#)
- Oil pipeline operator Colonial Pipeline Company, attacked by [DarkSide](#)

The ongoing rise in attacks shows that it's more important than ever for governments, cybersecurity practitioners, financial institutions, and cryptocurrency businesses to work together against ransomware. This was recently recognized by the Biden Administration, which [issued an executive order](#) that proposes plans to improve the nation's cybersecurity by modernizing cybersecurity defenses and protecting federal networks, improving information-sharing between the U.S. government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur. We hope this ransomware research report can support those goals. Inside, you'll find updated numbers on overall victim payments and the activity of the most prolific strains, as well as a breakdown of emerging trends and a few policy recommendations that may be helpful to regulators and policymakers.



If your company suffers a ransomware attack, we encourage you to follow the steps [outlined by CISA](#), who may be able to provide specific guidance to help evaluate and remediate ransomware incidents. You can also request threat response assistance by contacting your local [FBI Field Office](#) or [United States Secret Service Office](#). Reporting the incident, which includes providing essential information such as cryptocurrency addresses provided by the attackers, is the only way to ensure law enforcement entities can effectively investigate your attack and, in the long term, understand the scope of the wider ransomware issue so that others are less likely to be attacked in the future.

Thank you,

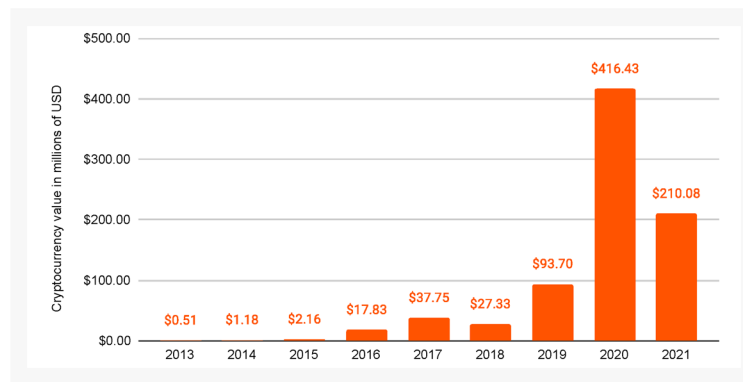
Don Spies
Director of Strategic Initiatives
Chainalysis



Ransomware in 2021 YTD

Ransomware exploded in 2020 and shows no signs of slowing down nearly seven months into 2021.

Total cryptocurrency value received by ransomware addresses | 2016 - 2021 (YTD)



Currencies included: BCH, BTC, ETH, USDT

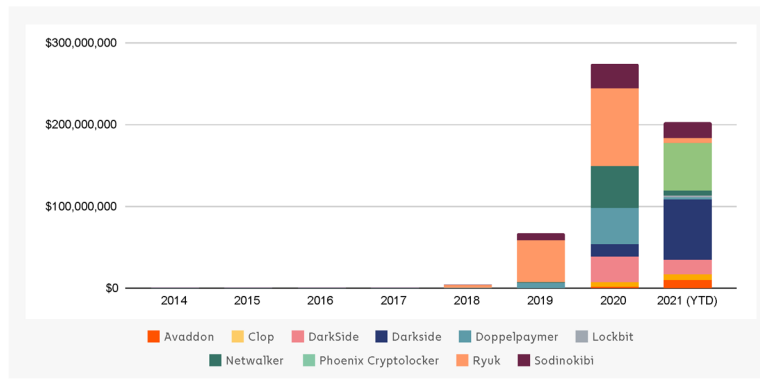
When we published the 2021 Crypto Crime Report in February, blockchain analysis showed that the total amount paid by ransomware victims increased by 311% in 2020 to reach nearly \$350 million worth of cryptocurrency. No other category of cryptocurrency-based crime had a higher growth rate. However, we warned readers that that number was likely a lower bound of the true total. Sure enough, since publishing, we've identified new ransomware addresses with payments we'd yet to count, and now know that ransomware victims paid over **\$416 million** worth of cryptocurrency to attackers in 2020. Again, that number will continue to grow as we discover more ransomware addresses.



As of July 20, 2021, we know that ransomware attackers have taken in at least \$210 million worth of cryptocurrency from victims. Again though, \$210 million must be considered a floor for the time being, as the figure will almost certainly grow as we identify more ransomware addresses.

The increase in ransomware starting in 2020 has been driven by a number of new strains taking in large sums from victims, as well as a few pre-existing strains increasing earnings.

Top 10 ransomware strains by revenue by year | 2014 - 2021 YTD

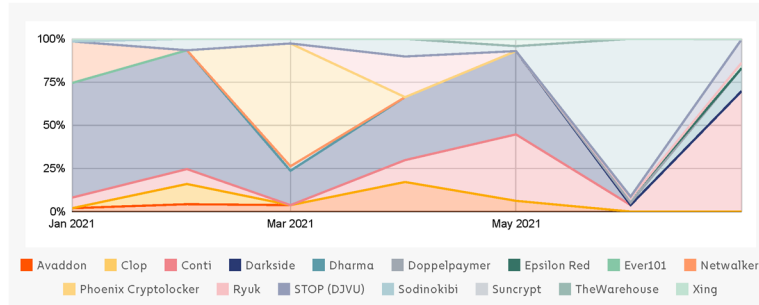


Currencies included: BCH, BTC

Ransomware strains don't operate consistently, even month-to-month. Below, we see that the top-earning strains have ebbed and flowed from the beginning of 2020 to the present, based on our current data and address attributions.



Ransomware lifecycles: Top monthly strains by share of all ransomware payments | 2021 - YTD



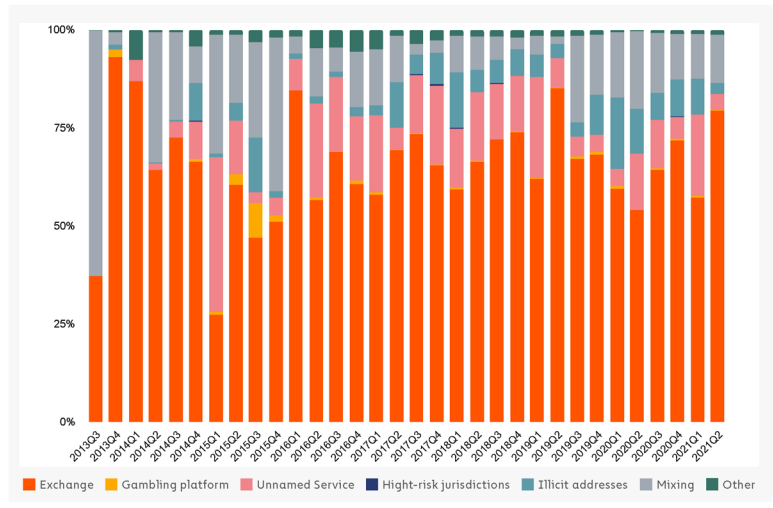
Currencies included: BTC

The number of strains active throughout the year may give the impression that there are several distinct groups carrying out ransomware attacks, but this may not be the case. As we explored in last year's Crypto Crime Report, many strains function on the [RaaS model](#) (Ransomware as a Service model), in which attackers known as affiliates "rent" usage of a particular ransomware strain from its creators or administrators, who in exchange get a cut of the money from each successful attack affiliates carry out.

Many RaaS affiliates migrate between strains, suggesting that the ransomware ecosystem is smaller than one might think at first glance. In addition, many cybersecurity researchers believe that some of the biggest strains may even have the same creators and administrators, who publicly shutter operations of one strain before simply releasing a new, very similar strain under a new name. With blockchain analysis, we can shed light on some of these connections by analyzing how addresses associated with different ransomware strains transact with one another.



Destination of funds leaving ransomware wallets | 2013 Q3 - 2021 Q1



Currencies included: BTC, BCH, ETH

Ransomware attackers move most of the funds taken from their victims to mainstream exchanges, high-risk exchanges (meaning those with loose to non-existent compliance standards), and mixers.



Sanctions risk in ransomware

In October 2020, the U.S. Department of the Treasury's [Office of Foreign Assets Control \(OFAC\)](#) and the [Financial Crimes Enforcement Network \(FinCEN\)](#) released separate advisories related to ransomware payments that could be a sanctions violation for victims or financial intermediaries who facilitate payments for victims. The facilitation point is important, as there is a robust industry of consultants and subject matter experts (SMEs) who help ransomware victims negotiate with, and pay, ransomware attackers. The OFAC alert cited examples of ransomware creators and attackers who have been put on the OFAC sanctions list, such as the [two Iranian nationals](#) who laundered proceeds from the SamSam ransomware strain.

OFAC's alert bolsters [previous government guidance](#) not to pay ransomware attackers, as this incentivizes future attacks. However, OFAC's alert goes a step further in warning that ransomware victims and consultants who help them make payments could face the heavy penalties associated with sanctions violations. It also notes that license applications made to OFAC that involve ransomware payments demanded as a result of malicious cyber-enabled activities would be reviewed by OFAC, but with a presumption of denial.

To some industry members, this appeared to create a "catch-22" where ransomware victims were forced to choose between paying the ransom and possibly suffering an additional penalty in the form of OFAC sanctions, or not paying the ransom and suffering the loss of their data and the resulting financial and reputational harm. It also arguably created a disincentive for ransomware victims to do their due diligence in determining whether a ransomware payment would, in fact, open the victim or its financial intermediary to OFAC sanctions based on the attacking strain.

But how big is the sanctions violation risk in ransomware payments? We looked back at all ransomware payments Chainalysis has tracked since 2016 and calculated the percentage of payment volume that was associated with known sanctions risks, as defined below.

We counted all known ransomware payments that meet any of the three criteria below as constitutive of sanctions violation risk:

- Payments to addresses identified by OFAC as belonging to sanctioned individuals (note: this includes payments made before the addresses were actually sanctioned).
- Payments to addresses connected to ransomware strains whose creators have been sanctioned by OFAC.



- Payments to addresses connected to ransomware strains associated with cybercriminals based in heavily sanctioned jurisdictions such as Iran and North Korea.

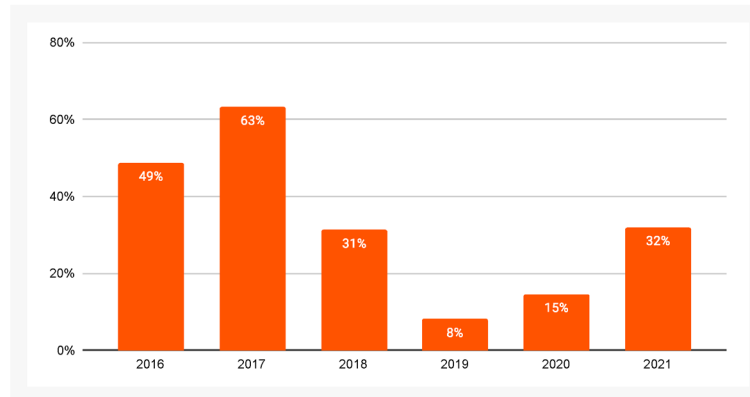
Those criteria cover the following ransomware strains:

| Strain | Description |
|--------------|--|
| SamSam | OFAC designated cryptocurrency address |
| Ouroboros | Linked to Iranian actors |
| VoidCrypt | Linked to Iranian actors |
| Sorena | Linked to Iranian actors |
| Pay2Key | Linked to Iranian actors |
| WannaCry 1.0 | Linked to North Korean actors |
| WannaCry 2.0 | Linked to North Korean actors |
| NotPetya | Associated with sanctioned actors in Russia. |
| CryptoLocker | Associated with sanctioned actors in Russia. |
| Bitpaymer | Speculated to be associated with sanctioned group Evil Corp. |
| Locky | Speculated to be associated with sanctioned group Evil Corp. |
| Doppelpaymer | Speculated to be associated with sanctioned group Evil Corp. |
| WastedLocker | Speculated to be associated with sanctioned group Evil Corp. |
| Hades | Speculated to be associated with sanctioned group Evil Corp. |

Based on those designations, we found that 15% of all known ransomware payments made in 2020 and 32% of those made so far in 2021 carried a risk of sanctions violations. Our 2021 estimates have grown significantly since we first published this report on May 14, following the identification of a few large payments to Phoenix CryptoLocker, a strain speculated to be associated with Evil Corp.



Share of known ransomware payments associated with OFAC designations and other sanctions risk | 2016 - 2021 (YTD)



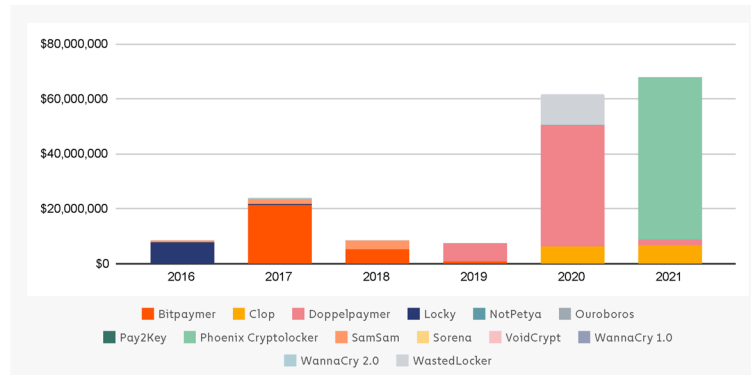
Currencies included: BCH, BTC, ETH, USDT

Because overall ransomware payments increased in 2020, the dollar figure for ransomware payments with sanctions risk skyrocketed last year, and is on pace to grow again in 2021. Again, it's worth noting that nearly all 2021 payments to ransomware strains with sanctions risk are composed of a few large payments to Phoenix CryptoLocker. We could see increases in ransomware payments with sanctions risk if Phoenix CryptoLocker continues to carry out successful attacks, if emerging strains receiving payments are connected to potential sanctions nexuses, or if OFAC were to designate additional addresses. For instance, we've noticed that some Iranian strains have resurfaced recently under new names to disguise their connections to organizations and individuals with sanctions risk. This makes ransomware payment due diligence using blockchain analysis solutions even more critical, as the ability to determine actual sanctions risk improves while the amount of risk in each payment remains low.



Below, we show the yearly volume of known ransomware payments that constitute sanctions violation risk, broken down by strain.

Total value received by ransomware addresses associated with sanction risk by ransomware strain | 2016 - 2021



Currencies included: BCH, BTC

Nearly all of the known ransomware payments with sanctions risk in 2020 and 2021 went to Doppelpaymer and WastedLocker. In previous years, Bitpaymer, SamSam, and Locky have also been responsible for a high volume of ransomware payments associated with sanctions risk. We should also note that there are reports of increased activity from Iranian ransomware strains with sanctions risk in 2021, though our data doesn't yet confirm this trend.

Dealing with a ransomware attack is incredibly stressful. In cases where hospitals and other critical infrastructure systems have been attacked, lives have been at risk where computer systems were rendered inoperable. It is imperative that businesses and government entities prepare in advance so that during a stressful situation, a plan is already in place. Having a ransomware response plan that includes working with SMEs, who can coordinate with law enforcement and perform the necessary blockchain analytics on proposed payments to avoid sanctions violations, is critical. Further policy recommendations around ransomware and sanctions risk are provided below.



Case study: Netwalker

Earlier this year, the U.S. Department of Justice (DOJ) [announced](#) a coordinated international law enforcement action to disrupt the Netwalker ransomware strain, including the seizure of nearly half a million dollars in cryptocurrency, the disablement of a dark web resource used to communicate with Netwalker ransomware victims, and the arrest of a Canadian national, Sebastien Vachon-Desjardins, who obtained tens of millions of dollars by acting as a Netwalker affiliate.

This case highlights the sophistication with which Netwalker operated, the global impact of ransomware attacks, and the substantial funds ransomware actors steal from their victims.



Seizure page of dark web hidden resource used to communicate with Netwalker ransomware victims.

Source: [U.S. Department of Justice](#)

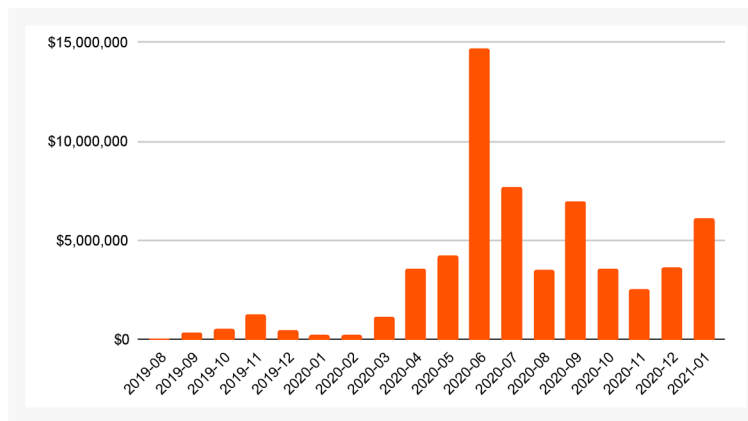


Below, we'll break down what blockchain analysis tells us about the Netwalker strain of ransomware and highlight specific elements of the investigation to show how law enforcement was able to trace the illicit funds.¹

Like many strains, Netwalker functions on the [\(RaaS\) model](#), in which attackers known as affiliates "rent" usage of a particular ransomware strain from its creators or administrators, who in exchange get a cut of the money from each successful attack affiliates carry out. RaaS has led to more attacks, making it even more difficult to quantify the full financial impact. But the trend is clear; no other category of cryptocurrency-based crime had a higher growth rate than ransomware in 2020.

Netwalker was a top ransomware strain by revenue in 2020, along with Ryuk, Maze, Doppelpaymer, and Sodinokibi. Chainalysis has traced nearly \$94 million worth of funds in Netwalker ransoms, with payment dating back to 2018. It picked up steam in mid-2020, growing the average ransom to \$33,000 last year, up from \$7,000 in 2019. Payments stopped after the strain was taken down in late January of 2021.

Ransomware payments received by Netwalker | Monthly



¹Chainalysis has a policy against commenting on active law enforcement cases prior to adjudication. However, an exception was made in this case after consultation and approval from our law enforcement partners.



According to U.S. authorities, Netwalker has impacted at least 305 victims from 27 different countries, including 203 in the U.S.

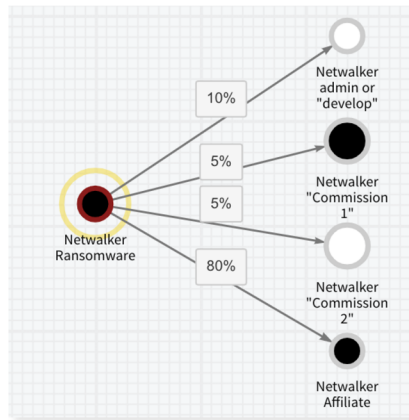
Hundreds of Netwalker victims around the world



Chart created by Chainalysis with support and approval from law enforcement partners

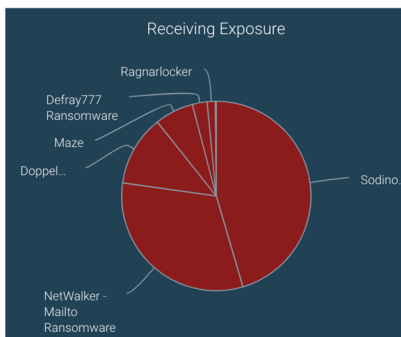
What blockchain analysis tells us about Netwalker operations and financials

Typically, there are four roles that receive proceeds from Netwalker attacks: the likely administrator or developer (8-10%), the affiliate (76-80%), and two commissioned roles (2.5%-5% each). An affiliate, like Vachon-Desjardins, is usually responsible for obtaining access to the victim network and deploying the malware. There are also cases when one wallet gets 100% of the payment, which we believe belongs to the Netwalker administrator and indicates that he or she may also be directly involved in some of the attacks.



This screenshot of Chainalysis Reactor shows the typical transfer of funds from the ransom payment address to the different Netwalker actors.

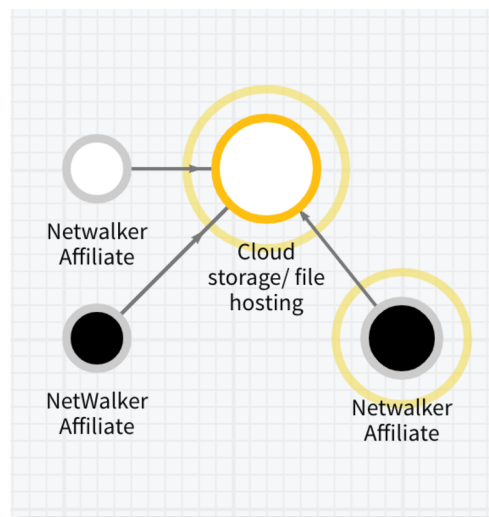
Blockchain analysis reveals that there were actually fewer than 20 unique affiliates. Of those affiliates, some rarely deployed Netwalker. Some moved on to other RaaS strains, and we can use the Chainalysis Reactor exposure wheel to show that some affiliates have received payments from other variants.





The Netwalker administrator, who goes by the moniker “Bugatti” on darknet forums, posted an advertisement in May 2020 on a forum seeking additional Russian-speaking affiliates as vacancies had “freed up,” which confirms our assessment of affiliates migrating to other strains.

Blockchain analysis can also show ransomware actors paying for services they need to operate their criminal enterprise. For example, we can see below that Netwalker actors paid for cloud storage hosting with cryptocurrency, likely used to host stolen victim data for further extortion. Indeed, Netwalker ramped up its extortion efforts [in May 2020](#) by not only locking victims out of their data, but also by stealing it. Before encrypting computer files on a victim’s network, Netwalker actors began to steal the data and automatically publish victim data on a leak site if the ransom was not paid by the deadline, another growing trend among several ransomware strains.





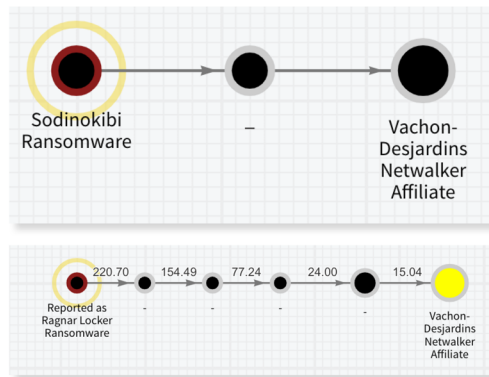
How authorities used blockchain analysis to trace the flow of Netwalker funds

According to the indictment unsealed this past January, Vachon-Desjardins was charged with intentional damage to a protected computer and transmitting a demand in relation to it. This involved a Netwalker ransomware attack against a victim company located in Florida.

Blockchain analysis revealed at least 345 addresses associated with Vachon-Desjardins going back to February 2018 with transactions continuing through late January of 2021. He allegedly received more than \$14 million worth of Bitcoin at the time of receipt of the funds, ultimately possessing at least \$27.6 million given its rising value.

According to government partners, Vachon-Desjardins was involved in at least 91 attacks using Netwalker ransomware since April 2020, deploying the malware as an affiliate and receiving 80% of the ransom.

In addition to Netwalker, we suspect Vachon-Desjardins was involved in the deployment of other RaaS strains like Sodinokibi, Suncrypt, and RagnarLocker. This is relatively common; we often see affiliates migrate to different strains over time. Additionally, the Netwalker admin Bugatti has listed proof of prior hacking experience as a prerequisite to become a Netwalker affiliate, so it would make sense that affiliates like Vachon-Desjardins would have a track record.





The Chainalysis Reactor graphs above show Netwalker affiliates with exposure to Sodinokibi and Ragnar Locker ransomware strains.

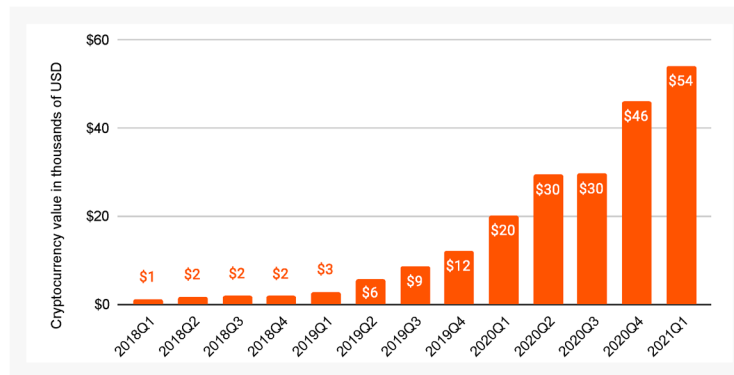
Affiliate overlap is an important phenomenon for authorities to understand in the fight against ransomware, as it suggests a relatively small number of attackers driving the issue despite the many strains active at any given time. This, along with our [previous research](#) showing that a small group of service deposit addresses receive most funds stolen in ransomware attacks, suggest that law enforcement can significantly reduce ransomware activity by disrupting a relatively small group of attackers and money laundering service providers.



Ransom sizes grow in 2021

One key trend we've observed starting in 2020 is the drastic growth in the size of the average known ransomware payment.

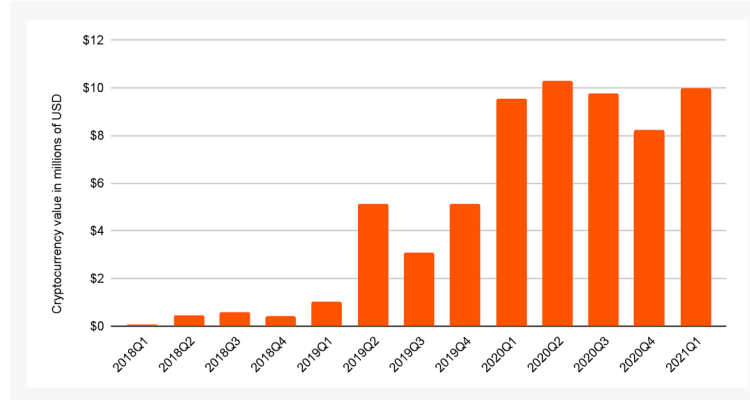
Average known payment to identified ransomware strains by quarter | 2018 - 2021 Q1



The average known ransomware payment has more than quadrupled from \$12,000 in Q4 2019 to \$54,000 in Q1 2021. News stories have highlighted much larger outlier ransoms, such as the [\\$50 million](#) ransom payment that REvil demanded from computer parts manufacturer Acer earlier this year, though it's unclear if Acer paid. While we've yet to observe payments of that size, the largest observed ransom payment per quarter has grown substantially over the last two years.



Largest known payments to identified ransomware strains by quarter | 2018 - 2021 Q1



Prior to Q1 2020, we never saw a ransomware payment above \$6 million, but since then have seen at least one per quarter.

These rises in ransom payment sizes coincide with an increase in payments from ransomware addresses to other illicit addresses associated with ancillary ransomware services. Illicit third-party services refer to a number of providers, some of whom operate explicitly as criminals, who can help cybercriminals carry out larger, more effective attacks. These tools, many of which are available on darknet markets, include:

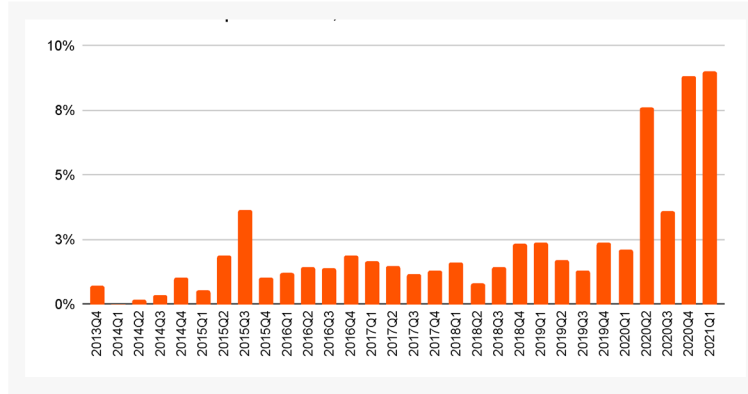
- Infrastructure as a Service providers.** Ransomware attackers need cyber infrastructure such as [bulletproof web hosting](#), domain registration services, botnets, proxy services, and email services to carry out attacks. Additionally, many rely on cloud hosting and other forms of infrastructure to carry out data exfiltration attacks, which refers to a new strategy in which ransomware attackers leak data stolen from victims in an effort to force faster and larger payments. We see an example of this in the [ongoing attack](#) on the Washington, D.C. police force, reportedly by the ransomware group Babuk. Babuk has released the personal information of several D.C. police officers since the attack began in order to put pressure on the department.



- **Hacking tools and access providers.** Ransomware attackers may purchase network access to victims who have already been compromised under a framework known as Access-as-a-Service. Others will buy tools to help them break into victims' networks themselves. One example is exploit kits. Exploit kits scan for vulnerabilities to establish an initial foothold on the network or deploy a payload like ransomware. These exploits make it possible for ransomware attackers to go after larger organizations with more advanced cybersecurity, who can typically afford higher ransoms than less sophisticated organizations. Another example would be malware as a service, which allows cybercriminals to lease software to distribute ransomware more effectively.
- **Fraud shops.** Fraud shops also play an important role in ransomware operations. Fraud shops are a subset of darknet markets that sell stolen data, including passwords and personally identifying information (PII) for many individuals, and even compromised RDP credentials used to gain access to a victim's network. Similar to the exploits and access described above, this information can help ransomware attackers break into victims' computer networks.
- **Post-attack services:** Some Ransomware and RaaS have adopted enhanced methods of extortion, such as hiring underground call centers to call victims directly, and layering in DDoS attacks on victims refusing to pay, likely leased through DDoS-as-a-Service providers. Ransomware administrators are even paying for salaried employees to help victims through the ransom payment process, including professional negotiators.

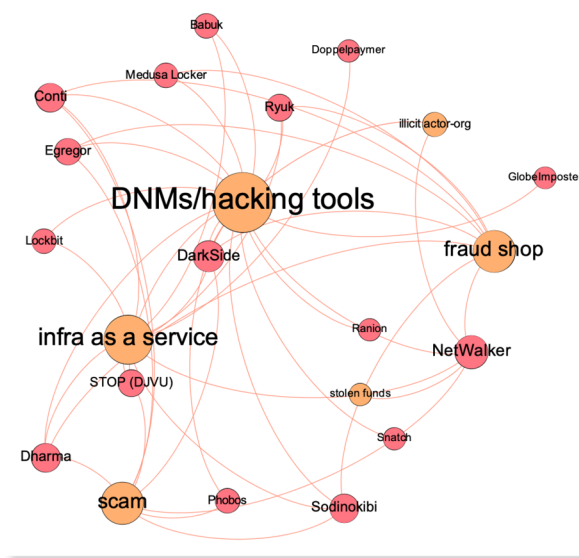


Share of ransomware funds going to illicit third-party providers
 | Q4 2013 - Q1 2021



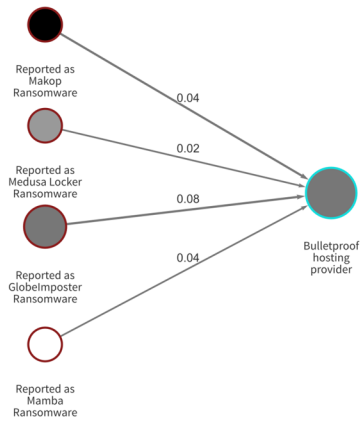
Prior to 2020, illicit third-party services rarely accounted for more than 3% of funds sent from ransomware addresses. Since then, they've increased significantly, often accounting for as much as 9% of spending. Keep in mind too that from 2020 on, the raw total of funds sent from ransomware addresses has increased significantly, meaning these figures represent significant increases in dollars spent on illicit services by ransomware attackers.

All of these third-party vendors enable ransomware attackers to target bigger organizations more effectively, and their increasing usage could be one reason for the higher ransom payments we've been seeing since 2020. Blockchain analysis reveals that these illicit service providers have become the connective tissue of the ransomware ecosystem. In the network chart below, for instance, we show how different types of providers in the aggregate connect many of the most prolific ransomware strains based on cryptocurrency transaction history.

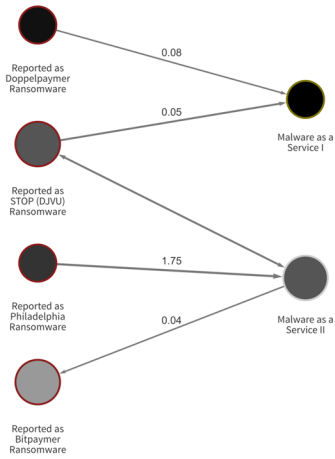


Red bubbles represent individual ransomware strains, while orange bubbles represent aggregated groups of services in the labeled category.

The Chainalysis Reactor graphs below provide more granular examples of this phenomenon. In the first, we see multiple ransomware strains sending funds to a popular bulletproof hosting provider.



In the second, we see other strains transacting with two Malware as a Service providers.





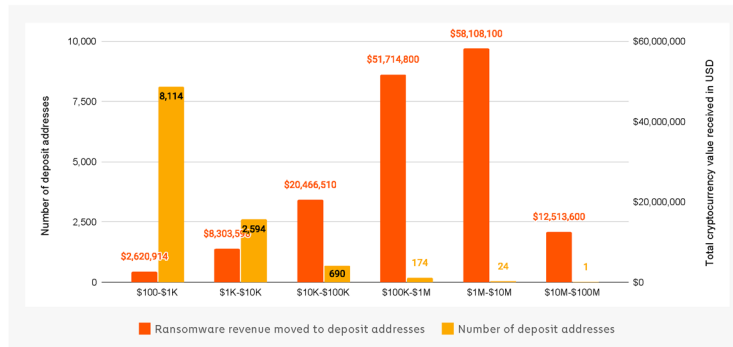
If ransomware attackers continue to have access to advanced infrastructure and tools provided by third-party vendors, we expect ransom payment sizes to continue increasing. Law enforcement and cryptocurrency businesses must work together to take down not just the attackers themselves, but also the providers of tools facilitating attacks.



Money laundering and ransomware

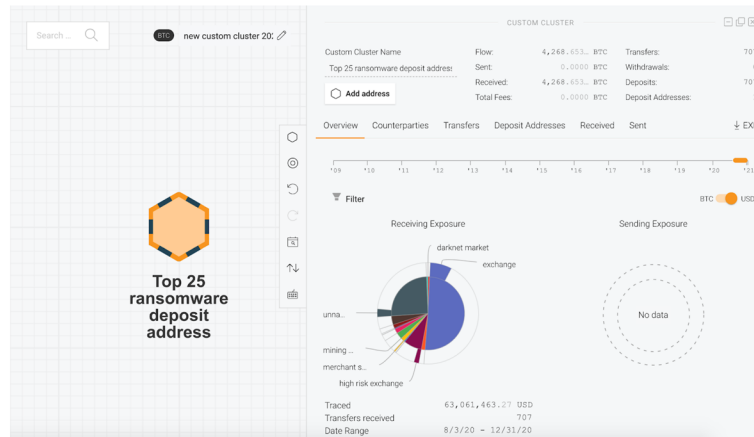
Most funds sent from ransomware addresses go to cryptocurrency exchanges. This activity is relatively concentrated to just a few services – in 2020, a group of just five receives 82% of all ransomware funds. But what about when we look at the deposit address level?

Total criminal value received by deposit addresses by ransomware risk bucket vs. Number of deposit addresses per ransomware risk bucket | 2020



Accounts are bucketed by range of total value received from ransomware addresses. Each orange bar represents the total amount ransomware addresses sent to all addresses in the corresponding bucket, while each blue bar represents the number of individual deposit addresses in the bucket. Currencies included: BTC.

The data shows that ransomware money laundering is even more concentrated at the deposit address level. **Just 199 deposit addresses received 80% of all funds sent by ransomware addresses in 2020. An even smaller group of 25 addresses accounted for 46%.** Below, we look more closely at the addresses receiving the most from ransomware, and in particular the share of their total activity that's devoted to ransomware.



Please note that Chainalysis Reactor doesn't show sending activity for service deposit addresses, as services often move the funds received to their own internal addresses as needed. This means that tracing funds through service addresses can produce misleading results.

This deposit address belongs to a nested service hosted at a large, international cryptocurrency exchange and has been active since August 3, 2020. Between that date and the end of 2020, it received over \$63 million worth of Bitcoin in total. Most of it appears to be non-illicit activity – nearly half of those funds come from other mainstream exchanges, though a quarter comes from unknown services that may be identified as linked to criminal activity at a later date. However, while the share is low, the address has still received over \$1 million worth of Bitcoin from ransomware addresses, as well as \$2.4 million from multiple scams. Overall, criminal activity accounts for 10% of the address' total cryptocurrency received. Most of the other deposit addresses on our scatter chart with low shares of total funds coming from ransomware fit a similar profile.

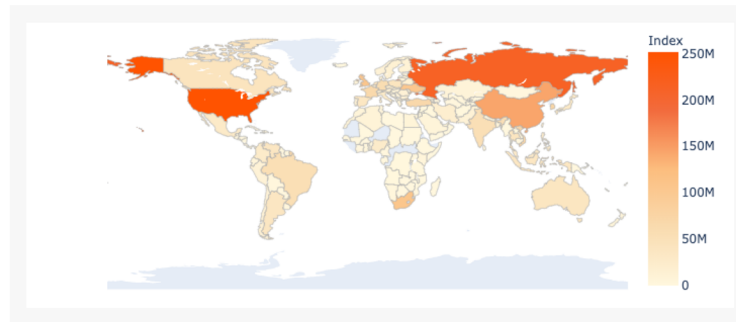
The data shows that money laundering of ransomware proceeds is heavily concentrated, not just at the service level, but even more so at the deposit address level. This suggests that a relatively small group of individuals and money laundering service providers is responsible for this activity. Law enforcement could put a huge dent in ransomware operators' ability to convert funds into cash by disrupting those in control of the deposit addresses responsible for the most money laundering.



More ransomware attacks from Russian-affiliated cybercriminals

As we covered above, many ransomware strains are associated with sanctioned cybercriminal groups based in or affiliated with Russia, such as the notorious Evil Corp, whose leadership reportedly has [ties to the Russian government](#). Generally speaking, cybercriminals affiliated with Russia and other Russian-speaking countries in the Commonwealth of Independent States (CIS) — an intergovernmental organization of former Soviet countries — have been among the most prolific in the world. Russian-affiliated services [received more cryptocurrency](#) from illicit addresses than those in any other country, suggesting that Russian-affiliated cybercriminals were the year's biggest financial beneficiaries of cryptocurrency-based crime. Much of this activity was [driven by Hydra](#), a Russia-based darknet market, which in addition to drugs sells stolen data that can be useful to ransomware attackers.

Destination of funds leaving illicit services | 2020



In 2021, ransomware strains associated with Russia and other CIS countries are accounting for a larger share of overall ransomware activity. We show this on the graph below by comparing activity in 2020 and 2021 for two categories of ransomware strains:

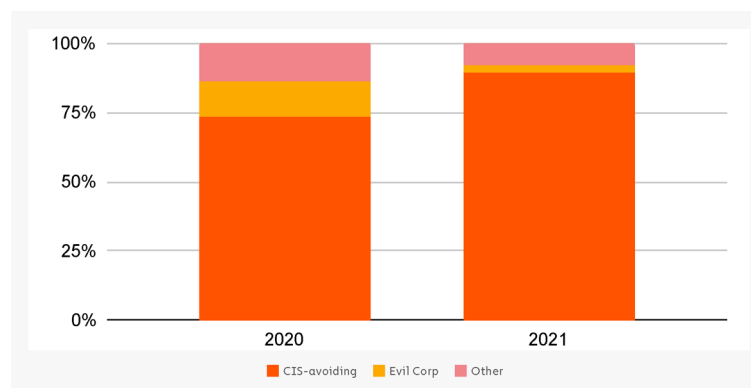
- Strains associated with Evil Corp.



- Strains with code that prevents encryption if the ransomware detects the victim's operating system is located in a CIS country. These strains can generally be assumed to have originated in Russia or other CIS countries.

The numbers are clear: Taken together, these ransomware strains are accounting for more activity in 2021 compared to 2020.

Share of ransomware proceeds: 2020 vs. 2021



Please note: This graph reflects the total amount of ransomware activity accounted for by the ten most prolific strains in 2020 and 2021. While this excludes many individual strains, it still reflects the majority of activity in both years.

In 2020, roughly 86% of ransomware proceeds studied could be attributed to ransomware strains that are either associated with Evil Corp or are designed to avoid CIS countries. So far in 2021, that figure is at 92%.

The U.S. government is already taking the threat of Russian cybercrime seriously, as President Biden [announced several new sanctions](#) against Russian groups and individuals following the SolarWinds hack earlier this year. The data on ransomware specifically suggests that blockchain analysis, as well as collaboration with other firms throughout the cryptocurrency industry, will be crucial to fighting cybercrime from groups aligned with Russia and other hostile nation states.



United States ransomware regulatory updates

As instances of ransomware have increased over the past few years, regulators and law enforcement have taken notice and issued guidance. As mentioned earlier, two bureaus within the U.S. Department of the Treasury– the [Office of Foreign Assets Control](#) (OFAC) and the [Financial Crimes Enforcement Network](#) (FinCEN)– issued advisories related to facilitating ransomware payments. [OFAC's advisory](#) focused on the potential sanctions risks associated with ransomware payments, while [FinCEN's advisory](#) highlighted that the facilitation of ransomware payments may trigger FinCEN registration and Bank Secrecy Act (BSA) requirements and discussed financial red flag indicators of ransomware and associated payments.

Neither of these advisories includes major changes to the U.S. government's guidance; regulators and law enforcement have consistently stated that paying ransoms only encourages bad actors to make future ransomware payment demands. But they do make it clear that ransomware victims and those who facilitate payments on behalf of victims can be found in violation of sanctions violations and/or the BSA.

Ransomware victims, third party intermediaries that facilitate ransomware payments such as digital forensics and incident response companies and cyber insurance companies, cryptocurrency exchanges, and financial institutions should take a risk-based approach to managing responses to ransomware on behalf of themselves and their customers.

Here we break down the key takeaways from the OFAC and FinCEN advisories and point out where and how blockchain analysis can help mitigate risk of sanctions violations when making ransomware payments and ensuring compliance with BSA obligations.

OFAC [advisory](#) on potential sanctions risks for facilitating ransomware payments

OFAC has [designated](#) many malicious cyber actors, including perpetrators of ransomware attacks and those who facilitate ransomware transactions. U.S. persons are prohibited from engaging in transactions, directly or indirectly, with individuals or entities on OFAC's [Specially Designated Nationals and Blocked Persons List \(SDN List\)](#) and those covered by comprehensive country or region embargoes. A threat actor demanding a ransomware payment may be sanctioned or otherwise have a sanctions nexus, which means that ransomware victims, or those facilitating payments on their behalf, must conduct the appropriate due diligence before



making ransomware payments in order to avoid violating OFAC regulations. OFAC makes several important clarifications in their advisory:

1. Facilitating ransomware payments on behalf of a victim may violate OFAC sanctions.

Third party ransomware facilitators and cryptocurrency exchanges could be in violation of sanctions if they facilitate a payment to a sanctioned actor.

For example, Garmin reportedly [used](#) a third party to pay the WastedLocker ransomware demand rather than paying it directly. In this case, WastedLocker ransomware is believed to be a variant developed by Evil Corp, a designated entity. Blockchain analysis tools, including Chainalysis Reactor, can help victims and those working on their behalf identify cryptocurrency wallets associated with specific ransomware variants and OFAC designated actors to avoid making payments in violation of sanctions.

The Evil Corp example also underscores the importance of understanding the various strains that designated entities run over time. OFAC originally sanctioned Evil Corp for its development and distribution of the Dridex strain, which was largely active in late 2015 and early 2016 before the group moved to other variants such as WastedLocker. It is therefore important to keep up with known variants that were operated in the past by an entity on the [SDN List](#), as well as any new ones they begin to operate. One of the best ways to understand this connectivity is by using blockchain analysis to investigate where payments intersect. Blockchain analysis will provide insight into payment connections between strains and alert victims and those working on their behalf so they can avoid making payments to sanctioned addresses and individuals.

2. Addresses and individuals covered by comprehensively sanctioned jurisdictions are also applicable.

OFAC's advisory not only covers entities on their SDN list, but also comprehensive country or region [embargoes](#) (e.g. Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria), as malicious cyber activities may enable criminals and adversaries in these jurisdictions to profit and advance their illicit aims or threaten U.S. national security interests. It can be difficult to determine where entities are located based on their cryptocurrency wallets or addresses. However, using blockchain analysis tools, it is possible to see where a cryptocurrency deposit address is located at an exchange or has interacted with an exchange, and to review that exchange's jurisdictional information to see whether they are located in a comprehensively sanctioned jurisdiction. Blockchain analytics is imperative for this research.



3. OFAC will review licensing applications involving ransomware payments on a case-by-case basis with a presumption of denial.

OFAC has a licence application [process](#) by which it is possible to apply to receive authorization from OFAC to engage in a transaction that otherwise would be prohibited. However, this advisory makes clear that licence applications involving ransomware payments as a result of malicious cyber-enabled activities will probably not be approved.

4. Self-initiated, timely, and complete reports of a ransomware attack to law enforcement will be considered a significant mitigating factor if the situation is later determined to have a sanctions nexus.

OFAC also notes in the advisory that if a victim of a ransomware attack reports the attack to law enforcement, they will consider the “self-initiated, timely, and complete report” to be a significant mitigating factor if the situation is later determined to have a sanctions nexus when OFAC considers appropriate enforcement outcomes. They will also consider the victim’s full and timely cooperation with law enforcement during and after the attack. Because effort is measured in relation to possible violations, it is important to work directly with law enforcement, OFAC, and FinCEN to ensure compliance with all of the appropriate obligations.

FinCEN advisory on ransomware and the use of the financial system to facilitate ransom payments

FinCEN’s advisory provides important information on the role of financial intermediaries in the processing of ransomware payments, trends and typologies of ransomware and associated payments, ransomware-related red flag indicators, and information reporting and sharing. Typically, because ransomware attackers demand ransom be paid in cryptocurrency, processing ransomware payments usually involves at least one depository institution and one or more money service businesses (MSB). Upon receipt of the ransom, the attacker will launder the funds, integrating it back into the financial system. Because of this, the financial sector can play a critical role in identifying ransomware payments and financial institutions can play an important role in protecting the U.S. financial system from ransomware threats through compliance with their BSA obligations. Here are three important takeaways from the FinCEN advisory:



1. Third-party ransomware facilitators like DFIR companies and CICs might be engaged in MSB activities.

Digital forensics and incident response (DFIR) and cyber insurance companies (CICs) that facilitate ransomware payments on behalf of their customers to ransomware attackers by converting their customers' fiat currency into cryptocurrency may be engaged in MSB activities (such as money transmission). This would trigger FinCEN registration and BSA requirements, including filing Suspicious Activity Reports (SARs). It is likely SAR filing reporting requirements would be triggered by every payment they process to ransomware attackers.

The applicability of this guidance to DFIR companies and CICs would depend on whether payments were made directly, or whether they walked their customer through the process or connected them with someone who paid on their behalf.

Any DFIR company or CIC making ransomware payments on behalf of customers should be aware of any OFAC-related obligations related to that activity as well, as outlined above.

2. FinCEN considers a link between a customer's cryptocurrency wallet and ransomware activity to be a red flag indicator.

FinCEN identified several financial red flag indicators of ransomware-related illicit activity to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with ransomware attacks. Many of these red flags and typologies are associated with cryptocurrency, or convertible virtual currency (CVC), activity.

In particular, red flag #3 is "*a customer's CVC address, or an address with which a customer conducts transactions, appears on open sources, or commercial or government analyses have linked those addresses to ransomware strains, payments, or related activity.*" Blockchain analysis is required to identify this in most circumstances.

3. It still isn't clear if it's illegal to pay ransom if the entity is not sanctioned.

While we are still lacking clarity around the legality of paying ransom if the entity isn't sanctioned, what is clear is that operating as a money transmitter/MSB and not registering or filing SARs violates the BSA.



The recent OFAC and FinCEN advisories clarify two important regulatory grey areas: (1) there are potential sanctions issues associated with ransom payments, and licenses probably will not be granted and (2) companies facilitating ransom payments may need to register with FinCEN and file SARs. Blockchain analysis tools will be critical in enabling financial institutions, MSBs, and others to be compliant with regulatory guidance.

The FBI's Internet Crime Complaint Center (IC3) issued an [advisory](#) on common types of ransomware, how to minimize ransomware risks, and how to report attacks. CISA stood up a [campaign](#) focused on reducing the risk of ransomware and has [released](#) a number of guides and other resources focused on raising awareness and helping the public and private sectors mitigate ransomware risks. USSS Cybercrime Investigations has also released a [guide](#) to ransomware outlining how to prepare against, prevent, and respond to a ransomware attack.

U.S. ransomware policy recommendations

Given the recent increase in ransomware attacks, as well as their potentially devastating impacts, Chainalysis believes it is important to enact meaningful policies to deter, detect, and disrupt ransomware. The foundation of these policies must be a comprehensive, whole-of-U.S. government strategy for reducing ransomware attacks. Recently, positive efforts were spearheaded by the White House as President Biden [issued an Executive Order](#) on May 12th to improve U.S. cybersecurity (the "Executive Order"). We laud any efforts towards promoting and implementing a cohesive cybersecurity policy. We believe that clear guidance and direction from the President will enable a unified inter-agency response and facilitate government agencies to work more effectively with the private sector to combat this important issue and protect U.S. national security interests. This threat is too big for one agency or entity to attack themselves -- it must be a concerted joint public-private effort with strong, unequivocal leadership. We outline below some specific policies that Congress and government agencies should consider when determining future legislation and strategies necessary to combat ransomware.

Update and strengthen cyber hygiene regulations and standards

Current cybersecurity regulations and standards in the United States do not specifically address ransomware in a manner that would meaningfully prevent these attacks. The Executive Order will improve cybersecurity standards at the Federal level. This will be vital to improving our national security. It is also important that cybersecurity standards for private sector and non-profit businesses be updated and strengthened, in order to prevent the sorts



of ransomware attacks we have seen cripple our critical infrastructure, healthcare systems, schools, and private businesses. Regulations should be reviewed and updated, and legislation enacted if needed, to incorporate measures that would more directly mitigate ransomware attacks. One mechanism to consider, given how quickly this threat and technology progress compared to the process for updating laws and regulations, would be for Congress to mandate standards be set through a private- or public-sector standards body that reviews and sets minimum required cybersecurity standards on an annual basis.

Improve information sharing

In order to disrupt the existing ransomware ecosystem, public-private information sharing could be improved and incentivized. Information is not currently shared in a consistent or reliable manner, and it does not always reach a broad enough audience. There is also currently underreporting of ransomware events, which obfuscates the true scope of the issue and means that law enforcement does not have all of the necessary information to prioritize and investigate ransomware events.

Campaigns educating the general public and the private sector about ransomware attacks, how they can be prevented, and encouraging the reporting of events could be developed. In conjunction with these campaigns, mechanisms for sharing information related to ransomware incidents could be developed. The development of information sharing networks, both within the government, and between the government and the private sector, would improve the quality and volume of information about ransomware incidents. It may be worth considering a standard format for ransomware incident reporting to promote consistency, or providing suggested fields to include, such as cryptocurrency wallet addresses, transaction hashes, and ransom notes. Incentives could be put in place to facilitate information sharing between the private sector, financial institutions and MSBs, law enforcement, and regulators.

The Executive Order removes barriers to threat information sharing between government and the private sector, and is an important start. However, it does so through proposed revisions to government contracting language that would only impact businesses contracting with the federal government. Congressional action that regulates or incentivizes private companies to share intelligence about ransomware actors with law enforcement, by removing legal barriers and requiring providers to share breach information, is critical. Additionally, regulatory advisories to the private sector that include information about ransomware threat actors' tactics and techniques, indicators of compromise, and other ransomware trends would also allow the private sector to better identify and protect itself against potential attacks, as well as raise awareness, which would likely promote increased reporting. Increased information



sharing would also better enable investigators to prioritize incidents and the private sector to prepare themselves and improve their security measures against ransomware incidents.

Increase investigative resources

In order to comply with Treasury Department regulatory guidance on ransomware payments, ransomware victims must report attacks to law enforcement. If victims want to pay ransom to a sanctioned address, individual, or entity, they must apply for a license from OFAC. It will be critical that regulators and law enforcement have the tools and resources they need to conduct compliance checks and investigations into ransomware attacks. Ransomware is usually paid in cryptocurrency, so blockchain analysis tools are a vital tool in the investigator's toolkit.

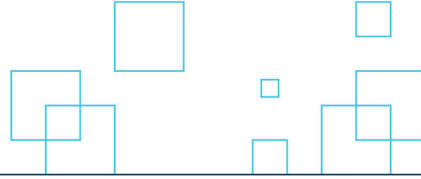
Using blockchain analysis tools, regulators can confirm compliance with regulatory guidance and law enforcement can trace the ransom paid in cryptocurrency to attackers to its cashout points at cryptocurrency exchanges. Law enforcement can serve subpoenas to these cryptocurrency exchanges, which are required to register as money service businesses here in the United States and collect Know Your Customer (KYC) information from their customers. In their response to legal process, the exchange will provide any identifying information that they have related to the cryptocurrency address, such as name, address, and government identification documentation, to law enforcement, allowing them to further their investigation.

Conclusion

The importance of more comprehensive and standardized information gathering in ransomware investigations, whether provided by victims or gathered by law enforcement, cannot be understated. This may require Congress, Federal agencies, or State and Local governments to remove legal barriers and potentially provide incentives for public and private sector entities to be able to report ransomware incidents without fear of additional damages. Ransomware is a crime that can threaten every aspect of our lives, from infrastructure and commerce, to national security risks. And while some argue that the nature of cryptocurrency facilitates the crime of ransomware, its nature also facilitates incomparable visibility that benefits law enforcement immensely. By incentivizing and encouraging the reporting of cryptocurrency addresses that are associated with known threat actors, and by providing the resources necessary to understand and combat them, law enforcement and the U.S. government as a whole will be able to do more comprehensive analysis of ransomware attacks, provide better threat prevention assistance to the public, and protect the country from national security risks.



Building trust in blockchains



STATEMENT FOR THE RECORD OF THE
CHAMBER OF DIGITAL COMMERCE
HEARING BEFORE THE SENATE JUDICIARY COMMITTEE
JULY 27, 2021

“America Under Cyber Siege: Preventing and Responding to Ransomware Attacks”

The Chamber of Digital Commerce is the world’s leading trade association representing the digital asset and blockchain industry. The Chamber’s mission is to promote the acceptance and use of digital assets and blockchain-based technologies. Through education, advocacy, and working closely with policymakers, regulatory agencies, and industry, our goal is to develop an environment that fosters innovation, jobs, and investment. Members of the Chamber provide blockchain analytics and other services to industry and government that have been used to trace the flow of cryptocurrency payments, including those made as a result of ransomware attacks.

The Chamber of Digital Commerce co-founded the Blockchain Alliance, which works closely with key law enforcement agencies around the globe. The Blockchain Alliance is a public-private forum that enables the blockchain community and law enforcement to work together to help combat criminal activity. It is comprised of 20+ state, federal and international law enforcement agencies. This forum serves as a resource for law enforcement and regulatory agencies by providing educational resources, technical assistance, and periodic informational sessions regarding the use of blockchain-based technologies.

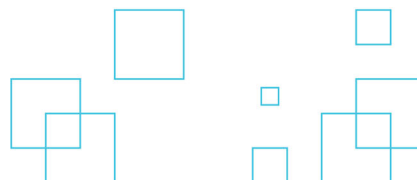
Ransomware is not a cryptocurrency and blockchain problem

Ransomware may be defined as a type of malicious software designed to block access to a computer system until a sum of money is paid. Ransomware attacks on information infrastructure date to at least 1989, when attendees to an international AIDS conference were targeted with infected computer disks.¹ Ransomware payments have taken many forms over the past few decades, including through wire transfers, prepaid debit cards, iTunes gift cards, cash payments, and other forms.²

In other words, ransomware criminality pre-dates the development of blockchain and cryptocurrencies by many decades. While it is true that ransomware attacks began to increase in frequency starting in 2011, the fundamentals of ransomware criminality were well established before the advent of cryptocurrency. The vulnerability of information infrastructure, combined with a monetary incentive to lock and unlock networks in return for payment, mean that as workspaces

¹ <https://www.varonis.com/blog/a-brief-history-of-ransomware/>

² <https://www.aier.org/article/fighting-ransomware-doesnt-require-banning-cryptocurrency/>



become increasingly digitized, bad actors will increasingly be incentivized to engage in ransomware attacks – particularly as the cybersecurity defenses of America’s small businesses remain dangerously weak.

Indeed, ransomware attacks against small businesses with poor cybersecurity defenses can cost less than \$100 to perpetrate.³ Until carrying out ransomware attacks becomes prohibitively expensive thanks to the proliferation of strong cybersecurity defenses across American small businesses, criminals will be incentivized to continue to carry out these attacks. Payment activities related to or involving cryptocurrencies do not alter that harsh reality that the recent surge in ransomware attacks was primarily enabled by a rapid nationwide embrace of digital workplaces that was not accompanied by sufficient improvements in cybersecurity defenses. To stop ransomware attacks in an increasingly online world, resources are best spent developing programs and initiatives aimed at bolstering the cybersecurity of American small businesses, which are disproportionately victimized by ransomware attacks.⁴

Ransomware criminals using cryptocurrency can be traced on the blockchain

In fact, the attributes of cryptocurrencies actually enable regulators and law enforcement to trace ransomware transactions back to perpetrators. As lawmakers, regulators, and prosecutors gain a better understanding of cryptocurrency, we believe they will understand how it can be leveraged to combat the ongoing surge in ransomware attacks. This is because cryptocurrencies are created on an open blockchain, and as such, there is a public record of each transaction that cannot be altered. This auditability function helps explain why authorities have been able to track down and arrest the criminals behind some of the largest ransomware attacks,⁵ and/or recover amounts paid by victims.

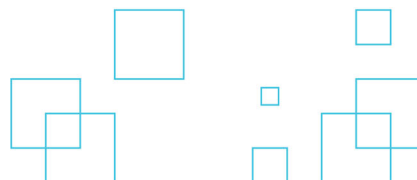
Indeed, the recent Colonial Pipeline ransomware attack ultimately resulted in almost all related criminal bitcoin transfers being traced and recovered. In fact, DOJ announced in a press release on June 7, 2021, that “by reviewing the Bitcoin public ledger, law enforcement was able to track multiple transfers of bitcoin and identify that approximately 63.7 bitcoins, representing the proceeds of the victim’s ransom payment, had been transferred to a specific address.”⁶ The FBI obtained the “private key” for the address and recovered the payments. Had the DarkSide hackers in the Colonial Pipeline case instead demanded payment in cash or through another payments channel, recovering the funds could have been much more difficult.

³ <https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report>

⁴ <https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report>

⁵ <https://apnews.com/article/europe-malware-netherlands-coronavirus-pandemic-7de5f74120a968bd0a5bec3c57899fed>

⁶ <https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>



As this example shows, cryptocurrency enables law enforcement to utilize technological tools and methods to track criminals that are unavailable for financial crimes that cannot be traced on a blockchain. In order to halt the recent increase in ransomware attacks, law enforcement can embrace new technologies to aggressively track and prosecute criminals.

Blockchain and other distributed ledger technology (DLT) can reduce financial crime

At the same time, it is critical for policymakers to embrace digital assets as well as blockchain and other forms of DLT, which if integrated into the traditional financial system, could lead to a large overall reduction of financial crime. The United Nations estimates that the amount of money laundered globally in one year is 2 to 5% of global GDP, or \$800 billion to \$2 trillion.⁷ Conversely, one study estimates that total ransomware paid via cryptocurrencies in 2020 equaled \$350 million⁸ – in other words, an amount less than one-tenth of a percent of the value of total money laundered annually.

Most money laundering and financial crime takes place via traditional financial intermediaries. For the same reasons that the blockchains of cryptocurrencies like bitcoin enable authorities to track and trace financial criminals such as ransomware attack perpetrators, the adaptation of DLT and blockchain solutions could help traditional financial institutions combat the massive global problem of financial crime. DLT is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions, and certain applications of blockchain technology—a form of DLT—have characteristics that can help governments and businesses combat financial crime, including the following:

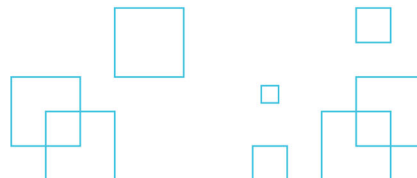
Distributed: Blockchain creates a shared system of record among business network members – eliminating the need to reconcile disparate ledgers.

- Transactions via blockchain networks can be constructed and held throughout the network and ultimately accessible via secured channels for audit and tracking purposes. This can be very helpful with respect to both client and transaction-related data, and the protection and presentment of Know Your Customer (identity) data between corresponding financial intermediaries

Immutability: Consensus is required from all members and all validated transactions are permanently recorded. Even a system administrator cannot delete or alter a transaction.

⁷ <https://www.unodc.org/unodc/en/money-laundering/overview.html>

⁸ <https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf>



- Transactions can be recorded for auditability and transaction monitoring. Transaction history and specifics cannot be altered once inputted, which means the associated identities of senders and receivers of a transaction can be verified as associated with the transaction itself. The immutability of the ledger can therefore benefit ongoing client and transaction monitoring real time – increasing process efficiencies and reducing costs associated with compliance activities.

Permissioned: Each member of the network must have access privileges and information is shared only on a need-to-know basis between network nodes.

- Information regarding the transaction origin (sender) and recipient can be permissioned between nodes for easy and secure access without disclosure to third parties without permission, and be leveraged for verification/validation purposes, managing against fraud, and assisting network participants in a common financial ecosystem.

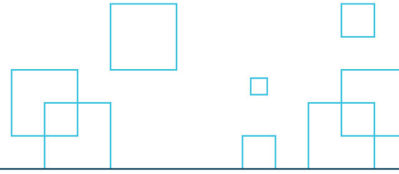
How the Chamber of Digital Commerce Can Help

The Chamber applauds recent actions taken by the Administration and Congress related to combating ransomware, such as proposals to increase resources to prosecute these criminals,⁹ and a willingness to leverage technologies that can trace cryptocurrency transactions.¹⁰ Ransomware is a crime, and we stand ready to work closely with government officials to continue to thwart attacks, raise awareness of cybersecurity initiatives, and help on the back end to trace the cryptocurrencies paid in each attack. We have attached to this document the most up to date [report](#) on the state of ransomware.

In conclusion, the Chamber of Digital Commerce hopes to be a valuable resource to the Judiciary Committee and law enforcement as we develop policy solutions to stop ransomware attacks. History demonstrates that criminals will pursue potentially lucrative ransomware attacks when and where they detect security weakness. Recent events, however, also demonstrate that criminals who demand payment in cryptocurrencies open the door to novel investigative and enforcement strategies that permit recovery of ransom funds. By embracing and expanding policy initiatives aimed at improving Main Street's cyber defenses while also increasing capabilities to aggressively track and prosecute cyber-criminals through analyzing cryptocurrency blockchains, we can put an end to ransomware attacks. We are also hopeful that an embrace of blockchain technology will lead to a reduction of illicit financial flows through traditional financial channels as well.

⁹ <https://www.justice.gov/jmd/page/file/1398826/download>

¹⁰ <https://www.bloomberg.com/news/articles/2021-07-15/u-s-plans-to-counter-ransomware-attacks-through-crypto-tracing>



Thank you for considering our views. We would be interested in meeting with you to provide a demo that illustrates the cryptocurrency traceability and auditability referred to in this letter.

A P P E N D I X
to
**AMERICA UNDER CYBER SIEGE:
PREVENTING AND RESPONDING
TO RANSOMWARE ATTACKS**

| | |
|---|-----|
| Chamber of Digital Commerce, July 27, 2021, statement | 166 |
| Ransomware 2021, July 2021 | 125 |

