Labor. If you believe he can be an impartial arbiter, then I have swampland in New Mexico to sell you. The head of the AFL–CIO herself expressed approval of Walsh's willingness to work ''behind the scenes.''

Walsh's infamous picket line participation with strikers at the Kellogg's factory won't be his last attempt to interfere with labor-management disputes. Politico recently reported Walsh is ''eager to help with others.''

Walsh's pro-union advocacy disqualifies him from acting as an honest broker. He would rather protect his union boss cronies than protect workers and job creators.

OUR ECONOMY IS STRONGER THAN EVER

(Ms. GARCIA of Texas asked and was given permission to address the House for 1 minute and to revise and extend her remarks.)

Ms. GARCIA of Texas. Mr. Speaker, I rise to celebrate the country's tremendous economic improvements.

While our economy is stronger than ever, the America COMPETES Act will strengthen the economy even more in the near future. But one key economic accomplishment during Biden's first year I would like to highlight is the large budget deficit decrease he produced.

In his first year, the deficit decreased by $360 billion. That is an average drop of $30 billion each month. That is huge.

This is a night-and-day difference from the past administration, which only increased the budget deficit year after year during his time in office. But even better, Biden is on track to reduce the deficit by more than $1 trillion this year. This is truly remarkable.

We really are building a better America for generations to come.

VICTORY FOR UKRAINE

(Mr. WILSON of South Carolina asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. WILSON of South Carolina. Mr. Speaker, Ukraine, led by President Volodymyr Zelenskyy, is winning and will be victorious over Putin. Biden must send military aid now.

The ruse provided by incompetent Russian generals to claim eastern Ukraine is a trick. Just as America would not surrender by giving up a small part of the Eastern United States, such as Delaware, we know Putin must be defeated by peace through strength.

Victory is the only option to stop autocracy by rule of gun against democracy by rule of law, a clash of civilizations. The Chinese Communist Party will be stopped from mass murder in Taiwan. Iranian mullahs will be stopped from vaporizing the people of Israel. The world's largest democracy of India can thrive in a stabilized world.

I have faith in the Russian people, a great culture with great cultural influence adopted in America. There is legislation for defecting Russian troops, diplomats, and Duma members to be provided immediate refugee status to America and up to $100,000 for any Russian military equipment turned over to Ukraine.

God bless Ukraine. God save Ukraine. Long live Volodymyr Zelenskyy.

CONGRATULATING IOWA'S HIGH SCHOOL BASKETBALL ALL-STATE HONOREES

(Mrs. MILLER-MEEKS asked and was given permission to address the House for 1 minute and to revise and extend her remarks.)

Mrs. MILLER-MEEKS. Madam Speaker, I rise today to recognize the achievements of several young men from Iowa's Second Congressional District.

Earlier this month, the Iowa high school basketball State championships were held in Des Moines. It was a weekend of competition and sportsmanship. While no school from the Second District won the championship, several young men recently earned all-State honors from the Des Moines Register.

Dayton Davis of Fort Madison and Shawn Gilbert of Central DeWitt were named to the Class 3A team. Eric Mulder of Pella Christian was named to the Class 2A team, and Maddox Griffin of Wapello was named to the Class 1A team.

In addition, Kaden Hall of English Valleys, Carter Harmsen of Mid-Prairie, Karl Miller of Pella, Pete Moe of Iowa City West, and Blaise Porter of New London earned honorable mention recognition.

Congratulations to all of these young men, teams, families, schools, and communities on achieving these honors. They are all well deserved.

Madam Speaker, I also knowledge that tomorrow, March 29, my daughter, Taylor Miller-Meeks, was born, which was one of the best days of my life.

BIDEN FOOD INSECURITY

(Mr. LAMALFA asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. LAMALFA. Madam Speaker, I rise today to talk about the situation we have with agriculture and water in California and the President's acknowledgment just a couple of days ago that we are going to see a food shortage in the world but partially even in the United States of America.

That is unbelievable to me. How could we, the United States of America, be facing possible food shortages? Indeed, already on the store shelves is empty space.

I remember a story just a few years ago where Boris Yeltsin, President of Russia, of all places, came over and was visiting. They took him to a grocery store in the United States, and he was amazed and blown away and even emotional by the variety we have here.

Yet, the priorities don't seem to be producing for Americans or even producing for those we help around the world. It seems to be based more on environmental needs, like in my home State of California where they are releasing more water out to the ocean than what is going to go to agriculture this year.

Why does this affect all Americans? Why does this affect you? Because so many of the crops that we grow in California supply somewhere between 90 and 98 percent of what Americans eat of those crops, and we are still doing this environmental stuff in California.

RECESS

The SPEAKER pro tempore (Ms. GARCIA of Texas). Pursuant to clause 12(a) of rule I, the Chair declares the House in recess subject to the call of the Chair.

Accordingly (at 2 o'clock and 12 minutes p.m.), the House stood in recess.

□ 1645

AFTER RECESS

The recess having expired, the House was called to order by the Speaker pro tempore (Mr. VEASEY) at 4 o'clock and 45 minutes p.m.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, the Chair will postpone further proceedings today on motions to suspend the rules on which the yeas and nays are ordered.

The House will resume proceedings on postponed questions at a later time.

BETTER CYBERCRIME METRICS ACT

Ms. JACKSON LEE. Mr. Speaker, I move to suspend the rules and pass the bill (S. 2629) to establish cybercrime reporting mechanisms, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

S. 2629

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Better Cybercrime Metrics Act''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) Public polling indicates that cybercrime could be the most common crime in the United States.

(2) The United States lacks comprehensive cybercrime data and monitoring, leaving the country less prepared to combat cybercrime that threatens national and economic security.

(3) In addition to existing cybercrime vulnerabilities, the people of the United

States and the United States have faced a heightened risk of cybercrime during the COVID–19 pandemic.

(4) Subsection (c) of the Uniform Federal Crime Reporting Act of 1988 (34 U.S.C. 41303(c)) requires the Attorney General to ''acquire, collect, classify, and preserve national data on Federal criminal offenses as part of the Uniform Crime Reports'' and requires all Federal departments and agencies that investigate criminal activity to ''report details about crime within their respective jurisdiction to the Attorney General in a uniform matter and on a form prescribed by the Attorney General''.

SEC. 3. CYBERCRIME TAXONOMY.

(a) IN GENERAL.—Not later than 90 days after the date of enactment of this Act, the Attorney General shall seek to enter into an agreement with the National Academy of Sciences to develop a taxonomy for the purpose of categorizing different types of cybercrime and cyber-enabled crime faced by individuals and businesses.

(b) DEVELOPMENT.—In developing the taxonomy under subsection (a), the National Academy of Sciences shall—

(1) ensure the taxonomy is useful for the Federal Bureau of Investigation to classify cybercrime in the National Incident-Based Reporting System, or any successor system;

(2) consult relevant stakeholders, including—

(A) the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security;

(B) Federal, State, and local law enforcement agencies;

(C) criminologists and academics;

(D) cybercrime experts; and

(E) business leaders; and

(3) take into consideration relevant taxonomies developed by non-governmental organizations, international organizations, academies, or other entities.

(c) REPORT.—Not later than 1 year after the date on which the Attorney General enters into an agreement under subsection (a), the National Academy of Sciences shall submit to the appropriate committees of Congress a report detailing and summarizing—

(1) the taxonomy developed under subsection (a); and

(2) any findings from the process of developing the taxonomy under subsection (a).

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section $1,000,000.

SEC. 4. CYBERCRIME REPORTING.

(a) IN GENERAL.—Not later than 2 years after the date of enactment of this Act, the Attorney General shall establish a category in the National Incident-Based Reporting System, or any successor system, for the collection of cybercrime and cyber-enabled crime reports from Federal, State, and local officials.

(b) RECOMMENDATIONS.—In establishing the category required under subsection (a), the Attorney General shall, as appropriate, incorporate recommendations from the taxonomy developed under section 3(a).

SEC. 5. NATIONAL CRIME VICTIMIZATION SURVEY.

(a) IN GENERAL.—Not later than 540 days after the date of enactment of this Act, the Director of the Bureau of Justice Statistics, in coordination with the Director of the Bureau of the Census, shall include questions relating to cybercrime victimization in the National Crime Victimization Survey.

(b) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section $2,000,000.

SEC. 6. GAO STUDY ON CYBERCRIME METRICS.

Not later than 180 days after the date of enactment of this Act, the Comptroller General of the United States shall submit to Congress a report that assesses—

(1) the effectiveness of reporting mechanisms for cybercrime and cyber-enabled crime in the United States; and

(2) disparities in reporting data between—

(A) data relating to cybercrime and cyber-enabled crime; and

(B) other types of crime data.

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from Texas (Ms. JACKSON LEE) and the gentleman from Oregon (Mr. BENTZ) each will control 20 minutes.

The Chair recognizes the gentlewoman from Texas.

GENERAL LEAVE

Ms. JACKSON LEE. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days to revise and extend their remarks and include extraneous materials on S. 2629.

The SPEAKER pro tempore. Is there objection to the request of the gentlewoman from Texas?

There was no objection.

Ms. JACKSON LEE. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in support of S. 2629, the Better Cybercrime Metrics Act. This legislation improves our understanding and tracking of cybercrime so that we can do more to prevent it.

A 2018 Gallup Poll found that 1 in 4 Americans had been a victim of cybercrime. And I might say that it has exponentially grown during the pandemic. From stolen financial information, to system-wide shutdowns, to ransomware attacks, these crimes harm our families, our businesses, and our government.

The Council of Economic Advisers estimates that malicious cyber activities cost our economy as much as $109 billion in 2016, and experts believe these costs are growing. The COVID–19 pandemic has increased opportunities for cybercrime with increases in remote work and the time people are spending online. Hackers also took advantage of our recovery efforts, stealing identities to file fake unemployment claims or fraudulent loan applications. And again, in the midst of other innocent Americans not being able to secure those dollars, and not being able to secure unemployment claims because of the fake process that clouded this system.

Many of the victims of these scams only learned that they were attacked when they went to file genuine claims and were told had already been submitted using their names or businesses.

Sadly, cybercriminals often target older Americans. In 2020, people over 60 accounted for the most complaints of any age group as collected by the FBI Internet Crime Complaint Center. People over 60 also had the greatest losses, with over $966 billion lost to cybercrime in 2020.

We must do more to protect Americans from cybercrime, and that starts with a better understanding of what it is and how it occurs. The Better Cybercrime Metrics Act will gather experts in law enforcement, business, and technology to create a taxonomy of cybercrime so we can define it and classify it in a uniform way.

This legislation also adds cybercrime to two important law enforcement tools used to track crimes: The National Incident-Based Reporting System and the National Crime Victimization Survey. Together, these provisions will ensure that law enforcement has a complete picture of when and where cybercrime occurs and who is harmed by it.

Finally, this bill directs the Government Accountability Office to conduct a study on reporting mechanisms for cybercrime and the disparities in cybercrime data relative to other types of crime data. Together, this legislation will put in place the tools to clearly define and classify cybercrime, to track cybercrime, and to better understand this serious threat.

Mr. Speaker, it is a very serious threat. And in addition to the monetary damages, people have been personally and psychologically impacted by losses, by lack of employability, by being rejected, for some of these claims having to be delayed when the individual who needs it is desperate and experiencing a desperate economic condition, to find that they have been, in essence, gamed by a cybercriminal. We must stop this.

And as I said earlier, one of the most vulnerable populations are individuals over 60. And really when you find those in their seventies, eighties, nineties, who have lived their lives, supported this Nation, and become victims of cybercrime, it is something that compels you to really want to stop this threat.

I commend Senators BRIAN SCHATZ and THOM TILLIS for their work on this bipartisan legislation. I also thank Representative ABIGAIL SPANBERGER for her leadership on the House companion to this bill. I was proud to stand with her in introducing the House companion, along with our Republican colleagues, Representative BLAKE MOORE and Representative ANDREW GARBARINO.

We must give law enforcement the tools to keep pace with new technology and to get a step ahead of the threats faced by our ever-evolving world. This bill takes an important step in that effort, and I urge my colleagues to support it.

Mr. Speaker, I reserve the balance of my time.

MEMORANDUM EXCERPT

To: Members of the House Judiciary Committee

From: The Honorable Jerrold Nadler, Chairman, Committee on the Judiciary

Re: Markup of H.R. 4977, the ''Better Cybercrime Metrics Act''; H.R. 55, the ''Emmett Till Antilynching Act''; H.R. 5338, the ''Radiation Exposure Compensation Act Amendments of 2021''; and H.R. 5796, the ''Patents for Humanity Act of 2021''

Date: Tuesday, December 7, 2021

On Wednesday, December 8, 2021 at 10:00 a.m. in 2141 Rayburn House Office Building, the House Judiciary Committee will mark up the following measures: H.R. 3359, the ''Homicide Victims' Families' Rights Act of 2021''; H.R. 4977, the ''Better Cybercrime Metrics Act''; H.R. 55, the ''Emmett Till Antilynching Act''; H.R. 5338, the ''Radiation Exposure Compensation Act Amendments of 2021''; and H.R. 5796, the ''Patents for Humanity Act of 2021''.

II. H.R. 4977, THE ''BETTER CYBERCRIME METRICS ACT''

H.R. 4977, the ''Better Cybercrime Metrics Act'' would improve the U.S. government's understanding, measurement, and tracking of cybercrime. The bill would direct the Department of Justice to work with the National Academy of Sciences, in consultation with relevant stakeholders, to develop a taxonomy of cybercrime that could be used by law enforcement to ensure that the National Incident-Based Reporting System (NIBRS), or any successor system, include cybercrime reports from federal, state, and local officials. It also directs the Bureau of Justice Statistics to include questions relating to cybercrime in the National Crime Victimization Survey. The bill also directs the Government Accountability Office (GAO) to report on the effectiveness of current cybercrime reporting mechanisms and highlight disparities in reporting data between cybercrime data and other types of crime data. This bipartisan bill was introduced on August 6, 2021 by Representative Abigail Spanberger (D–VA) and currently has 18 cosponsors. An identical Senate companion, S. 2629 (Schatz–HI, Tillis–NC, Cornyn–TX, Durbin–IL), was marked up by the Senate Judiciary Committee on November 18 and favorably reported on a unanimous voice vote. The Chairman will offer an amendment in the nature of a substitute to H.R. 4977.

A. GENERAL BACKGROUND

Cybercrime continues to be a significant threat to businesses, governments, and individual Americans. Cybercrime includes a broad range of conduct including phishing, ransomware, identity theft, and data breaches.[1] A recent survey found one in five Americans have been victims of ransomware.[2] The COVID–19 pandemic created new opportunities for cybercrime, including COVID-related phishing and malware, with 35.9% of the world's COVID–19 cyber threats occurring in the United States.[3] Cyber attackers mainly rely on phishing attacks, which is the most common attack as measured by the number of victims.[4] Attackers also use online tools for extortion, data breaches, identity theft, extracting ransoms, email compromise schemes, impersonating charities and government actors, and other schemes.[5] Researchers attribute the rise in attacks to the increase in remote work and the lower security protections at one's home compared to an office.[6]

Cybercrime is costly and harms individuals, government entities, and businesses across a broad range of industries. The average data breach in 2020 cost companies $3.83 million dollars.[7] Email compromise schemes, in which email accounts are compromised to conduct unauthorized transfers of funds, accounted for over $1.8 billion in losses in 2020.[8] In the first six months of 2021, six ransomware organizations hacked 292 organizations and stole $45 million dollars.[9] Organizations that experienced cybercrime this year include the Colonial Pipeline, the Steamship Authority of Massachusetts, JBS Foods, and the Washington D.C. Metropolitan Police Department.[10] As shown by the gas shortage due to the Colonial Pipeline breach, these attacks can shut down critical infrastructure, create shortages, increase the cost of goods and services, and cost organizations money from both operational shutdowns and paying ransoms to hackers.[11] Likewise, the December 2020, SolarWinds attack targeted SolarWinds' 300,000 customers and endangered the cybersecurity of many federal government agencies, including the Department of Defense, as well as 425 of the U.S. Fortune 500 companies.[12] Cybercrime harms businesses across all industries, but it had a particular effect on companies responding to the COVID–19 pandemic by disrupting COVID–19 supply chains and the government's efforts to address the spreading virus.[13]

Bad actors gravitate to cyber-attacks because of the anonymity the internet provides and the low chances of getting caught. The detection and prosecution rate of cyber criminals in the United States is .05%.[14] Given the difficulty in tracing and prosecuting these crimes, it is important to further study and track them so that we can work to prevent cybercrime. H.R. 4977, the Better Cybercrime Metrics Act will provide law enforcement with the tools to uniformly classify and track cybercrime, furthering the government's understanding of this serious problem and building the foundation for improved cybercrime prevention efforts.

B. SECTION-BY-SECTION ANALYSIS FOR THE AMENDMENT IN THE NATURE OF A SUBSTITUTE

Section 1. Short Title. Section 1 sets forth the short title of the bill as the ''Better Cybercrime Metrics Act.''

Section 2. Cybercrime Taxonomy. Section 2 requires, within 90 days of the passage of the Act, the DOJ and the National Academy of Sciences to develop a taxonomy that can be used by law enforcement to categorize and track cybercrime, and requires that the taxonomy be presented to Congress. The bill authorizes $1,000,000 to carry out this section.

Section 3. Cybercrime Reporting. Section 3 requires, not later than 2 years after the passage of the Act, the DOJ to establish a category in the National Incident-Based Reporting System to enable the collection of cybercrime and cyber-enabled crime reports from Federal, State, and local officials, incorporating the taxonomy developed under Section 2 as appropriate.

Section 4. National Crime Victimization Survey. Section 4 requires cybercrime to be added to the National Crime Victimization Survey. The bill authorizes $2,000,000 to carry out this section.

Section 5. GAO Study on Cybercrime Metrics. Section 5 directs the GAO to do a study on the current reporting mechanisms of cybercrime and the disparities in data between (A) data relating to cybercrime and cyber-enabled crime; and (B) other types of crime data.

ENDNOTES

[1] Fed. Bureau of Investigation, Internet Crime Complaint Ctr., Internet Crime Report 2020 19 (2021) https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[2] Joe Franscella, *Anomali Harris Poll: Ransomware Hits 1 in 5 Americans*, Anomali (Aug. 16, 2019), https://www.anomali.com/blog/anomali-harris-poll-ransomware-hits-1-in-5.

[3] Trend Micro Research, Attacks from All Angles: 2021 Midyear Cybersecurity Report 23 (2021) https://documents.trendmicro.com/assets/rpt/rpt-attacks-from-all-angles.pdf.

[4] Fed. Bureau of Investigation, Internet Crime Complaint Ctr., Internet Crime Report 2020 6 (2021) https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[5] *Id.* at 19.

[6] *The 10 Biggest Ransomware Attacks of 2021*, Touro College Illinois (Nov. 12, 2021). https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php.

[7] Ken Brisco, *Cost of a Data Breach: Behind the Numbers of a Cybersecurity Response Plan*, Secureworks (Jul. 27, 2021), https://www.secureworks.com/blog/data-breach-response-planning-cyber-threat-intelligence.

[8] Fed. Bureau of Investigation, Internet Crime Complaint Ctr., Internet Crime Report 2020 10 (2021) https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[9] *Six Ransomware Gangs Claim 290+ New Victims in 2021, Potentially Reaping $45 Million for the Hackers*, eSentire. https://www.esentire.com/resources/library/six-ransomware-gangs-claim-290-new-victims-in-2021-potentially-reaping-45-million-for-the-hackers (last visited Dec. 3. 2021).

[10] *The 10 Biggest Ransomware Attacks of 2021*, Touro College Illinois (Nov. 12, 2021), https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php.

[11] *Id.*

[12] Jake Williams, *What You Need to Know About the SolarWinds Supply-Chain Attack*, SANS Institute (Dec. 15, 2020) https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack.

[13] Jackie Drees, *Cyberattacks on COVID–19 vaccine supply chain much larger than initially thought, IBM says*, Becker's Hospital Review (Apr. 30, 2021) https://www.beckershospitalreview.com/cybersecurity/cyberattacks-on-covid-19-vaccine-supply-chain-much-larger-than-initially-thought-ibm-savs.html.

[14] Mieke Eoyang, Alison Peters, Ishan Mehta, Brandon Gaskew, *To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors*, Third Way (Dec. 3, 2021) https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors.

Mr. BENTZ. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, American businesses and American citizens face a growing number of cybercrimes. Cybercrime is a particularly complicated form of criminal conduct and one that costs Americans billions of dollars a year in theft.

This bill would require the Attorney General to enter into an agreement with the National Academy of Sciences to develop a method for categorizing different types of cybercrime. The Attorney General would also establish a cybercrime category in the National Incident-Based Reporting System so that States can better report cybercrime data to the Federal Government.

The bill would also require the Bureau of Justice Statistics to include cybercrime victimization questions in the National Crime Victimization Survey. There is no question that we must do more to bring cybercriminals to justice.

In August of 2021, the Biden administration released a notorious Russian cybercriminal early from Federal custody. The individual is described as, ''one of the most connected and skilled malicious hackers ever apprehended by the U.S. authorities.'' And for unknown reasons, the administration let him out of Federal prison early and shipped him back to Moscow.

We have asked the Biden administration's Justice Department for more information about this early release of this cybercriminal, but we have received nothing as of yet. Similarly, we don't have enough information to determine whether this legislation will bring more cybercriminals to justice. We haven't heard from relevant stakeholders on these issues, and we haven't held hearings with experts to determine whether this is the right step at this time.

This bill would require GAO to submit a report to Congress that assesses the effectiveness of reporting mechanisms for cybercrime and disparities in reporting data between cybercrime and other types of crime.

Why aren't we starting with that?

Why are we making changes to cybercrime reporting mechanisms before the GAO can evaluate whether the existing reporting mechanisms are effective?

It makes more sense for us to have hearings, evaluate GAO's findings, and hear from experts. Then we can examine whether the other provisions of this bill are necessary and appropriate.

In another instance of putting the cart before the horse, the Committee on the Judiciary is scheduled to hear from Bryan A. Vorndran, the assistant director of Cyber Division at the FBI tomorrow. Perhaps we should have waited to see what he had to say before rushing this legislation to the floor.

Mr. Speaker, I reserve the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, I yield 5 minutes to the gentlewoman from Virginia (Ms. SPANBERGER), who was astute enough to be able to offer the companion bill, and I thank her for her leadership and career leadership on these issues.

Ms. SPANBERGER. Mr. Speaker, I rise today in support of my Better Cybercrime Metrics Act and its companion bill in the U.S. Senate, S. 2629. And I thank the gentlewoman from Texas (Ms. JACKSON LEE) for that introduction and for her support of this bill since the moment we introduced it.

Mr. Speaker, our Nation is under constant attack from cybercriminals. And with the range of new threats emanating from adversaries around the world, including the Russian Federation, Congress has an obligation to move legislation forward that can better protect the American people, their data, their finances, and their personal information.

Over the last few years, we have seen massive rates of cybercrime. Millions of Americans have had their personal data compromised, their money stolen, their identity taken, or their safety put at serious risk. In fact, cybercrime remains the most common crime in America, and this trend was only exacerbated by the pandemic and the many fraudsters looking to scam vulnerable Americans in a moment of crisis or make a quick buck off of a global catastrophe.

Unfortunately, a vast majority of these crimes are not properly reported or tracked by law enforcement. Far too often, they are not measured or even documented. And to make matters worse, our government lacks the preparedness required to fully address the next generation of cybercrime and cyberattacks.

Our legislation would give law enforcement agencies the tools they need to better track and identify cybercrime, prevent attacks, and hold perpetrators accountable. Our bill would require Federal reporting on the effectiveness of current cybercrime mechanisms.

And it would go one step further—it would also highlight disparities in reporting data between cybercrime data and other types of crime data. This is such an important step for strengthening our understanding and our defenses against the phishing attempts, extortion, identity theft, and ransomware attacks that are plaguing everyday Americans in communities and across our country. Additionally, our bill would make sure America's law enforcement is prepared for the next generation of cyberattacks.

Mr. Speaker, I am a proud former Federal law enforcement officer, and I understand that local and State police and sheriff's departments are often strained for resources. And I know that their time is precious, so I recognize the importance of having their backs and making sure that we have as much information as possible about potential threats.

This legislation follows through on that commitment and it is why I am glad to see it endorsed by several national organizations—including the National Fraternal Order of Police, the National Association of Police Organizations, the Major Cities Chiefs Association, and the National White Collar Crime Center, which has a presence in Virginia's Seventh District.

In fact, this legislation—bipartisan and bicameral—was partially inspired by the attack on the Colonial pipeline last year, something that impacted many communities across my district.

After thousands of Virginians, their gas tanks, and their wallets were impacted by this disruptive ransomware attack, I was proud to build a bipartisan coalition focused on improving America's efforts to undercut hackers, protect critical infrastructure, and strengthen existing cybercrime prevention efforts.

Mr. Speaker, I thank my colleagues in the U.S. House of Representatives who joined this bipartisan coalition. I thank Congressman BLAKE MOORE, Congressman ANDREW GARBARINO, and Congresswoman SHEILA JACKSON LEE for their partnership. Clearly, there is still bipartisan consensus for cybersecurity reforms and protections.

Mr. Speaker, I also thank our friends across the Capitol complex for ushering the Senate version through the process. Thank you to Senators SCHATZ, TILLIS, CORNYN, and BLUMENTHAL for your cooperation and leadership on this important bicameral effort.

When our bipartisan bill passes the House tonight, it will head to the President's desk to be signed into law. And with a stroke of a pen, we will ensure that our national crime classification system can properly identify cybercrimes and prevent future attacks.

Once our legislation is signed into law, we will be protecting more families who bank online. We will be protecting more businesses who manage their employees' payroll information over the internet. We will be protecting more seniors who are using the internet to communicate with their loved ones far away or rely on the internet to manage their Federal benefits, such as Social Security.

Together, we will thwart cybercriminals. And together, we will prevent more Americans from becoming targets or victims online.

Mr. BENTZ. Mr. Speaker, I reserve the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, I am prepared to close, and I reserve the balance of my time.

□ 1700

Mr. BENTZ. Mr. Speaker, I urge my colleagues to oppose this bill, and I yield back the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, let me just take an opportunity to thank Congresswoman SPANBERGER for the knowledge she brings to this issue and to this legislation. We have already said that this is not a harmless crime.

Mr. Speaker, I include in the RECORD Cybercrime predictions for 2022: Deepfakes, cryptocurrencies, and misinformation, to further emphasize the lack of the harmlessness that it is. It is harmful. One sentence says it all: Fake news 2.0 and the return of misinformation campaigns. They cite in particular COVID–19. I think all of us can attest to the terrible damage that was done during the pandemic with the huge issues of the question of COVID and the vaccination. Fake vaccine passport certificates were on sale for $100 to $125, and the volume of advertising groups and group sizes publishing sellers and multiplied over and over again.

[From the Future, December 4, 2021]

CYBERCRIME PREDICTIONS FOR 2022: DEEPFAKES, CRYPTOCURRENCIES, AND MISINFORMATION

(By Maya Horowitz)

While cybercriminals continue to leverage the impact of the COVID–19 pandemic, they

will also find new opportunities to attack such as deepfakes, cryptocurrency and mobile wallets.

In 2021, cyber criminals adapted their attack strategy to exploit vaccination mandates, elections and the shift to hybrid work, to target organizations' supply chains and networks for them to achieve maximum disruption.

The sophistication and scale of cyberattacks will continue to break records and we can expect a huge increase in the number of ransomware and mobile attacks. Looking ahead, organizations should remain aware of the risks and ensure that they have the appropriate solutions in place to prevent them without disrupting their normal business flow. To stay ahead of threats, organizations must be proactive and leave no part of their attack surface unprotected or unmonitored or otherwise risk becoming the next victim of sophisticated, targeted attacks.

GLOBAL CYBERCRIME PREDICTIONS FOR 2022

Fake news 2.0 and the return of misinformation campaigns

The claim of 'fake news' surrounding contentious issues has become a new attack vector over previous years without people really understanding its full impact. Throughout 2021, misinformation was spread about the COVID–19 pandemic and vaccination information. The black market for fake vaccine certificates expanded globally, now selling fakes from 29 countries. Fake 'vaccine passport' certificates were on sale for $100–120 and the volume of advertisement groups and group sizes publishing sellers multiplied within the year. In 2022, cyber groups will continue to leverage these types of fake news campaigns to execute cybercrime through various phishing attacks and scams.

In addition, prior to the 2020 US presidential election, Check Point researchers spotted surges in malicious election-related domains and the use of ''meme camouflage'' aimed at shifting public opinion. In the run-up to the US midterm elections in November 2022, we can expect to see these activities in full effect and for misinformation campaigns to return on social media.

Cyberattacks targeting supply chains

Supply chain attackers take advantage of a lack of monitoring within an organization's environment. They can be used to perform any type of cyberattack, such as data breaches and malware infections.

The well known cybercrime—SolarWinds supply chain attack stands out in 2021 due to its scale and influence, but other sophisticated supply chain attacks have occurred such as Codecov in April, and most recently, Kaseya. Kaseya provides software for Managed Service Providers and the REvil ransomware gang exploited the company to infect over 1,000 customers with ransomware. The group demanded a ransom of $70 million to provide decryption keys for all affected customers.

Supply chain attacks will become more common and governments will have to establish regulations to address these attacks and protect networks. They will also look into collaborating with the private sectors and internationally to identify and target more threat groups operating on global and regional scales. In 2022, expect to discover more about the global impact of the infamous Sunburst attack.

The cyber 'cold war' intensifies

The cyber way is intensifying, and taking place online as more nation-state actors push Western governments to continue to destabilize society. Improved infrastructure and technological capabilities will enable terrorists groups and political activists to further their cybercrime agendas and carry out more sophisticated, widespread attacks. Cyberattacks will increasingly be used as proxy conflicts to destabilize activities globally.

Data breaches are larger scale and more costly

Going into 2022 we will see an increase in data breaches that will be larger scale. These breaches will also have the potential to cost organizations and governments more to recover. In May 2021, a US insurance giant paid $40 million in ransom to hackers. This was a record, and we can expect ransom demanded by attackers to increase in 2022.

TECHNOLOGY CYBERSECURITY PREDICTIONS FOR 2022

Mobile malware attacks increase as more people use mobile wallets and payment platforms:

In 2021, 46 percent of organizations had at least one employee download a malicious mobile application. The move to remote work for almost entire populations across the world during the COVID–19 pandemic saw the mobile attack surface expand dramatically, resulting in 97 percent of organizations facing mobile threats from several attack vectors. As mobile wallets and mobile payment platforms are used more frequently, cybercrimes will evolve and adapt their techniques to exploit the growing reliance on mobile devices.

Cryptocurrency becomes a focal point for cyberattacks globally

When money becomes purely software, the cybersecurity needed to protect us from hackers stealing and manipulating bitcoins and altcoins is sure to change in unexpected ways. As reports of stolen crypto wallets triggered by free airdropped NFTs become more frequent, Check Point Research (CPR) investigated OpenSea and proved it was possible to steal crypto wallets of users by leveraging critical security. In 2022, we can expect to see an increase in cryptocurrency related attacks.

Attackers leverage vulnerabilities in microservices to launch largescale attacks

The move to the cloud and DevOps will result in a new form of cybercrime. With microservices becoming the leading method for application development, and microservices architecture being embraced by Cloud Service Providers (CSPs), attackers are using vulnerabilities found in microservices to launch their attacks. We can also expect to see large scale attacks targeting CSPs.

Deepfake technology weaponized

Techniques for fake video or audio are now advanced enough to be weaponized and used to create targeted content to manipulate opinions, stock prices or worse. As in the case of other mobile attacks that rely on social engineering, the results of a phishing attacks can range from fraud to more advanced espionage. For instance in one of the most significant deepfake phishing attacks, a bank manager in the United Arab Emirates fell victim to a threat actor's scam. Hackers used AI voice cloning to trick the bank manager into transferring $35 million. Threat actors will use deepfake social engineering attacks to gain permissions and to access sensitive data.

Penetration tools continue to grow

Globally in 2021, 1 out of every 61 organizations was being impacted by ransomware each week. Cybercrime through ransomware will continue to grow, despite the efforts of law enforcement to limit this growth globally. Threat actors will target companies that can afford paying ransom, and ransomware attacks will become more sophisticated in 2022. Hackers will increasingly use penetration tools to customize attacks in real time and to live and work within victim networks. Penetration tools are the engine behind the most sophisticated ransomware attacks that took place in 2021. As the popularity of this attack method grows, attackers will use it to carry out data exfiltration and extortion attacks.

Ms. JACKSON LEE. Mr. Speaker, I include in the RECORD the article: ''Ho, Ho, Ho, Holiday Scams'' FBI Portland. During the 2020 holiday season, this article says this FBI Internet Compliance Center received more than 17,000 complaints regarding the nondelivery of goods resulting in losses of more than $53 billion.

[From FBI Portland, December 1, 2021]

HO, HO, HO, HOLIDAY SCAMS!

(By Beth Anne Steele)

If you're doing online shopping this holiday season, be on the lookout for scammers trying to steal a deal, too!

During the 2020 holiday shopping season, the FBI Internet Crime Complaint Center (IC3.gov) received more than 17,000 complaints regarding the non-delivery of goods, resulting in losses of more than $53 million. The FBI anticipates this number could increase during the 2021 holiday season due to rumors of merchandise shortages and the ongoing pandemic.

''Oftentimes when we talk about cyber crimes, we are referring to massive intrusions into financial institutions or ransomware attacks against large providers. Smaller cyber scams run by individuals or groups can be just as frustrating and difficult for families this time of year when all you want to do is provide the perfect gift for your family. The best thing you can do to be a savvy shopper is to know what scams are out there and take some basic precautions,'' says Kieran L. Ramsey, special agent in charge of the FBI in Oregon.

Here's a look at some of the more common scams:

Online Shopping Scams:

Scammers often offer too-good-to-be-true deals via phishing emails, through social media posts, or through ads. Perhaps you were trying to buy tickets to the next big concert or sporting event and found just what you were looking for—at a good deal—in an online marketplace? Those tickets could end up being bogus. Or, perhaps, you think you just scored a hard-to-find item like a new gaming system? Or a designer bag at an extremely low price? If you actually get a delivery, which is unlikely, the box may not contain the item you ordered in the condition you thought it would arrive. In the meantime, if you clicked on a link to access the deal. you likely gave the fraudster access to download malware onto your device, and you gave him personal financial information and debit/credit card details.

Social Media Shopping Scams:

Consumers should beware of posts on social media sites that appear to offer special deals, vouchers, or gift cards. Some may appear as holiday promotions or contests. Others may appear to be from known friends who have shared the link. Often, these scams lead consumers to participate in an online survey that is designed to steal personal information. If you click an ad through a social media platform, do your due diligence to check the legitimacy of the website before providing credit card or personal information.

Gift Card Scams:

Gift cards are popular and a great time saver. but you need to watch for sellers who say they can get you cards below-market value. Also, be wary of buying any card in a

store if it looks like the security PIN on the back has been uncovered and recovered. Your best bet is to buy digital gift cards directly from the merchant online. Another twist on this scam involves a person who receives a request to purchase gift cards in bulk. Here's how it works: the victim receives a spoofed email, a phone call, or a text from a person who they believe is in authority (such as an executive at the company). The fraudster tells the victim to purchase multiple gift cards as gifts. The victim does so and then passes the card numbers and PINs to the ''executive'' who cashes out the value.

Charity Scams:

Charity fraud rises during the holiday season when people want to make end-of-year tax deductible gifts or just wish to contribute to a good cause. These seasonal scams can be more difficult to stop because of their widespread reach, limited duration and, when done online, minimal oversight. Bad actors target victims through cold calls, email campaigns, crowdfunding platforms, or fake social media accounts and websites. Fraudsters make it easy for victims to give money and to feel like they're making a difference. The scammer will divert some or all the funds for personal use, and those most in need will never see the donations.

Tips to Avoid Being Victimized:

Pay for items using a credit card dedicated for online purchases, checking the card statement frequently, and never saving payment information in online accounts.

Never make purchases using public Wi-Fi.

Beware of vendors that require payment with a gift card, wire transfer, cash, or cryptocurrency.

Research the seller to ensure legitimacy. Check reviews and do online searches for the name of the vendor and the words ''scam'' or ''fraud.''

Check the contact details listed on the website to ensure the vendor is real and reachable by phone or email.

Confirm return and refund policies.

Be wary of online retailers who use a free email service instead of a company email address.

Don't judge a company by its website. Flashy websites can be set up and taken down quickly.

Do not click on links or provide personal or financial information to an unsolicited email or social media post.

Secure credit card accounts, even rewards accounts, with strong passwords or passphrases. Change passwords or passphrases regularly.

Make charitable contributions directly, rather than through an intermediary, and pay via credit card or check. Avoid cash donations, if possible.

Only purchase gift cards directly from a trusted merchant.

Make sure anti-virus/malware software is up to date and block pop-up windows.

What to Do if You Are a Victim:

If you are a victim of an online scam, the FBI recommends taking the following actions:

Report the activity to the Internet Crime Complaint Center at IC3.gov, regardless of dollar loss. Provide all relevant information in the complaint.

Contact your financial institution immediately upon discovering any fraudulent or suspicious activity and direct them to stop or reverse the transactions.

Ask your financial institution to contact the corresponding financial institution where the fraudulent or suspicious transfer was sent.

Ms. JACKSON LEE. Mr. Speaker, I include in the RECORD the article: ''Without major changes, more Americans can be victims of online crime'' The Hill. ''When you turn on the TV or read the newspaper, it is hard to ignore headlines: 'Colonial Pipeline a Victim of Massive Ransomware Attack.' '50 Million People Affected by T-Mobile Data Breach.' 'Hackers Exploit SolarWinds to Spy on U.S. Government Agencies.' ''

[From The Hill, Aug. 30, 2021]

WITHOUT MAJOR CHANGES, MORE AMERICANS COULD BE VICTIMS OF ONLINE CRIME

(By Rep. Abigail Spanberger (D–VA))

When you turn on the TV or read the newspaper, it's hard to ignore the headlines: ''Colonial Pipeline a Victim of Massive Ransomware Attack.'' ''50 Million People Affected by T-Mobile Data Breach.'' ''Hackers Exploit SolarWinds to Spy on U.S. Government Agencies.''

These major attacks represent a serious threat to our economy and our national security. After the Colonial Pipeline attack impacted thousands of our neighbors in Central Virginia, I was adamant about how our government must vastly improve its efforts to undercut the activity of hackers, protect critical infrastructure, and strengthen our cybercrime prevention efforts.

But the story of cybercrime in 2021 goes far beyond these news-making cyberattacks—it extends into our communities, our neighborhoods, and our homes.

If you are a family banking online, a business managing your employees' payroll information, or a senior accessing federal benefits on the internet, you are no stranger to thinking about how a cyber breach or attack could affect you. Even worse, you might already be one of the millions of Americans whose personal data has been compromised, money or identity stolen, or safety put at risk.

In 2018, Gallup found that nearly one in four U.S. households has been a victim of cybercrime—making it the most common crime in America. To confront cybercriminals and their enablers, we need to have a better understanding of these incidents. However, many of these cases—a vast majority of these crimes—are not properly reported or tracked by law enforcement Often, they are not measured at all.

By some estimates, the Federal Bureau of Investigation (FBI) may only collect about one in 90 of all cybercrime incidents in its Internet Crime Complaint Center (IC3) database. The lack of information about cyber and cyber-enabled crime is divorced from what Americans are actually facing on a day-to-day basis an increased risk of cybercrime. What's more, these crimes are rising at an alarming rate.

Compounding this challenge is the fact that federal, state, and local governments do not have a comprehensive, effective system to measure cybercrime. In 2021—decades after the dawn of the internet age—we remain woefully unprepared to prevent or respond to the next generation of cyberattacks.

Accountability for these crimes—and protection against them—can't fully take shape until we have a clear picture of the current state of play. For this reason, we need to take real steps to improve how we track, measure, analyze, and prosecute cybercrime.

Earlier this month, I introduced the bipartisan Better Cybercrime Metrics Act, which would allow our federal government and law enforcement to better track and identify cybercrime, prevent attacks, and go after perpetrators. This bill would strengthen our understanding and our defenses against the phishing attempts, extortion, ransomware, and identity theft that are plaguing everyday Americans.

As a former federal law enforcement agent, I understand that local and state police and sheriff's departments are often strained for resources and time. And as a former CIA case officer, I recognize the importance of gathering as much information as possible about potential threats—so that we can prevent attacks on American citizens and American businesses.

If signed into law, the Better Cybercrime Metrics Act would improve our cybercrime metrics, anticipate future trends, and make sure law enforcement has the tools and resources they need.

Our bill would require federal reporting on the effectiveness of current cybercrime mechanisms and highlight disparities in reporting data between cybercrime data and other types of crime data.

Additionally, it would require the National Crime Victimization Survey to ask questions related to cybercrime in its surveys—and it would make sure that the FBI's National Incident Based Reporting System include cybercrime reports from federal, state, and local officials.

Notably, our bill would also require the U.S. Department of Justice to contract with the National Academy of Sciences to develop a standard taxonomy for cybercrime. These metrics could be used by law enforcement across the board.

I was proud to introduce this legislation alongside my colleagues U.S. Reps. Blake Moore (R–Utah), Andrew Garbarino (R–N.Y.), and Sheila Jackson Lee (D–Texas). Clearly, there is consensus for these reforms and protections across the political spectrum.

In the Senate, a companion bill is being led by Sen. Brian Schatz (D–Hawaii). Joining him are Thom Tillis (R–N.C.), John Cornyn (R–Texas), and Richard Blumenthal (D–Conn.). I am proud to have their partnership on this important, bicameral effort.

With this legislation and an improved understanding of the threats ahead, we can prevent more Americans from becoming targets—or victims—online.

Ms. JACKSON LEE. Mr. Speaker, I include in the RECORD the article titled: ''U.S. Military Has Acted Against Ransomware Groups, General Acknowledges.''

[From the New York Times, December 5, 2021]

U.S. MILITARY HAS ACTED AGAINST RANSOMWARE GROUPS, GENERAL ACKNOWLEDGES

(By Julian E. Barnes)

SIMI VALLEY, CALIF.—The U.S. military has taken actions against ransomware groups as part of its surge against organizations launching attacks against American companies, the nation's top cyberwarrior said on Saturday, the first public acknowledgment of offensive measures against such organizations.

Gen. Paul M. Nakasone, the head of U.S. Cyber Command and the director of the National Security Agency, said that nine months ago, the government saw ransomware attacks as the responsibility of law enforcement.

But the attacks on Colonial Pipeline and JBS beef plants demonstrated that the criminal organizations behind them have been ''impacting our critical infrastructure,'' General Nakasone said.

In response, the government is taking a more aggressive, better coordinated approach against this threat, abandoning its previous hands-off stance. Cyber Command, the N.S.A. and other agencies have poured resources into gathering intelligence on the ransomware groups and sharing that better understanding across the government and with international partners.

''The first thing we have to do is to understand the adversary and their insights better than we've ever understood them before,'' General Nakasone said in an interview on the sidelines of the Reagan National Defense Forum, a gathering of national security officials.

General Nakasone would not describe the actions taken by his commands, nor what ransomware groups were targeted. But he said one of the goals was to ''impose costs,'' which is the term military officials use to describe punitive cyberoperations.

''Before, during and since, with a number of elements of our government, we have taken actions and we have imposed costs;'' General Nakasone said. ''That's an important piece that we should always be mindful of.''

In September, Cyber Command diverted traffic around servers being used by the Russia-based REvil ransomware group, officials briefed on the operation have said. The operation came after government hackers from an allied country penetrated the servers, making it more difficult for the group to collect ransoms. After REvil detected the U.S. action, it shut down at least temporarily. That Cyber Command operation was reported last month by The Washington Post.

Cyber Command and the N.S.A. also assisted the F.B.I. and the Justice Department in their efforts to seize and recover much of the cryptocurrency ransom paid by Colonial Pipeline. The Bitcoin payment was originally demanded by the Russian ransomware group known as DarkSide.

The first known operation against a ransomware group by Cyber Command came before the 2020 election, when officials feared a network of computers known as TrickBot could be used to disrupt voting.

Government officials have disagreed about how effective the stepped-up actions against ransomware groups have been. National Security Council officials have said activities by Russian groups have declined. The F.B.I. has been skeptical. Some outside groups saw a lull but predicted the ransomware groups would rebrand and come back in force.

Asked if the United States had gotten better at defending itself from ransomware groups, General Nakasone said the country was ''on an upward trajectory.'' But adversaries modify their operations and continue to try to attack, he said.

''We know much more about what our adversaries can and might do to us. This is an area where vigilance is really important,'' he said, adding that ''we can't take our eye off it.''

Since taking over in May 2018, General Nakasone has worked to increase the pace of cyberoperations, focusing first on more robust defenses against foreign influence operations in the 2018 and 2020 elections. He has said that his commands have been able to draw broad lessons from those operations, which were seen as successful, and others.

''Take a look at the broad perspective of adversaries that we've gone after over a period of five-plus years: It's been nation-states, it's been proxies, it's been criminals, it's been a whole wide variety of folks that each require a different strategy,'' he said. ''The fundamental piece that makes us successful against any adversary are speed, agility and unity of effort. You have to have those three.''

Last year's discovery of the SolarWinds hacking, in which Russian intelligence agents implanted software in the supply chain, giving them potential access to scores of government networks and thousands of business networks, was made by a private company and exposed flaws in America's domestic cyberdefenses. The N.S.A's Cybersecurity Collaboration Center was set up to improve information sharing between the government and industry and to better detect future intrusions, General Nakasone said, although industry officials say more needs to be done to improve the flow of intelligence.

General Nakasone said those kinds of attacks are likely to continue, by ransomware groups and others.

''What we have seen over the past year and what private industry has indicated is that we have seen a tremendous rise in terms of implants and in terms of zero-day vulnerabilities and ransomware,'' he said, referring to an unknown coding flaw for which a patch does not exist. ''I think that's the world in which we live today.''

Speaking on a panel at the Reagan Forum, General Nakasone said the domain of cyberspace had changed radically over the past 11 months with the rise of ransomware attacks and operations like SolarWinds. He said it was likely in any future military conflict that American critical infrastructure would be targeted.

''Borders mean less as we look at our adversaries, and whatever adversary that is, we should begin with the idea that our critical infrastructure will be targeted:' he told the panel.

Cyber Command has already begun building up its efforts to defend the next election. Despite the work to expose Russian, Chinese and Iranian efforts to meddle in American politics, General Nakasone said in the interview that foreign malign campaigns were likely to continue.

''I think that we should anticipate that in cyberspace, where the barriers to entry are so low, our adversaries are always going to be attempting to be involved;'' he said.

The recipe for success in defending the election, he said, is to provide insight to the public about what adversaries are trying to do, share information about vulnerabilities and adversarial operations, and finally take action against groups trying to interfere with voting.

While that might take the form of cyberoperations against hackers, the response can be broader. Last month, the Justice Department announced the indictment of two Iranian hackers the government had identified as being behind an attempt to influence the 2020 election.

''This really has to be a whole-of-government effort,'' General Nakasone said. ''This is why the diplomatic effort is important. This is why being able to look at a number of different levers within our government to be able to impact these type of adversaries is critical for our success.''

Ms. JACKSON LEE. The roll call goes on and on and on.

I thank my colleagues for their words of support for this bipartisan legislation. I believe the time is now. We are going to continue this journey. This is not the last legislative initiative, that is why we will be holding a hearing tomorrow with the representative from the FBI because this is a growing continuing project and problem. If I might use the terminology, we will have to re-image constantly.

This legislation is also supported by law enforcement groups and those with particular expertise in cybercrime, including the National Fraternal Order of Police, the Major Cities Chiefs Association, and the National Association of Police Organizations, the National White Collar Crime Center, and the Cybercrime Support Network.

Mr. Speaker, I thank Senator SCHATZ, Senator TILLIS, and as I indicated, our colleague, Representative SPANBERGER for their leadership on this bipartisan legislation. I am glad to have joined it and I urge all of my colleagues to join me in supporting it.

Mr. Speaker, I yield back the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, I rise in support of S. 2629, the ''Better Cybercrime Metrics Act.''

This legislation improves our understanding and tracking of cybercrime so that we can do more to prevent it.

A 2018 Gallup poll found that one in four Americans has been a victim of cybercrime.

From stolen financial information, to system-wide shutdowns, to ransomware attacks, these crimes harm our families, our businesses, and our government.

The Council of Economic Advisers estimated that malicious cyber activities cost our economy as much as $109 billion in 2016, and experts believe these costs are growing.

The COVID–19 pandemic has increased opportunities for cybercrime, with increases in remote work and the time people spend online.

Hackers also took advantage of our recovery efforts, stealing identities to file fake unemployment claims or fraudulent loan applications.

Many of the victims of these scams only learned they were attacked when they went to file genuine claims and were told that one had already been submitted using their name or business.

Sadly, cyber criminals often target older Americans. In 2020, people over 60 accounted for the most complaints of any age group, as collected by the FBI Internet Crime Complaint Center.

People over 60 also had the greatest losses, with over $966 million lost to cybercrime in 2020.

We must do more to protect Americans from cybercrime, and that starts with a better understanding of what it is and how it occurs.

The Better Cybercrime Metrics Act will gather experts in law enforcement, business, and technology to create a taxonomy of cybercrime so that we can define it and classify it in a uniform way.

This legislation also adds cybercrime to two important law enforcement tools used to track crimes, the National Incident-Based Reporting System and the National Crime Victimization Survey.

Together these provisions will ensure that law enforcement has a complete picture of when and where cybercrime occurs, and who is harmed by it.

Finally, this bill directs the Government Accountability Office to conduct a study on reporting mechanisms for cybercrime, and the disparities in cybercrime data relative to other types of crime data.

Together this legislation will put in place the tools to clearly define and classify cybercrime, to track cybercrime, and to better understand this serious threat.

I commend Senators BRIAN SCHATZ and THOM TILLIS for their work on this bipartisan legislation. I also thank Representative ABIGAIL SPANBERGER for her leadership on the House companion to this bill. I was proud to stand with her in introducing the House companion, along with our Republican colleagues, Representative BLAKE MOORE and Representative ANDREW GARBARINO.

We must give law enforcement the tools to keep apace with new technology and to get a step ahead of the threats faced by our ever-evolving world.

This bill takes an important step in that effort and I urge my colleagues to support it.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from Texas (Ms. JACKSON LEE) that the House suspend the rules and pass the bill, S. 2629.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. CLYDE. Mr. Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

Pursuant to clause 8 of rule XX, further proceedings on this motion are postponed.

HOMICIDE VICTIMS' FAMILIES' RIGHTS ACT OF 2021

Ms. JACKSON LEE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3359) to provide for a system for reviewing the case files of cold case murders at the instance of certain persons, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3359

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Homicide Victims' Families' Rights Act of 2021''.

SEC. 2. CASE FILE REVIEW.

(a) IN GENERAL.—The head of an agency shall review the case file regarding a cold case murder upon written application by one designated person to determine if a full reinvestigation would result in either the identification of probative investigative leads or a likely perpetrator.

(b) REVIEW.—The review under subsection (a) shall include—

(1) an analysis of what investigative steps or follow-up steps may have been missed in the initial investigation;

(2) an assessment of whether witnesses should be interviewed or reinterviewed;

(3) an examination of physical evidence to see if all appropriate forensic testing and analysis was performed in the first instance or if additional testing might produce information relevant to the investigation; and

(4) an update of the case file using the most current investigative standards as of the date of the review to the extent it would help develop probative leads.

(c) CERTIFICATION IN LIEU OF REVIEW.—In any case in which a written application for review has been received under this Act by the agency, review shall be unnecessary where the case does not satisfy the criteria for a cold case murder. In such a case, the head of the agency shall issue a written certification, with a copy provided to the designated person that made the application under subsection (a), stating that final review is not necessary because all probative investigative leads have been exhausted or that a likely perpetrator will not be identified.

(d) REVIEWER.—A review required under subsection (a) shall not be conducted by a person who previously investigated the murder at issue.

(e) ACKNOWLEDGMENT.—The agency shall provide in writing to the applicant as soon as reasonably possible—

(1) confirmation of the agency's receipt of the application under subsection (a); and

(2) notice of the applicant's rights under this Act.

(f) PROHIBITION ON MULTIPLE CONCURRENT REVIEWS.—Only one case review shall be undertaken at any one time with respect to the same cold case murder victim.

(g) TIME LIMIT.—Not later than 6 months after the receipt of the written application submitted pursuant to subsection (a), the agency shall conclude its case file review and reach a conclusion about whether or not a full reinvestigation under section 4 is warranted.

(h) EXTENSIONS.—

(1) IN GENERAL.—The agency may extend the time limit under subsection (g) once for a period of time not to exceed 6 months if the agency makes a finding that the number of case files to be reviewed make it impracticable to comply with such limit without unreasonably taking resources from other law enforcement activities.

(2) ACTIONS SUBSEQUENT TO WAIVER.—For cases for which the time limit in subsection (g) is extended, the agency shall provide notice and an explanation of its reasoning to one designated person who filed the written application pursuant to this section.

SEC. 3. APPLICATION.

Each agency shall develop a written application to be used for designated persons to request a case file review under section 2.

SEC. 4. FULL REINVESTIGATION.

(a) IN GENERAL.—The agency shall conduct a full reinvestigation of the cold case murder at issue if the review of the case file required by section 2 concludes that a full reinvestigation of such cold case murder would result in probative investigative leads.

(b) REINVESTIGATION.—A full reinvestigation shall include analyzing all evidence regarding the cold case murder at issue for the purpose of developing probative investigative leads or a likely perpetrator.

(c) REVIEWER.—A reinvestigation required under subsection (a) shall not be conducted by a person who previously investigated the murder at issue.

(d) PROHIBITION ON MULTIPLE CONCURRENT REVIEWS.—Only one full reinvestigation shall be undertaken at any one time with respect to the same cold case murder victim.

SEC. 5. CONSULTATION AND UPDATES.

(a) IN GENERAL.—The agency shall consult with the designated person who filed the written application pursuant to section 2 and provide him or her with periodic updates during the case file review and full reinvestigation.

(b) EXPLANATION OF CONCLUSION.—The agency shall meet with the designated person and discuss the evidence to explain to the designated person who filed the written application pursuant to section 2 its decision whether or not to engage in the full reinvestigation provided for under section 4 at the conclusion of the case file review.

SEC. 6. SUBSEQUENT REVIEWS.

(a) CASE FILE REVIEW.—If a review under subsection (a) case file regarding a cold case murder is conducted and a conclusion is reached not to conduct a full reinvestigation, no additional case file review shall be required to be undertaken under this Act with respect to that cold case murder for a period of five years, unless there is newly discovered, materially significant evidence. An agency may continue an investigation absent a designated person's application.

(b) FULL REINVESTIGATION.—If a full reinvestigation of a cold case murder is completed and a suspect is not identified at its conclusion, no additional case file review or full reinvestigation shall be undertaken with regard to that cold case murder for a period of five years beginning on the date of the conclusion of the reinvestigation, unless there is newly discovered, materially significant evidence.

SEC. 7. DATA COLLECTION.

(a) IN GENERAL.—Beginning on the date that is three years after the date of enactment of this Act, and annually thereafter, the Director of the National Institute of Justice shall publish statistics on the number of cold case murders.

(b) MANNER OF PUBLICATION.—The statistics published pursuant to subsection (a) shall, at a minimum, be disaggregated by the circumstances of the cold case murder, including the classification of the offense, and by agency.

SEC. 8. PROCEDURES TO PROMOTE COMPLIANCE.

(a) REGULATIONS.—Not later than one year after the date of enactment of this Act, the head of each agency shall promulgate regulations to enforce the right of a designated person to request a review under this Act and to ensure compliance by the agency with the obligations described in this Act.

(b) PROCEDURES.—The regulations promulgated under subsection (a) shall—

(1) designate an administrative authority within the agency to receive and investigate complaints relating to a review initiated under section 2 or a reinvestigation initiated under section 4;

(2) require a course of training for appropriate employees and officers within the agency regarding the procedures, responsibilities, and obligations required under this Act;

(3) contain disciplinary sanctions, which may include suspension or termination from employment, for employees of the agency who are shown to have willfully or wantonly failed to comply with this Act;

(4) provide a procedure for the resolution of complaints filed by the designated person concerning the agency's handling of a cold case murder investigation or the case file evaluation; and

(5) provide that the head of the agency, or the designee thereof, shall be the final arbiter of the complaint, and that there shall be no judicial review of the final decision of the head of the agency by a complainant.

SEC. 9. WITHHOLDING INFORMATION.

Nothing in this Act shall require an agency to provide information that would endanger the safety of any person, unreasonably impede an ongoing investigation, violate a court order, or violate legal obligations regarding privacy.

SEC. 10. MULTIPLE AGENCIES.

In the case that more than one agency conducted the initial investigation of a cold case murder, each agency shall coordinate their case file review or full reinvestigation such that there is only one joint case file review or full reinvestigation occurring at a time in compliance with section 2(f) or 4(d), as applicable.

SEC. 11. APPLICABILITY.

This Act applies in the case of any cold case murder occurring on or after January 1, 1970.

SEC. 12. DEFINITIONS.

In this Act:

(1) The term ''designated person'' means an immediate family member or someone similarly situated, as defined by the Attorney General.

(2) The term ''immediate family member'' means a parent, parent-in-law, grandparent, grandparent-in-law, sibling, spouse, child, or step-child of a murder victim.

(3) The term ''victim'' means a natural person who died as a result of a cold case murder.

(4) The term ''murder'' means any criminal offense under section 1111(a) of title 18, United States Code, or any offense the elements of which are substantially identical to such section.

(5) The term ''agency'' means a Federal law enforcement entity with jurisdiction to engage in the detection, investigation, or prosecution of a cold case murder.

(6) The term ''cold case murder'' means a murder—