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" and "tumblers" 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”.