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

Questions from Senator Tillis:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Questions from Senator Grassley:

1. What do you see as our options to best deter and punish state-affiliated ransomware attacks?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Questions from Senator Sasse:

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

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

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

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

b. Should public attribution inherently lead to OFAC designations?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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