Department of Justice

STATEMENT OF

SUJIT RAMAN
ASSOCIATE DEPUTY ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE

SUBCOMMITTEE ON CRIME AND TERRORISM
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"CYBER THREATS TO OUR NATION'S CRITICAL INFRASTRUCTURE"

PRESENTED

AUGUST 21, 2018

STATEMENT OF
SUJIT RAMAN
ASSOCIATE DEPUTY ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE
SUBCOMMITTEE ON CRIME AND TERRORISM
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED
"CYBER THREATS TO OUR NATION'S CRITICAL INFRASTRUCTURE"

PRESENTED
AUGUST 21, 2018

Good afternoon Chairman Graham, Ranking Member Whitehouse, and distinguished Members of the Subcommittee. Thank you for the opportunity to testify on behalf of the Department of Justice regarding our efforts to combat cyber threats.

The Attorney General identified this issue as a priority when he created a Cyber-Digital Task Force within the Department earlier this year. I have the privilege of chairing this Task Force, and as you know, last month the Task Force issued a public report that provides a comprehensive assessment of the cyber-enabled threats confronting our Nation. The Department appreciates the Subcommittee's interest in making sure that the Department has the tools it needs to disrupt and deter cyber actors who seek to do our Nation harm.

As I describe below, the Department's principal role in responding to cyber threats is the investigation and prosecution of federal crimes, but our investigations can yield more than criminal charges. The Department is committed to using all of the tools at our disposal, including civil injunctions, information sharing, and technical operations, to counter malicious cyber activity, as well as to support our federal partners' tools, like economic sanctions, diplomatic pressure, intelligence operations, and military action. Successfully protecting the Nation from cyberattacks also requires robust information sharing with the private sector, which is why we work with other departments and agencies to share cybersecurity information beyond the federal government.

I will cover three areas in my testimony today. First, I will describe the seriousness of the cyber threats to our critical infrastructure, which includes our election systems. Second, I will discuss how the Department of Justice is responding to those threats, as described in our recent Task Force report. Finally, I will address some of the ways in which Congress can promote the Department's mission to combat cyber threats, including those aimed at the Nation's critical infrastructure.

I. Cyber Threats to U.S. Critical Infrastructure

Cyber threats to critical infrastructure deserve particular attention, because our Nation's critical infrastructure provides the essential services that underpin American society and serves as the backbone of our economy, security, and health systems. Critical infrastructure includes the financial services sector, the electrical grid, dams, electoral systems, and over a dozen other sectors of society. Those assets, systems, and networks are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on our national security, national economic security, or our national public health or safety — or any combination thereof.[1] Our adversaries seek to identify and exploit vulnerabilities in the sophisticated computer networks that these sectors employ.

It is important to note that private entities own and operate the vast majority of the Nation's critical infrastructure. Therefore, securing U.S. critical infrastructure is a shared responsibility. The Department recognizes that the private sector requires timely cyber threat information to secure its systems. Accordingly, the Federal Bureau of Investigation ("FBI") makes threat information available to affected sectors through briefings and widely distributed technical alerts developed jointly with the Department of Homeland Security ("DHS"). In March 2018, for example, the FBI and DHS announced that Russian government cyber actors had "targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors."[2] The technical alert described a multistage Russian intrusion campaign that compromised small commercial facilities' networks. Russian cyber actors used the networks to stage malware and to conduct spear-phishing attacks, which allowed the Russians to gain remote access into energy sector networks. The Russian cyber actors then explored those networks and moved across the networks to collect information pertaining to Industrial Control Systems. To respond to this nefarious cyber activity, information uncovered as part of this investigation led, at least in part, to economic sanctions against Russia when the Treasury Department announced sanctions against five Russian entities and nineteen Russian individuals on March 15, 2018.[3]

---

[1] 42 U.S.C. § 5195c(e).

[2] Alert TA18-074A, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure," U.S. COMPUTER EMERGENCY READINESS TEAM, U.S. DEPT. OF HOMELAND SECURITY (March 15, 2018), available at: https://www.us-cert.gov/ncas/alerts/TA18-074A (last accessed August 7, 2018). For information regarding more recent Russian cyber threats, *see, e.g.*, Press Release, "Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices," U.S. DEPT. OF JUSTICE (May 23, 2018), available at: https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected (last accessed August 7, 2018).

[3] Press Release, "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks," U.S. DEPT. OF TREASURY (March 15, 2018), available at: https://home.treasury.gov/index.php/news/press-releases/sm0312 (last accessed August 7, 2018).

Cyber operations could also target our election systems. For example, adversaries could use cyber-enabled means to target voter registration databases and voting machines. In fact, the Intelligence Community assessed in 2017 that Russian intelligence "accessed elements of multiple state or local electoral boards" during the 2016 U.S. presidential election.[4] DHS has assessed that the types of systems the Russian cyber actors targeted or compromised were not involved in vote tallying,[5] and to our knowledge, no foreign government has succeeded in perpetrating ballot fraud. Nonetheless, the risk is real. Securing these systems and ensuring the integrity of our elections is one of our utmost priorities.

Russia is not the only state sponsor of malicious cyber activity. To take one prominent publicly available example, we know that the Iranian government has targeted our critical infrastructure, specifically our financial sector, with cyberattacks. In response, in March 2016, a federal grand jury indicted seven Iranian hackers belonging to two companies that worked for Iran's Islamic Revolutionary Guard Corps for their role in Distributed Denial of Service ("DDoS") attacks targeting the public-facing websites of nearly fifty U.S. banks. These DDoS attacks against the U.S. financial sector began in approximately December 2011, and occurred sporadically until September 2012, at which point they escalated in frequency to a near-weekly basis. At their peak, the attacks disrupted hundreds of thousands of customers' ability to access their accounts online and conduct transactions, and the affected banks' remediation costs ran into the tens of millions of dollars. Furthermore, one of the hackers also repeatedly gained access to the Supervisory Control and Data Acquisition ("SCADA") system of a dam in New York, allowing him to obtain information regarding the dam's status and operation.[6]

To take another example — this one involving North Korea — in May 2018, the FBI and DHS issued a technical alert notifying the public about the FBI's high confidence that malicious North Korean government cyber actors have been using malware since at least 2009 "to target multiple victims globally and in the United States," across various sectors — including critical infrastructure sectors.[7]

These examples highlight the varied nature of the cyber threats to our Nation's critical infrastructure. Preventing and responding to cyber intrusions and attacks requires a strong defense using a coordinated government approach, with the support of the private sector. The Department of Justice plays an important role in this combined effort.

---

[4]Office of the Director of National Intelligence, Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections": The Analytic Process and Cyber Incident Attribution 2 (Jan. 2017) ("ODNI Report"), available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf (last accessed August 7, 2018).

[5]*Id*.

[6]*See* Indictment in *United States v. Ahmad Fathi, et al*., No. 16-CRM-48 (S.D.N.Y., March 24, 2016), available at: https://www.justice.gov/opa/fle/834996/download (last accessed August 7, 2018).

[7]Alert TA18-149A, "HIDDEN COBRA – Joanap Backdoor Trojan and Brambul Server Message Block Worm," U.S. COMPUTER EMERGENCY READINESS TEAM, U.S. DEPT. OF HOMELAND SECURITY (last revised May 31, 2018), available at: https://www.us-cert.gov/ncas/alerts/TA18-149A (last accessed August 7, 2018).

II. The Department of Justice's Role in Combating Cyber Threats

The Department of Justice's core mission is to investigate and prosecute federal crimes, including computer intrusions and attacks, whether perpetrated by a transnational criminal group, a lone hacker, or an officer of a foreign military or intelligence service. Our primary role is to investigate those incidents, determine who was responsible, prosecute them where the evidence supports it, and share intelligence we gather in connection with our investigations. We work closely with our partners across the Government and around the world to arrest such actors, extradite them, prosecute them, and obtain restitution for victims whenever possible. Further, through our Office of Justice Programs, we also support training law enforcement, prosecutors, and public safety officers in cyber-related crimes, both through online and classroom training. This training assists in identifying cyber crimes and infrastructure intrusions, in preparation for either possible State or federal prosecution.

These partnerships across the Government are important. To take election infrastructure as an example, other Departments, like DHS, are primarily responsible for designing security standards, helping protect private and government networks, and assisting victims in their recovery from cyberattacks. By contrast, we are responsible for investigating intrusions and attacks, figuring out who perpetrated them, and bringing those malicious actors to justice. Based on our cyber investigations, we also share cybersecurity threat information to help victims protect themselves.

As I mentioned at the outset, the Attorney General has prioritized the Department's efforts to combat cyber-enabled threats. The report that the Attorney General's Cyber-Digital Task Force issued last month discusses in detail our extensive efforts to help secure the Nation.

The report begins in chapter 1 by focusing on the threat posed by malign foreign influence operations. We define such operations as covert actions by foreign governments that are intended to sow division in our society, undermine confidence in our democratic institutions, and otherwise affect political sentiment and public discourse to achieve strategic geopolitical objectives. While cyber operations that target election systems (such as voting machines and voter databases) and related infrastructure represent one aspect of the problem, foreign malign influence operations also are designed to affect the views of American voters, depress voter turnout, or undermine confidence in election results. Chapter 1 of the Task Force report categorizes these operations and outlines the Department's framework to counter them ahead of the 2018 midterm elections. The chapter also describes the work of the FBI's Foreign Influence Task Force, which integrates the FBI's cyber, counterintelligence, counterterrorism, and criminal law enforcement resources to better counter malign foreign influence operations. Finally, chapter 1 announces a new disclosure policy pursuant to which the Department will notify victims, social media providers, or the public, as appropriate, regarding efforts by foreign adversaries to target them in connection with a malign foreign influence operation.

As the Cyber-Digital Task Force report observes, the Department of Justice plays an important role in combating foreign efforts to interfere in our elections, but the Department is only one part of an effective response. Combating foreign influence operations requires a whole-of-society approach involving coordinated actions by federal, State, and local government agencies, including State and local agencies that are responsible for election systems; cooperation from victims and the private sector, including social media companies; and the active engagement of an informed public.

In chapters 2 and 3, the Task Force report discusses other significant cyber-enabled threats confronting our Nation, including attacks intended to damage computer systems; data theft; fraud schemes; crimes threatening personal privacy, such as sextortion and other forms of blackmail and harassment; and attacks on critical infrastructure. These chapters detail the important work that the Department of Justice is doing to keep America safe in the face of these complex and evolving threats. Chapter 4 focuses on a critical aspect of the Department's mission in which the FBI plays a lead role, namely, responding to cyber incidents. Chapter 5 then turns inward, focusing on the Department's efforts to recruit and train our own personnel on cyber matters. Finally, the report concludes in chapter 6 with observations about certain priority policy matters, including how the global nature of cyber-enabled crime brings with it technological and legal impediments to the Department's ability to identify and locate malicious actors and bring them to justice, as well as other ideas discussed below.

We hope that the report provides the Subcommittee and the public with a better understanding of the Department's role in combating cyber threats; the tools we rely on to confront these threats; how we support other government efforts to address these threats; and the challenges we continue to face.

III. New Ideas to Combat Cyber Threats

In the face of these disturbing and ever-increasing threats, I know the Subcommittee has on its mind a key question: How can Congress help, today? The Department continues to explore how to respond to today's threat of malign foreign influence and whether additional enforcement and disclosure tools would be useful and appropriate. In the meantime, as our Task Force concluded, there are several key changes to federal law that would greatly aid our work to combat threats online.

I first want to thank this Subcommittee and, specifically, the Chair and Ranking Member, for their leadership in shepherding the passage of the Clarifying Lawful Overseas Use of Data ("CLOUD") Act earlier this year. This important piece of legislation will greatly advance the Department's work and will enhance both security and privacy around the world. We appreciate that Congress has made clear that U.S. law-enforcement orders issued under the Stored Communications Act require the disclosure of data wherever a provider chooses to store that data. The impact of this clarification was immediate and dramatic, making Americans safer and investigations more efficient. As you know, the CLOUD Act also creates incentives for bilateral

agreements that enable investigators to seek data without causing unnecessary conflicts of laws. These bilateral agreements will help create more efficient processes among rights-respecting countries for solving crime, and will ease the burden on our Nation's mutual legal assistance procedures.

The CLOUD ACT has helped address one of the key challenges facing law enforcement in the area of cybercrime, but many others still exist. I would like to spend most of my time today focusing on areas of concern in the Computer Fraud and Abuse Act ("CFAA") and related statutes that currently hamper our work to combat threats online. The CFAA is the primary federal law against hacking. It protects the public against criminals who intrude into computers to steal information, install malicious software, and delete files. It was also intended to criminalize malicious conduct by insiders who abuse their right of access to computer systems and networks to commit online crime. The CFAA, in short, reflects our baseline expectation that people are entitled to have control over their own computers and are entitled to trust that the information they store in their computers remains safe.

The CFAA was enacted in 1986, at a time when the problem of online crime was still in its infancy. Over the years, Congress has enacted a series of measured, modest changes to the CFAA to encompass new technologies and to equip law enforcement to respond to changing threats. The CFAA has not been amended since 2008, however, and the intervening years have again witnessed the need for the enactment of modest, incremental changes. The CFAA needs to be updated to make sure that it continues to appropriately deter violations of Americans' privacy and security.

A. Deterring insider threats

The CFAA is a privacy statute. It deters criminals from stealing peoples' information. Yet, the CFAA's privacy protections now contain a significant gap. The statute was meant to apply both to hackers who gain access to victim computers without authorization from halfway around the world, and to so-called "insiders" who have some authorization to access a computer — like company employees entitled to access a sensitive database for specified work purposes — but who intentionally abuse that access. The part of the CFAA that covers the conduct of those who have some authorization to access a computer is the tool that Department prosecutors have used to charge, for example, police officers who misuse their access to confidential criminal records databases in order to look up sensitive information about a boyfriend or girlfriend, who sell access to private records to others, or who provide confidential law enforcement information to a charged drug trafficker. As a recent survey of 472 cybersecurity professionals indicated, 90% percent of organizations feel vulnerable to insider attacks, and 53% have confirmed insider attacks against their organization in the previous 12 months. The survey also found that the type of data most vulnerable to insider attacks is

confidential business information, and that a plurality of those surveyed estimated that the potential cost/loss of an insider attack was between $100,000 and $500,000.[8]

Unfortunately, recent judicial decisions have limited the Government's ability to prosecute such cases. As a result of these decisions, insiders cannot be charged under the CFAA — even where the insider has intentionally exceeded the bounds of his legitimate access to confidential information and has caused significant harm to his employer and to the people, often everyday Americans, whose data he has improperly accessed.

The insider threat is relevant to voting security. Currently, for example, if a foreign hacker accessed a State's voter registration database over the Internet, that could be charged under the CFAA as an access "without authorization." But if an insider, such as a State government employee, used his privileges to access the same information, that insider could not be prosecuted under the CFAA, at least as several courts have interpreted the statute.

The narrow judicial interpretation of the term "exceeds authorized access" in the CFAA stems from concerns that the statute potentially makes relatively trivial conduct a federal crime. One frequently cited hypothetical along these lines is the theoretical threat of prosecution faced by an employee who uses the Internet to check baseball scores at lunchtime in violation of his employer's strict business-only Internet use policy. We understand the concerns of the courts, and I would like to reiterate that the Department of Justice has no interest in prosecuting harmless violations of use restrictions like these.

However, by essentially barring all CFAA prosecutions of insiders, these court decisions have constrained our ability to bring certain cybercriminals to justice. Over the last several years, numerous Department of Justice officials have called on Congress to address this issue in a manner that would maintain the law's key privacy-protecting function, while ensuring that trivial violations of things like a website's terms of service do not constitute federal crimes.

The Department supports efforts that would accomplish this task. This can be done by clarifying that the definition of "exceeds authorized access" includes the situation where the person accesses the computer for a purpose that he knows is not authorized by the computer owner. This clarification is necessary to permit the prosecution of, for example, a law enforcement officer who is permitted access to criminal records databases, but only for official business purposes. At the same time, a legislative fix could add new limitations to make clear that trivial conduct does not constitute a crime. For example, a limitation could be put into the CFAA making clear that in order to constitute a crime under the new insider provision, not only must an offender access a protected computer in excess of authorization and obtain information, but the information must be worth $5,000 or more, the access must be in furtherance of a separate felony offense, or the information must be stored on a government computer.

---

[8]Crowd Research Partners, "Insider Threat: 2018 Report," available at: http://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf (last accessed August 7, 2018).

We strongly believe that the insider threat problem in the CFAA can be fixed in a way that ensures the CFAA does not inadvertently cover trivial conduct, while empowering the Department to prosecute and deter significant threats to privacy and security. Of all of the reforms to the CFAA under consideration by this Subcommittee, addressing this problem would have the most immediate, significant impact in improving our ability to punish and deter cybercriminals. We would like to work closely with Congress and, specifically, this Subcommittee, to find a way forward on this pressing issue.

B. Certain malicious activities as RICO predicates

We support the efforts in the proposed International Cybercrime Prevention Act ("ICPA"), sponsored by the Chair and Ranking Member, to update the Racketeering Influenced and Corrupt Organizations Act ("RICO") to make CFAA offenses and certain Wiretap Act offenses subject to RICO. As computer technology has evolved, it has become a key tool of organized crime. Criminal organizations operating around the world hack into public and private computer systems, including systems key to America's national security and defense. They hijack computers to steal Americans' identity and financial information; they extort American businesses with threats to disrupt computers; and they commit a range of other online crimes.

Accordingly, much of the fight against transnational organized crime has moved online. federal prosecutors have used RICO for over forty years to prosecute organized criminals ranging from mob bosses to Hells Angels to members of MS-13. Just as RICO has proven to be an effective tool to prosecute the leaders of these organizations who may not have been directly involved in committing the underlying crimes, it should be a tool to fight criminal organizations that use computer intrusions and other CFAA violations to further their schemes. These changes, as proposed in ICPA, would simply make clear that all types of CFAA violations should be considered criminal activities under the RICO statute, with the associated heavy penalties.

C. Protecting election computers from attack

Protecting election infrastructure from attack is another important goal. Yet, as the Department's recent Cyber-Digital Task Force report noted, "should hacking of a voting machine occur, the government would not, in many conceivable circumstances, be able to use the CFAA to prosecute the hackers." The CFAA's current definition of "protected computer" includes computers "affecting interstate or foreign commerce," a definition that attempts to encompass the breadth of congressional power under the Commerce Clause. We are concerned that courts might conclude that the Commerce Clause power, alone, does not reach voting machine computers that are not used in a commercial setting, are not used in interstate communication, and are typically never connected to the Internet or to any other network. We believe, however, that Congress could reach such hacking by other means, such as its power to regulate federal elections in Article I, Section 4, of the Constitution.

Expanding the definition of a protected computer to include electronic voting machines will strengthen confidence in the integrity of our electoral system and ensure that any attempts to manipulate the results of an election can be prosecuted to the fullest extent under federal law. We therefore applaud the introduction of S. 3311, which would accomplish this important goal.

D. Botnets

Another striking example of online crime that victimizes Americans is the threat from botnets — networks of victim computers surreptitiously infected with malicious software, or "malware." Once a computer is infected with malware, it can be controlled remotely from another computer with a so-called "command and control" server. Using that control, criminals can steal usernames, passwords, and other personal and financial information from the computer user, or hold computers and computer systems for ransom. Criminals can also use armies of infected computers to commit other crimes, such as DDoS attacks, or to conceal their identities and locations while perpetrating crimes ranging from drug dealing to online child sexual exploitation.

The scale and sophistication of the threat posed by botnets is increasing every day. Individual hackers and organized criminal groups are using state-of-the-art techniques to infect hundreds of thousands — sometimes millions — of computers and cause massive financial losses, all while becoming increasingly difficult to detect. If we want security to keep pace with criminals' technological innovations, we need to ensure that we have a variety of effective tools to combat rapidly evolving cyber threats like these.

One powerful tool that the Department has used to disrupt botnets and free victim computers from criminal 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 in 2014. (The Gameover Zeus botnet, which infected computers worldwide, inflicted over $100 million in losses on American victims alone, many of them small- and medium-sized businesses.) 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 limited categories of crimes, including certain frauds and illegal wiretapping. Botnets, however, can be used for many different types of illegal activity. They can be used to steal sensitive corporate information, to harvest email account addresses, to hack other computers, or to execute denial of service attacks against websites or other computers. Yet — depending on the facts of any given case — these crimes may not constitute fraud or illegal wiretapping. In those cases, courts may lack the statutory authority to consider an application by prosecutors for an injunction to disrupt

the botnets in the same way that injunctions were successfully used to incapacitate the Coreflood and Gameover Zeus botnets.

Thus, we support the provision in ICPA that would add activities like the operation of a botnet to the list of offenses eligible for injunctive relief. ICPA would allow the Department to seek an injunction to prevent ongoing hacking violations in cases where 100 or more victim computers have been hacked. This numerical threshold focuses the injunctive authority on enjoining the creation, maintenance, operation, or use of a botnet, as well as other widespread attacks on computers using malicious software (such as ransomware).

The same legal safeguards that currently apply to obtaining civil injunctions, and that applied to the injunctions obtained by the Department in the Coreflood and Gameover Zeus cases, would also apply under the ICPA proposal. Before an injunction is issued, the Government must civilly sue the defendant and demonstrate to a court that it is likely to succeed on the merits of its lawsuit and that the public interest favors an injunction; the defendants and enjoined parties have the right to notice and to have a hearing before a permanent injunction is issued; and the defendants and enjoined parties may move to quash or modify any injunctions that the court issues.

I would now like to turn to the criminal statutes that prohibit the creation and use of botnets. Unfortunately, these statutes also contain shortcomings. We find that criminals continue to find new ways to make money illegally through botnets. Law enforcement officers now frequently observe that creators and operators of botnets not only use botnets for their own illicit purposes, but also sell or even rent access to the infected computers to other criminals.

Current criminal law prohibits the *creation* of a botnet because it prohibits hacking into computers without authorization. It also prohibits the *use* of botnets to commit other crimes. But it is not similarly clear that the law prohibits 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 accordingly "bought" the botnet from the criminal and notified the 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. While trafficking in botnets is sometimes chargeable under other subsections of the CFAA, this problem has resulted in, and will increasingly result in, the inability to prosecute individuals selling or renting access to thousands of hacked computers.

We believe that it should be illegal to sell or rent surreptitious control over infected computers to another person, just like it is already clearly illegal to sell or transfer computer passwords. That is why we support the provision in ICPA to 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. In addition, we recommend replacing the current requirement that the Government prove that the offender had an "intent to defraud" with a requirement to prove that

the offender not only knew his conduct is "wrongful," but also that he knew or should have known that the means of access would be used to hack or damage a computer. This last change is necessary because, as noted above, criminals do not use botnets only to commit fraud — they also use them to commit a variety of other crimes.

Some commentators have raised the concern that this proposal would chill the activities of legitimate security researchers, academics, and system administrators. The Department takes this concern seriously. We have no interest in prosecuting such individuals, and our proposal would not prohibit legitimate activity. That is because the Government should have the burden to prove, beyond a reasonable doubt, that the individual intentionally undertook an act (trafficking in a means of access) that he or she knew to be wrongful. The Government should similarly have to prove that the individual knew or had reason to know that the means of access would be used to commit a crime by hacking someone else's computer without authorization.

ICPA's approach makes clear that ordinary conduct by legitimate security researchers and others is not a crime. We believe that ICPA's botnet injunction provision strikes the proper balance in prohibiting the pernicious conduct I have described without chilling the activities of those who are trying to improve cybersecurity for us all.

E. Enhanced penalties for malicious activity directed at critical infrastructure

The Department also supports the efforts in ICPA to strengthen the criminal code to better deter malicious activities directed at computers and networks that control our critical infrastructures. As I have discussed, America's open and technologically complex society includes, as a part of its critical infrastructure, numerous vulnerable targets. While the CFAA's maximum penalties apply to malicious efforts to harm the computers and networks that run our critical infrastructure, the statute does not currently require any enhanced penalties for such conduct. While it is reasonable to believe that judges would impose appropriate prison terms if malicious activity severely debilitates a critical infrastructure system, it is possible that courts may not impose adequate penalties for activities that cause less disruption — and they could conceivably impose no penalty at all in the case of an attempt that is thwarted before it is completed.

In light of the grave risk posed by those who might compromise our critical infrastructure, the Department believes that the enhanced penalties for such malicious activity called for in ICPA not only will appropriately punish offenders, but also will more effectively deter others who would engage in misconduct that puts public safety and national security at risk. Criminals and other malicious actors should know that any attempt to damage a vital national resource will result in serious consequences.

F. Updated tools for investigators and prosecutors

We have long had concerns about the text of the "Pen Register and Trap and Trace" ("PRTT") statute that is used, among other things, to support computer security. The PRTT statute's exceptions — which, for example, permit a provider, but not a user, of wire or electronic communications services to monitor their own network — are subtly and inexplicably different than the Wiretap Act's exceptions. The existing language in the PRTT statute has been difficult to apply, resulting in complex legal analyses for services as simple as Caller ID. The Wiretap Act's rules appropriately protect the content of communications; they are more than adequate to protect non-content information, which is much less sensitive. Importing the Wiretap Act's exceptions into the PRTT statute would remedy these problems and result in a more logical framework for applying these two related statutes that regulate the real-time collection of communications. There is no reason why a user of a PRTT device, whether a private or governmental entity, should be precluded from logging his or her own communications. We have proposed language under which the PRTT statute would continue to protect user privacy, but it would no longer inappropriately limit private entities' or the Government's ability to use PRTT devices on their own computer networks.

Finally, we support several amendments to the CFAA, which are reflected in the ICPA. Key amongst these changes would be amendments to 18 U.S.C. § 2513, which would bring the forfeiture provisions of the CFAA in line with other federal criminal statutes, providing concrete procedures for the forfeiture of property used to commit or facilitate a violation of this statute as well as the proceeds of such violation. These amendments support consistent application of the law, while maintaining the Government's ability to dismantle and disrupt criminal operations and deter future violations, both when prosecutors are able to reach violators and when those violators are located overseas beyond the judicial reach of our courts. The amendments in ICPA are a measured and sensible addition that will help assure that criminal hackers do not profit from their crimes.

We also support the change in ICPA that would make the sale or advertising of a surreptitious interception device under 18 U.S.C. § 2512 a predicate offense under the federal money laundering statutes. Section 2512, which is part of the Wiretap Act, has proven to be a valuable tool for protecting the privacy of innocent Americans by criminalizing the manufacture, distribution, possession, and advertising of devices, such as spyware, that unlawfully collect private communications. Section 2512 is not a predicate offense under 18 U.S.C. §§ 1956 and 1957, however, which impedes the Government's ability to punish and deter certain offenders who conceal and spend their ill-gotten gains by selling and advertising spyware and other illegal interception devices.

IV. Conclusion

I want to thank the Subcommittee again for providing me this opportunity to discuss these important issues on behalf of the Department of Justice. Americans should be able to turn to the Government for leadership, especially when facing cyberattacks from nation states and from equally sophisticated criminals. We look forward to continuing to work with Congress to improve the Government's ability to respond to these cyber threats. I am happy to answer any questions you may have.