Statement of Laura Parsky,
Deputy Assistant Attorney General
United States Department of Justice
U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Crime,
Terrorism and Homeland Security

Legislative Hearing on H.R. 5318, the "Cyber-Security Enhancement and Consumer Data Protection Act of 2006"

May 11, 2006

Good morning, Mr. Chairman, Ranking Member Scott, and Honorable Members of the Subcommittee. I am very pleased to be able to testify today to share with you the Department's view of the cybercrime problem and how we have responded to that problem and to describe what we see as the legislative needs in this important area.

I. THE CYBERCRIME LANDSCAPE

I would like to begin by giving you some perspective on the threat cybercrime poses to our security, our privacy, and our economy. Through our investigations and prosecutions over the past several years, we have begun to see a pattern emerge: hackers who at one time might have broken into computers out of curiosity or for "bragging rights" have turned to exploiting that access for financial gain.

This trend can be seen in a number of areas. Where several years ago a hacker might have invaded the security of a business or government agency simply for the thrill of breaking in, that individual is now much more likely to steal databases of personal information to sell to identity thieves on the black market. Indeed, an underground economy has developed where criminals, often residing overseas, buy and sell credit card numbers and bank account information. Some of these identity thieves advertise the fact that they have access to literally

millions of stolen credit card records. Although law enforcement has made inroads into addressing this problem, it appears to be getting worse.

The profit motive is also apparent in the use of malicious spyware. In one recent prosecution in the Southern District of California, for example, a criminal defendant is alleged to have commercially marketed a program that any buyer could secretly send in an email attachment to an ex-girlfriend or an estranged spouse. Marketed as "loverspy," this program would intercept all of the communications of the person using that computer and send them to the person who bought the program. Five individuals have been indicted in the Southern District of California to date for selling or using this program. Four of these defendants have pled guilty and are awaiting sentencing. Additional convictions relating to this case have been obtained in federal courts in Charlotte, North Carolina, Dallas, Texas, and Honolulu, Hawaii. Additional indictments are pending in Kansas City, Missouri, and Houston, Texas.

Criminals also commonly use malicious spyware as part of "phishing" schemes - the sending of spam email messages to unsuspecting users in an effort to obtain their credit card numbers and other financial information. By appearing to be a message from the user's bank, some of these messages try to trick users into giving up their bank account numbers and passwords. Other phishing schemes cause spyware to be installed on the user's computer that grabs the user's information, intercepts the user's communications, and sends it all back to the criminal. Because it is so cheap to send out millions of phishing emails, even a success rate of less than 5 percent allows the criminals to commit widespread fraud. Computer security experts estimated that in 2005 over $ 2 billion were stolen through unauthorized access to U.S. bank accounts.

The trend of computer crimes being driven by the allure of easy money is also evident in the growing prevalence of "botnets." While five years ago viruses and worms were often disseminated just to destroy networks or to gain notoriety, today they are used to make money. For example, worms often illegally install a kind of malicious software called a "bot" on the victim's computer. These "bots" can gain complete control over the computer and report back for instructions to the person who sent them. Such "bot herders" can gain control over thousands of computers in this way, forming a "botnet" - a kind of clone army that can be deployed either individually or as a group. Symantec recently estimated that four million computers are currently infected with bots.

Clever criminals have figured out how to exploit botnets to make money. Bot herders can send illicit spam emails through bots, thus obscuring the origin of the spam and making it harder for Internet service providers to block. Of course, such spam can also include the phishing schemes mentioned above. Bot herders also earn money by causing advertising to appear on a bot-infected computer's screen. And perhaps most perniciously, botnets have the combined power to knock other computers offline. Companies have paid to have such "distributed denial of service attacks" (or "DDOS attacks") render their competitors' websites inoperable, and bot herders have extorted hundreds of thousands of dollars from businesses and individuals by threatening to do so. Computer security experts estimate that denial of service attacks occurred approximately 1,400 times a day in 2005.

Not surprisingly, bot herders have found an additional way to profit from this general-purpose criminal tool: they have rented and sold botnets to anyone willing to pay. By this means, botnets can fall into the hands of any criminal, even one without the technical skill to create a botnet.

Consistent with these patterns, surveys show that the number of breaches of computer security remains high. The 2005 report produced by the Computer Security Institute and the Federal Bureau of Investigation ("FBI") found that about seventy-five percent of respondents suffered attacks from computer viruses, such as those used to infect computers with "bots." The report also showed that the incidence of attacks on wireless computer networks has continued to increase. Finally, the report revealed that victims of computer crime are consistently failing to report such incidents to law enforcement. Indeed, reporting to law enforcement dropped to only twenty percent, the lowest level recorded in the ten years that the study has been conducted.

Moreover, these attacks on computer networks threaten the stability of our modern economy, which has become increasingly reliant on such networks, and threaten our national security. Many of our critical national infrastructures - such as transportation, electricity transmission, and banking and finance - rely on the security and reliability of computer network communications. Any disruption of these networks, whether it is through criminal activity or terrorist acts, can cause widespread harm. This reality makes it all the more critical that we be able to respond quickly to threats to these networks and appropriately deter such misconduct.

II. THE LAW ENFORCEMENT RESPONSE

In response to this rapidly evolving problem, the Department of Justice has worked swiftly and decisively to address these growing threats. The cornerstone of the Department's prosecutorial efforts is the Computer Crime and Intellectual Property Section, a highly trained team of 40 expert prosecutors who specialize in coordinating multi-district and international investigations of computer crime and intellectual property offenses.

The Computer Crime and Intellectual Property Section trains, supports, and works closely with Computer Hacking and Intellectual Property ("CHIP") prosecutors in each of the 94

U.S. Attorneys' Offices. CHIP prosecutors are specially trained in computer crime and intellectual property prosecutions, and they work both individually and together to ensure a strong and coordinated domestic enforcement effort. In addition to individual CHIP attorneys, there are now 18 CHIP Units throughout the country. The CHIP prosecutors, CHIP Units, and CCIPS work closely with the FBI, the U.S. Secret Service ("Secret Service") and the Bureau of Immigration and Customs Enforcement ("ICE") of the Department of Homeland Security, and other investigative agencies.

The FBI has made cybercrime, including fraud, hacking, child pornography, and intellectual property crime on the Internet, one of its top three enforcement priorities. To this end, the FBI has ensured there is a cyber expert in each of its 56 field offices, and in many of these offices the FBI has established special "cyber squads." Similarly, the Secret Service has an extensive program comprised of agents specializing in electronic crimes (the Electronic Crimes Special Agent Program or "ECSAP").

It is also important to understand that the science of computer forensics is of increasing importance in cybercrime investigations. New computers sold for use in the home routinely have hard drives which could store the entire contents of the Library of Congress. Business computers store much greater volumes of data. When these computers are searched as part of a criminal investigation, the government must have forensic tools and trained forensic examiners to sift quickly through this massive amount of data to search for evidence of a crime. They must also be thoroughly familiar with where data can be hidden on a hard drive and how to use the Internet to recreate the trail of hackers and identity thieves that can operate from anywhere in the world. Furthermore, because many state and local law enforcement agencies do not have adequate computer forensic resources, the federal government is increasingly called upon to

provide forensic assistance in a broad variety of crimes prosecuted at that level. In order to provide greater assistance to state and local law enforcement, the FBI, through its Regional Computer Forensics Laboratories, and the Secret Service, through its Electronic Crimes Task Forces, have provided assistance and training to hundreds of local investigators.

All of these efforts have led to a number of important prosecutions. For example, a year-long investigation by the Secret Service led to the indictment of 27 U.S. and foreign members of the "Shadowcrew" organization in October 2004. Shadowcrew and its associated website, www.Shadowcrew.com, created an online hub for identity thieves to buy and sell stolen identity information and stolen credit and debit card numbers. It also provided extensive information to its members about how to hack into computers, how to make fraudulent identity documents and credit cards, and how to use stolen identity information to commit fraud. The members of this one-stop online marketplace trafficked in at least 1.5 million stolen credit and bank card numbers. Victims estimated losses in excess of $40 million. To date, 17 defendants have pled guilty in the case.

In addition, in the Eastern District of Arkansas, the Department of Justice, the FBI, and the Secret Service investigated and convicted the lead defendant of the largest data theft in history. At trial, the Government showed that between January and July of 2003, Scott Levine used sophisticated decryption software illegally to obtain passwords and then used those passwords to steal over a billion records containing personal information, such as physical addresses, email addresses, and telephone numbers. The data was worth tens of millions of dollars. The jury convicted Levine of 120 counts of unauthorized access to a protected computer. In February of this year, a federal judge in Little Rock, Arkansas, sentenced Levine to 96 months in prison.

In another recent case in the Northern District of California, a former manager of a debt collection company was convicted for using a computer code "time bomb" to corrupt the customer data base of his former employer. When the manager learned that he was facing dismissal, he designed and installed malicious code that would activate at a time after he left the company. The malicious code then deleted and modified financial records relating to over 50,000 customer accounts and caused over $100,000 in damages. The defendant was convicted after a jury trial and is currently awaiting sentencing.

We have also had some notable successes in investigating crimes involving botnets. In one recent case in Seattle, Washington, an individual pled guilty to using a botnet in a fraud scheme that netted him over $100,000. In the process of expanding the number of compromised computers in this botnet, however, he damaged the computer system of a hospital. When the system went down, it affected the hospital's systems in numerous ways: doors to the operating rooms did not open, pagers did not work, and computers in the intensive care unit shut down. By reverting to back up systems, the hospital was able to avoid any harm to patients, but obviously the consequences could have been much worse. The defendant is currently awaiting sentencing.

In addition, in the first prosecution of its kind in the nation, the FBI and the U.S. Attorney's Office for the Central District of California secured the conviction of Jeanson James Ancheta, a well-known member of the "botmaster underground," on charges related to his profitable use of botnets that were used to launch destructive attacks, to send huge quantities of spam email across the Internet, and to receive surreptitious installations of adware. Through his crimes, Ancheta controlled over 400,000 computers, including some computers owned by the Department of Defense. In addition to his guilty pleas to the criminal charges, Ancheta agreed to pay roughly $15,000 in restitution to the Weapons Division of the United States Naval Air

Warfare Center in China Lake and the Defense Information Systems Agency, whose national defense networks were intentionally damaged by Ancheta's malicious code. Ancheta was sentenced this week to 57 months' imprisonment and was ordered to forfeit his ill-gotten gains, including $60,000 in cash and his BMW automobile.

The Department's efforts to fight cybercrime do not stop at America's borders. Just as the Internet is unfettered by national boundaries, so Internet crime almost invariably involves computers, electronic evidence, and defendants across the globe. Indeed, even domestic criminals preying on domestic victims can route their communications through overseas networks, requiring the assistance of foreign law enforcement agencies to solve what is in essence a domestic crime.

Recognizing these difficulties, the Department has promoted international law enforcement capabilities and has assisted foreign lawmakers in modernizing their cybercrime laws. These efforts will enable foreign law enforcement to gather electronic evidence that is important to U.S. investigations, as well as to investigate and prosecute offenders in their own countries. For example, the U.S. Department of Justice has spearheaded efforts in the Group of Eight ("G8") to ensure that the world's eight major industrial economies have strategies and policies in place to fight cybercrime. Through this forum, we have created and led a network of high-tech law enforcement agencies from 43 nations that is now able to respond to urgent Internet crimes 24 hours a day, seven days a week.

In addition, the Department was an active participant in the negotiation of the historic Convention on Cybercrime (2001). The Convention on Cybercrime is essential to securing the international cooperation necessary to enforce our criminal and intellectual property laws and to protect the Nation and the critical information infrastructures of our commercial,

communication, and defense sectors. At the same time, it fully preserves existing protections regarding the rights and privacy of individuals. Ratification of the Convention is a top priority of this Administration. In the absence of the Convention, we may find ourselves unable to obtain critical computer evidence from overseas that might allow us to prevent a new terrorist attack, or to break up an international pedophile ring, or to prosecute those who defraud our fellow-citizens from locations abroad. Now under consideration for the advice and consent of the Senate to ratification, this first-of-its-kind treaty will promote our worldwide efforts to address such online crimes as computer hacking, Internet fraud, child pornography, and intellectual property theft.

III. THE NEED FOR LEGISLATIVE ACTION - COMMENTS ON THE COMPUTER SECURITY ENHANCEMENT AND CONSUMER DATA PROTECTION ACT OF 2006

Let me turn now to our own legal framework. As a result of Congressional efforts over the past ten years, federal laws available to combat cybercrime have improved significantly. However, we believe that Congressional action in several particular areas would improve our ability to investigate and prosecute these offenses. In particular, we recommend that Congress strengthen the penalties for computer hacking, close loopholes in certain criminal statutes, and clarify the scope and applicability of the laws that govern the collection of electronic evidence.

On May 1, 2006, the Department received a draft bill entitled, "The Computer Security Enhancement and Consumer Protection Act of 2006." This legislation, introduced this past Tuesday as H.R. 5318, includes a number of important provisions, and we firmly support the bill's goals. I would like sincerely to thank the Committee for its attention to this important issue and hope to highlight for you some of the ways we think the bill might be further strengthened. . I will touch on a few of these today with you. We intend to follow up with a views letter on behalf of the Administration that will provide a more comprehensive analysis and recommendations.

A. Section 3 - Theft of Information from Computers

We strongly support Section 3(b) of the bill that cures a problematic loophole in the Computer Fraud and Abuse Act (18 U.S.C. § 1030). This amendment would enhance our ability to investigate and prosecute hackers and identity thieves who steal information from computers. Under current law, federal courts only have jurisdiction over the theft of information from a computer if the criminal uses an interstate communication to access that computer (except if the computer belongs to the federal government or a financial institution). Yet in many cases criminals steal data through purely in-state actions. For example, corporate employees can exceed their authorization to access vast numbers of electronic records. Similarly, individuals often plant spyware programs on the computers of people they know in order to obtain their private communications and passwords.

Moreover, the advance of wireless technology has made the current provision outmoded. In one case in North Carolina, for example, an individual broke into a hospital computer's wireless access point and thereby stole patient records. State investigators and the victim asked the United States Attorney's Office to support the investigation and charge the criminal; however, because the communications occurred entirely intrastate, it did not violate the Computer Fraud and Abuse Act.

Section 3(b) corrects this significant loophole. This amendment will allow federal investigators and prosecutors to pursue intrastate theft of information without requiring proof that the conduct involved an interstate communication. Federal jurisdiction under the amended statute would be based, as it is in most other subsections of the Computer Fraud and Abuse Act,

on the fact that the victim computer itself is used in interstate or foreign commerce or communications.

B. Section 4 - Use of Computer Hacking by Organized Crime

Section 4 of the bill would make the Computer Fraud and Abuse Act a predicate offense for violations of the Racketeering Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1961 et seq., a charge used to prosecute organized crime groups and other criminal enterprises. We support this amendment but would recommend limiting it to the felony subsections of Section 1030 to ensure that it will apply only to the more serious hacking offenses.

As organized crime groups begin to turn to the Internet to commit such traditional crimes as fraud, money laundering, and gambling, and as hackers are increasingly motivated by the desire for financial gain, the activities of these criminal elements will increasingly overlap. Thus, it makes sense to include elements of the Computer Fraud and Abuse Act as RICO predicates.

The following fact patterns illustrate the involvement of criminal enterprises in the more serious types of violations of Section 1030:

- Section 1030(a)(2) (Theft of Information). Criminal enterprises have been tied to large-scale online thefts of credit card numbers and other financial information from banks and credit card processors. The investigation of the Shadowcrew organization described above is an example of such a criminal enterprise.

- Section 1030(a)(4) (Computer Hacking as Part of a Fraud Scheme). Organized criminal groups have used "phishing" attacks to place spyware on computers to gather users' financial information, credit card numbers, and similar information. For example, Brazilian authorities recently arrested over 50 individuals involved in a sophisticated, organized phishing ring that used spyware to steal roughly $66 million from online-banking customers. Under U.S. law, this sort of scheme would violate Section 1030(a)(4).

- Section 1030(a)(5) (Damage to Computers or Information). Criminal enterprises appear to be involved in the creation of botnets that can be used to launch denial of service attacks against online commercial activities. In at least two instances over the last two years, the Department has charged business owners for paying others to conduct distributed denial of service attacks on business competitors for commercial advantage.

- Section 1030(a)(7) (Extortion by Threatening to Damage Computers or Information). Criminal enterprises are committing extortion by threatening to disrupt online commercial activities. For example, British and Russian police have broken up several extortion rackets that targeted online gambling sites in the United Kingdom and the Caribbean.

As these examples demonstrate, criminal enterprises increasingly are finding ways to commit fraud and related criminal activities through and against computers, and they are doing so in ways that make it more difficult to prosecute the offenders using traditional conspiracy charges. Therefore, adding felony violations of the Computer Fraud and Abuse Act to the list of RICO predicates in Section 1961(1) would ensure that we have the necessary and appropriate tools to address evolving trends in cybercrime committed by criminal enterprises.

C. Section 5 – Cyber-Extortion

Section 5 of the bill amends the law relating to cyber-extortion. We appreciate the Committee's recognition of the importance of this provision, especially given current trends in cybercrime, as discussed above, and its recognition that the existing law has certain shortcomings; however, we recommend a different approach to addressing these shortcomings. Existing section 1030(a)(7), which governs threats to damage computers or information, does not cover certain types of extortion schemes that have come to our attention. For example, some cybercriminals extort companies without explicitly threatening to cause damage to computers. Instead, they steal confidential data and then threaten to make that data public if their demands are not met. Others cause the damage first – such as by accessing a corporate computer without authority and encrypting critical data – and then threaten that they will not correct the problem

unless the victim pays. These types of extortion should be covered by the Computer Fraud and Abuse Act, but we recommend covering such acts more explicitly. The Department will be glad to provide the specific language we recommend to address this issue.

D. Section 7 - Notice to Law Enforcement

Section 7 would require notifying law enforcement when a security breach of a system containing personal information occurs. We strongly support the goal of this provision, and we believe the language requiring prior notification to the Secret Service or the FBI will allow for appropriate law enforcement investigation of unauthorized access to personal information. Without such reporting, we cannot ensure that we are effectively punishing those who have committed these destructive crimes and deterring those who might do so in the future.

We have several suggestions, however, to improve the language:

1. Proposed Section 1039(a) (Section 7(a) of H.R. 5318)

This provision would only require law enforcement notification where the breach "causes economic harm to any person." We recommend striking this clause. If any type of security breach occurs - even one where prompt action prevented harm, there should be an appropriate law enforcement investigation. It is only through such investigations that the criminals can be identified and their conduct deterred. Moreover, in many cases, it may be difficult for the victim of the security breach to determine whether or not economic harm has occurred. Months might pass, for example, before it is determined that stolen personal information was used to commit identity theft. Notification in such cases should not turn on whether the victim can prove that economic harm has occurred. Further, even in those cases where there is no economic harm, the unauthorized access results in a breach of the confidentiality of personal information. Such privacy violations alone justify law enforcement action.

2. Proposed Section 1039(b)

We recommend that the scope of the definition of "major security breach" in this section be clarified to include any breach of the security of personal information. The Department would be pleased to work with the Committee on specific language.

E. Section 8 - Penalties for Section 1030 Violations

Section 8 accomplishes two goals: it increases the penalties for computer crimes, and it allows for forfeiture of the fruits and instrumentalities of computer crime. Let me address these points in order.

1. Criminal Penalties

First, Section 8 would eliminate the complex sentencing scheme for the various subsections of the Computer Fraud and Abuse Act and create a single overarching maximum penalty of 30 years in prison. While we believe that there are ways to strengthen the sentencing for offenses under Section 1030 and make the sentencing scheme less complex, we believe it is important to maintain a sentencing scheme that is tailored to the different gradations of harm caused by these offenses.

Unquestionably, there is a need for strong deterrence against computer hacking violations, and we recommend increasing the sentences for particularly harmful offenses. For example, the penalties for the theft of information (Section 1030(a)(2)) have become inadequate in light of the rise of identity theft, "phishing," and spyware activity. Under current law, obtaining information from another person's computer without authorization is generally a misdemeanor offense with a maximum penalty of one year in prison. 18 U.S.C. § 1030(a)(2)(C), (c)(2)(A). The offense becomes a 5-year felony only if the actor committed the violation for

financial gain, in furtherance of another crime or a tort, or if the value of the stolen information exceeds $5,000.

These statutory bases for an increased penalty do not take into account the serious privacy invasions that occur without a financial motive, such as when spyware programs steal the sensitive, private information of a computer user, and the person installing the spyware is motivated by revenge or prurient interest. Currently, these invasions of privacy do not constitute felony offenses, and the existing misdemeanor penalty does not create an adequate punishment or deterrent. Further, even when one of the aggravating factors listed in the statute is present, such as when the crime is committed in furtherance of a fraud scheme, the current five-year maximum sentence is not commensurate with the gravity of the harm caused. Thus, we recommend raising the maximum penalty for these offenses to 3 years' imprisonment for ordinary offenses under Section 1030(a)(2) and to 10 years' imprisonment where the actor committed the violation for financial gain, in furtherance of another crime or a tort, or if the value of the stolen information exceeds $5,000.

2. Forfeiture

Second, Section 8 also addresses the forfeiture of computers used in hacking crimes. Under current law, the Government can seek forfeiture of the proceeds of violations of the Computer Fraud and Abuse Act but not of the instrumentalities used to commit such crimes. While Section 8 seeks to address this shortcoming in the current forfeiture regime, we recommend adding text to clarify the procedure to be used in forfeiture proceedings. In addition, civil forfeiture is extremely important in cases of this nature, because the defendants may be overseas and thus beyond the reach of a criminal prosecution. Thus, we suggest adding a section

to allow for civil forfeiture. We would be happy to recommend to the Committee specific language for these provisions.

III. ADDITIONAL LEGISLATIVE PROPOSALS

In addition to our comments on the Cyber Security Enhancement and Consumer Data Protection Act of 2006, I would like to share with you some additional suggestions for ways to improve the laws we use to combat computer and Internet crime. I will touch on a few of these suggestions, and the Department will provide the Committee with a comprehensive list of our legislative proposals.

A. Enhancing the Prosecution of Attacks on Computers

As a result of recent investigations and prosecutions, we have discovered that the laws criminalizing attacks on computers contain several limitations that have made it more difficult to prosecute certain criminal conduct. For example, it has at times proved difficult to prosecute offenders who install malicious software on many computers when the harm to each computer is relatively slight. Although the aggregate harm may be quite significant and rise above the current $5,000 threshold for federal jurisdiction, it can be difficult to present evidence of each individual harm in court without calling as witnesses hundreds of computer owners. This problem could be solved simply by lowering or eliminating the monetary threshold or by adding an additional trigger for federal jurisdiction for this type of offense.

In addition, 18 U.S.C. § 2701, the law prohibiting unauthorized access to another's email, should be clarified to ensure that it protects all email. As currently drafted, this statute may only apply to email that has not yet been received by the intended recipient. A simple amendment would clarify Section 2701 to allow prosecution of criminals who harm the privacy of others by accessing their email, whether unread or read and then stored.

B. Clarifying the Procedures for Responding to Foreign Requests for Electronic Evidence

Under current law, the United States is generally able to provide assistance to foreign law enforcement agencies that are investigating computer crimes. Providing such assistance is particularly important, because it allows us to fulfill our obligations under various treaties, and because it creates the environment in which U.S. law enforcement agencies can, in turn, obtain assistance from foreign law enforcement agencies. Moreover, even to solve domestic computer crimes, it is often necessary to obtain some electronic evidence from overseas in order to identify and prosecute the offenders. Only by providing assistance to foreign law enforcement authorities can we expect to receive assistance where the crime involves an American victim. Thus, our ability to provide assistance to foreign investigators has a direct impact on the safety and security of Americans.

However, the statutes that govern the obtaining of electronic and other evidence based upon a foreign request contain certain ambiguities. With respect to electronic evidence, in 2001, Congress changed the wording of 18 U.S.C. § 2703 in a way that inadvertently introduced confusion in routine mutual legal assistance cases. For example, Section 2703(a) requires that the court issuing a search warrant for stored electronic evidence have "jurisdiction over the offense." Since a U.S. court often has no jurisdiction to try a foreign offender, the wording of Section 2703(a) needlessly complicates the use of this type of court process. Therefore, we recommend clarifying the definition of "court of competent jurisdiction" in section 2711.

IV. CONCLUSION

In conclusion, I would like again to thank the Subcommittee for the opportunity to testify here today. The threat of computer crime has an enormous impact on our nation's economy and on the security and privacy of all of our citizens. The Department is firmly committed to

addressing this threat by aggressively investigating and prosecuting these offenses and to deterring future offenders by seeking appropriately severe sentences. Congressional action now will significantly improve our ability to address the growing threat of cybercrime.

I would be happy to answer any questions that the Subcommittee may have. Thank you.