United States Government Accountability Office

GAO

Report to Congressional Requesters

June 2007

CYBERCRIME

Public and Private Entities Face Challenges in Addressing Cyber Threats

GAO-07-705

June 2007

CYBERCRIME

Public and Private Entities Face Challenges in Addressing Cyber Threats

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-705, a report to congressional requesters

Why GAO Did This Study

Computer interconnectivity has produced enormous benefits but has also enabled criminal activity that exploits this interconnectivity for financial gain and other malicious purposes, such as Internet fraud, child exploitation, identity theft, and terrorism. Efforts to address cybercrime include activities associated with protecting networks and information, detecting criminal activity, investigating crime, and prosecuting criminals.

GAO's objectives were to (1) determine the impact of cybercrime on our nation's economy and security; (2) describe key federal entities, as well as nonfederal and private sector entities, responsible for addressing cybercrime; and (3) determine challenges being faced in addressing cybercrime. To accomplish these objectives, GAO analyzed multiple reports, studies, and surveys and held interviews with public and private officials.

What GAO Recommends

GAO recommends that the Attorney General and the Secretary of Homeland Security help ensure adequate law enforcement analytical and technical capabilities. In written comments on a draft of this report, the FBI and the U.S. Secret Service noted efforts to assess and enhance these capabilities.

www.gao.gov/cgi-bin/getrpt?GAO-07-705.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Dave Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

Cybercrime has significant economic impacts and threatens U.S. national security interests. Various studies and experts estimate the direct economic impact from cybercrime to be in the billions of dollars annually. The annual loss due to computer crime was estimated to be $67.2 billion for U.S. organizations, according to a 2005 Federal Bureau of Investigation (FBI) survey. In addition, there is continued concern about the threat that our adversaries, including nation-states and terrorists, pose to our national security. For example, intelligence officials have stated that nation-states and terrorists could conduct a coordinated cyber attack to seriously disrupt electric power distribution, air traffic control, and financial sectors. Also, according to FBI testimony, terrorist organizations have used cybercrime to raise money to fund their activities. Despite the estimated loss of money and information and known threats from adversaries, the precise impact of cybercrime is unknown because it is not always detected and reported (cybercrime reporting is discussed further in GAO's challenges section).

Numerous public and private entities have responsibilities to protect against, detect, investigate, and prosecute cybercrime. The Departments of Justice, Homeland Security, and Defense, and the Federal Trade Commission have prominent roles in addressing cybercrime within the federal government, and state and local law enforcement entities play similar roles at their levels. Private entities such as Internet service providers and software developers focus on the development and implementation of technology systems to detect and protect against cybercrime, as well as gather evidence for investigations. In addition, numerous cybercrime partnerships have been established between public sector entities, between public and private sector entities, and internationally, including information-sharing efforts.

Entities face a number of key challenges in addressing cybercrime, including reporting cybercrime and ensuring that there are adequate analytical capabilities to support law enforcement (see table). While public and private entities, partnerships, and tasks forces have initiated efforts to address these challenges, federal agencies can take additional action to help ensure adequate law enforcement capabilities.

Challenges to Addressing Cybercrime

Challenge	Description
Reporting cybercrime	Accurately reporting cybercrime to law enforcement
Ensuring adequate law enforcement analytical and technical capabilities	Obtaining and retaining investigators, prosecutors, and cyberforensics examiners Keeping up-to-date with current technology and criminal techniques
Working in a borderless environment with laws of multiple jurisdictions	Investigating and prosecuting cybercrime that transcends borders with laws and legal procedures of multiple jurisdictions
Implementing information security practices and raising awareness	Protecting information and information systems Raising awareness about criminal behavior

Source: GAO.

Contents

Figures

Abbreviations

CCIPS	Computer Crimes and Intellectual Property Section
CHIP	Computer Hacking and Intellectual Property
DCIS	Department of Defense Criminal Investigative Service
DC3	Defense Cyber Crime Center
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FTC	Federal Trade Commission
IC3	Internet Crime Complaint Center
NCIS	Naval Criminal Investigative Service
NCSD	National Cyber Security Division
Secret Service	U.S. Secret Service
SAFETY	Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act
US-CERT	United States Computer Emergency Readiness Team

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

June 22, 2007

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Honorable Lamar S. Smith
Ranking Member
Committee on the Judiciary
House of Representatives

The rapid increase in computer interconnectivity has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While the benefits have been enormous, the accelerated use of the Internet has also enabled a dramatic rise in criminal activity that exploits this interconnectivity for illicit financial gain and other malicious purposes, such as Internet fraud, child exploitation, and identity theft. Efforts to address cybercrime[1] include activities associated with protecting networks and information, detecting criminal activity, investigating crime, and prosecuting criminals.

As agreed, our objectives were to (1) determine the impact of cybercrime on our nation's economy and security; (2) describe key federal entities, as well as nonfederal and private sector entities, responsible for addressing cybercrime; and (3) determine challenges being faced in addressing cybercrime. To accomplish these objectives, we analyzed multiple reports, studies, and surveys and held interviews with public and private officials. Appendix I provides further details on our objectives, scope, and methodology. We conducted this review from June 2006 to May 2007 in accordance with generally accepted government auditing standards.

[1]Cybercrime, as used in this report, refers to criminal activities that specifically target a computer or network for damage or infiltration and also refers to the use of computers as tools to conduct criminal activity.

Results in Brief

Cybercrime is a threat to U.S. national economic and security interests. Various studies and expert opinion estimate the direct economic impact from cybercrime to be in the billions of dollars annually. The annual loss due to computer crime was estimated to be $67.2 billion for U.S. organizations, according to a 2005 Federal Bureau of Investigation (FBI) survey. The estimated losses associated with particular crimes include $49.3 billion in 2006 for identity theft and $1 billion annually due to phishing.[2] These projected losses are based on direct and indirect costs that may include actual money stolen, estimated cost of intellectual property stolen, and recovery cost of repairing or replacing damaged networks and equipment. In addition, there is concern about threats that nation-states and terrorists pose to our national security through attacks on our computer-reliant critical infrastructures and theft of our sensitive information. For example, according to the U.S.-China Economic and Security Review Commission report, Chinese military strategists write openly about exploiting the vulnerabilities created by the U.S. military's reliance on advanced technologies and the extensive infrastructure used to conduct operations.[3] Also, according to FBI testimony, terrorist organizations have used cybercrime to raise money to fund their activities. Despite the reported loss of money and information and known threats from adversaries, there remains a lack of understanding about the precise magnitude of cybercrime and its impact because cybercrime is not always detected or reported (cybercrime reporting is discussed further in our challenges section).

Numerous public and private entities (federal agencies, state and local law enforcement, industry, and academia) have individual and collaborative responsibilities to protect against, detect, investigate, and prosecute cybercrime. The Departments of Justice (DOJ), Homeland Security (DHS), and Defense (DOD), and the Federal Trade Commission (FTC) have prominent roles in addressing cybercrime within the federal government. DOJ's FBI and DHS's U.S. Secret Service (Secret Service) are key federal organizations with responsibility for investigating cybercrime. State and local law enforcement organizations also have key responsibilities in

[2]Identity theft is the wrongful obtaining and using of another person's identifying information in some way that involves fraud or deception. Phishing is a high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information.

[3]U.S.-China Economic and Security Review Commission, *2006 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, D.C.: November 2006).

addressing cybercrime. Private entities—Internet service providers, security vendors, software developers, and computer forensics vendors—focus on developing and implementing technology systems to protect against computer intrusions, Internet fraud, and spam and, if a crime does occur, detecting it and gathering evidence for an investigation. In addition, numerous partnerships have been established between public sector entities, between public and private sector entities, and internationally to address various aspects of cybercrime. For example, the Cyber Initiative and Resource Fusion Unit is a partnership established among federal law enforcement, academia, and industry to analyze cybercrime and determine its origin and how to fight it.

Efforts by public and private entities to address cybercrime are impeded by major challenges that include

- reporting cybercrime—entities do not always detect or report cybercrimes;
- ensuring adequate law enforcement analytical and technical capabilities—law enforcement organizations often have difficulty obtaining and retaining investigators, prosecutors, and examiners with the specialized skills needed to address cybercrime; this is due in part to the staff rotation policies in place at certain law enforcement organizations;
- working in a borderless environment with laws of multiple jurisdictions—because cybercrime crosses national and state borders, law enforcement organizations have to deal with multiple jurisdictions with their own laws and legal procedures, a situation that complicates investigations; and
- implementing and raising awareness about strong information security practices—our experience in evaluating the information security of federal agencies demonstrates the difficulty that organizations face in maintaining strong information security programs; despite efforts by public and private entities to raise awareness about the importance of information security, many organizations and individuals remain insecure.

Public and private entities, cybercrime partnerships, and task forces have initiated efforts to address these challenges, including leveraging resources and technologies to fight cybercrime. However, more can be done to help ensure agencies have adequate law enforcement capabilities. Specifically, staff rotation policies at key law enforcement agencies may hinder the agencies' abilities to retain analytical and technical capabilities supporting law enforcement.

In order to address the challenge of ensuring adequate law enforcement analytical and technical capabilities, we are recommending that the Attorney General and the Secretary of Homeland Security reassess and modify, as appropriate, current rotation policies to retain key expertise necessary to investigate and prosecute cybercrime.

We received written comments on a draft of this report from the FBI and Secret Service (see app. II and III). In their comments, the Deputy Assistant Director from the FBI's Cyber Division and the Assistant Director, Office of Inspection, U.S. Secret Service mentioned efforts to assess and enhance their analytical and technical capabilities. The FBI official stated that the bureau's rotational policies for new Special Agents and senior field Supervisory Special Agents were put into place after careful consideration, and that five career paths—including a specific designation for cyber matters—have been established. The Secret Service official stated that the service is expanding its Electronic Crimes Special Agent Program and will have approximately 770 trained and active agents by the end of fiscal year 2007. The service also reported that the rotation of the Electronic Crimes Special Agent Program agents does not have a detrimental impact on the agency's cyber investigative capabilities because Secret Service field offices send additional agents through the program prior to a trained agent's departure, and because the Electronic Crime Task Forces allow the agency to draw on state and local law enforcement officials trained in cyber investigations and computer forensics. Despite these efforts to assess and expand cyber analytical and technical capabilities, our review showed that current rotational policies may result in both agencies underutilizing staff with cyber expertise; therefore, it is important for them to continually reassess the rotational policies that impact their ability to address the cyber threat.

DOD, DOJ, DHS, state and local government, and other officials also provided technical corrections that have been incorporated in this report as appropriate.

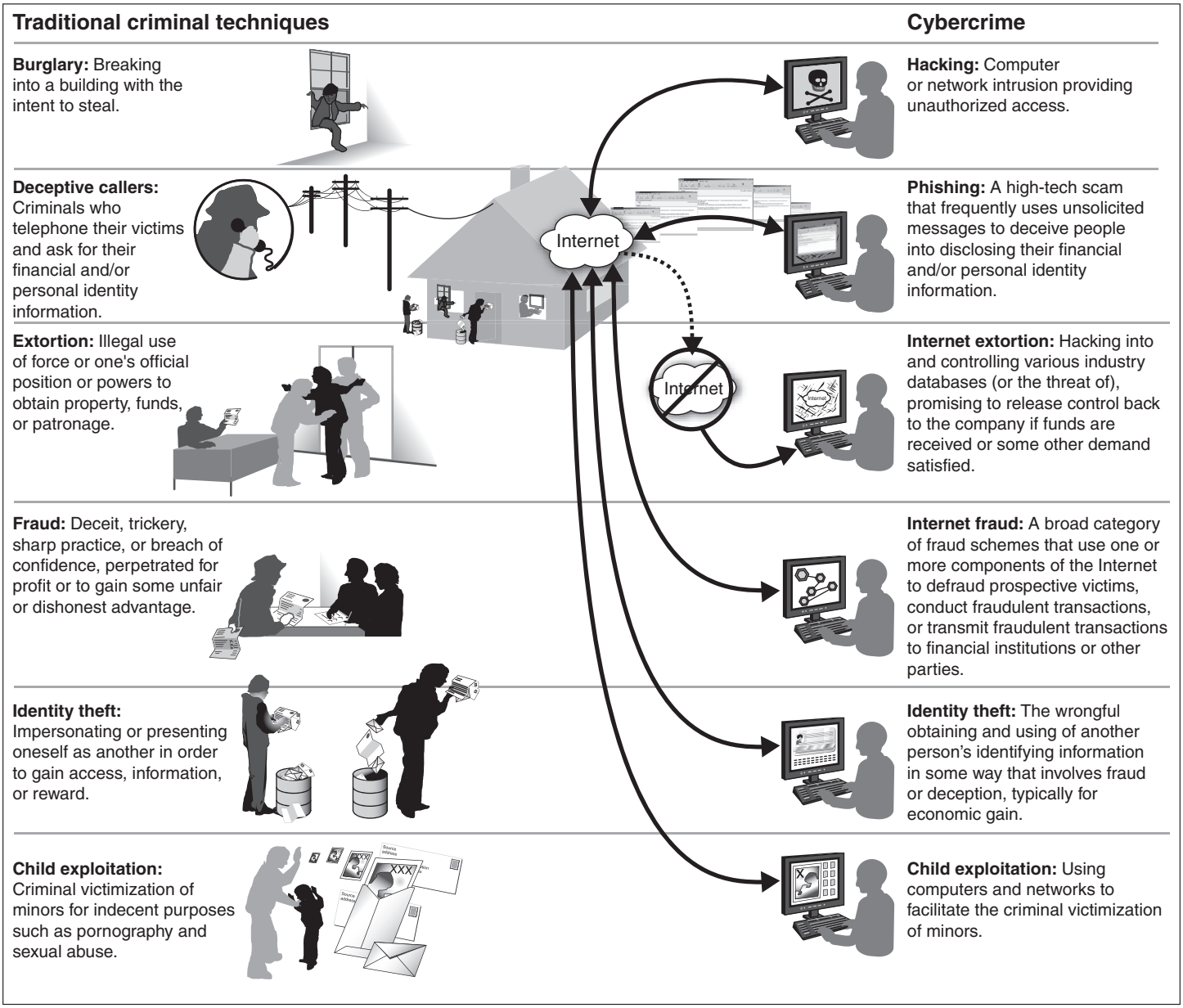
Background

Over 150 million U.S. citizens are connected to the Internet. According to the FBI, the number of people with access to the Internet increased 182 percent between 2000 and 2005. In 2006, total nontravel-related spending on the Internet was estimated to be $102 billion by a private sector entity, a 24 percent increase over 2005. While the benefits of interconnectivity have been enormous, it has provided new horizons and techniques for crime.

Cybercrime: Comparison between Cybercrime and Traditional Criminal Techniques

Cybercrime refers to criminal activities that specifically target a computer or network for damage or infiltration. For example, it can be a crime to access ("hack into") a computer without authorization or to distribute viruses. Cybercrime also includes the use of computers as tools to conduct criminal activity such as fraud, identity theft, and copyright infringement. Computers significantly multiply the criminal's power and reach in committing such crimes. Figure 1 describes and compares cybercrime and traditional criminal techniques.

Figure 1: Comparison between Traditional Criminal Techniques and Cybercrime



Source: GAO.

Cybercrime techniques have characteristics that can vastly enhance the reach and impact of criminal activity, such as the following:

- Criminals do not need to be physically close to their victims to commit a crime.
- Technology allows criminal actions to easily cross multiple state and national borders.
- Cybercrime can be carried out automatically, at high speed, and by attacking a vast number of victims at the same time.
- Cybercriminals can more easily remain anonymous.

To help facilitate cybercrimes, criminals use several techniques listed in table 1.

Table 1: Techniques Used to Commit Cybercrimes

Type	Description
Spamming	Sending unsolicited commercial e-mail advertising for products, services, and Web sites. Spam can also be used as a delivery mechanism for malware and other cyber threats.
Phishing	A high-tech scam that frequently uses spam or pop-up messages[a] to deceive people into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information. Internet scammers use e-mail bait to "phish" for passwords and financial data from the sea of Internet users.
Spoofing	Creating a fraudulent Web site to mimic an actual, well-known Web site run by another party. E-mail spoofing occurs when the sender address and other parts of an e-mail header are altered to appear as though the e-mail originated from a different source. Spoofing hides the origin of an e-mail message.
Pharming	A method used by phishers to deceive users into believing that they are communicating with a legitimate Web site. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed Web site when the user types in a legitimate Web address. For example, one pharming technique is to redirect users —without their knowledge—to a different Web site from the one they intended to access. Also, software vulnerabilities may be exploited or malware employed to redirect the user to a fraudulent Web site when the user types in a legitimate address.
Denial-of-service attack	An attack in which one user takes up so much of a shared resource that none of the resource is left for other users. Denial-of-service attacks compromise the availability of the resource.
Distributed denial-of-service	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Viruses	A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. A virus requires human involvement (usually unwitting) to propagate.

Type	Description
Trojan horse	A computer program that conceals harmful code. It usually masquerades as a useful program that a user would wish to execute.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
Malware	Malicious software designed to carry out annoying or harmful actions. Malware often masquerades as useful programs or is embedded into useful programs so that users are induced into activating them. Malware can include viruses, worms, and spyware.
Spyware	Malware installed without the user's knowledge to surreptitiously track and/or transmit data to an unauthorized third party.
Botnet	A network of remotely controlled systems used to coordinate attacks and distribute malware, spam, and phishing scams. Bots (short for "robots") are programs that are covertly installed on a targeted system allowing an unauthorized user to remotely control the compromised computer for a variety of malicious purposes.

Source: GAO analysis based on public and private sector sources.

[a]A pop-up message is a type of window that appears over the browser window of a Web site that a user has visited.

Companies that process large volumes of Internet traffic, such as Postini, Symantec, and IBM analyze their traffic for patterns and trends and have found that the cybercrime techniques in table 1 are prevalent. Table 2 shows reported volumes of cybercrime techniques.

Table 2: Reported Volume of Cybercrime Techniques

Type	Findings	Source
Spam	Has increased over 65 percent since January 2002.	Postini
	Approximately 88 percent of all e-mail processed at service centers is classified as "junk."	
	From September 2006 to March 2007, Postini collected over 60 billion pieces of spam totaling 537.7 terabytes of data.	
	Between July and December 2006, spam constituted 59 percent of all e-mail monitored.	Symantec
	Through 2005, hackers most frequently targeted the telecommunications and health care sectors, where almost 80 percent of all e-mail traffic was spam.	Counterpane
Botnets	Between July and December 2006, an average of 63,912 active, bot-infected computers per day were observed, an 11 percent increase from the previous reporting period.	Symantec
Phishing	Between July and December 2006, 166,248 unique phishing messages detected, a 6 percent increase over the first 6 months of 2006.	Symantec
	An average of 904 unique phishing messages per day was reported for the second half of 2006.	
	During the same period, over 1.5 billion phishing messages were blocked.	
	During 2006, U.S.-based businesses were the most targeted organizations of phishing e-mails, accounting for 71.37 percent of all phishing e-mail. In addition, more than 55 percent of the world's phishing attacks fabricate company Web sites that are hosted in the United States.	IBM

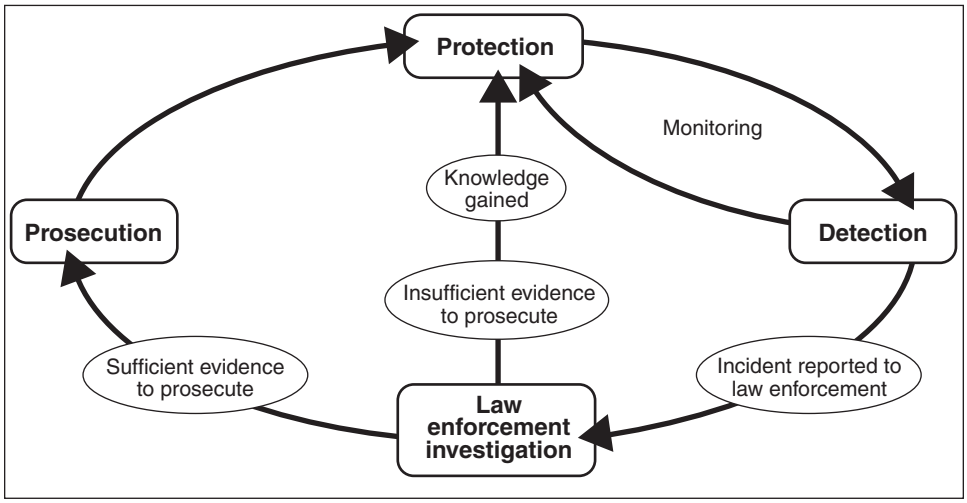
Type	Findings	Source
Malware	Between January and June 2006, approximately 2 million of the 4 million computers cleaned by the malicious software removal tool had at least one backdoor Trojan horse.	Microsoft
	43,000 new variants of malware were found in the same period.	
Trojan horses	In 2005, close to 40 percent of the financial services and banking industry sector suffered the most Trojan horse attacks.	Counterpane

Source: GAO analysis of private sector reports about Internet traffic processed.

Framework for Addressing Cybercrime

Efforts to address cybercrime follow the same basic process as efforts to address traditional crime. As figure 2 shows, this basic process is one of protection, detection, investigation, and prosecution.

Figure 2: Crime Mitigation Framework



Source: GAO.

To protect networks and information against cybercrime, organizations and individuals implement cybersecurity techniques such as access controls (passwords) and firewalls. In addition, they use monitoring devices or intrusion detection systems to detect incidents that could potentially be criminal intrusions. As figure 2 shows, monitoring unusual activity allows organizations and individuals to make adjustments to improve protection. When a suspected cybercrime is detected, organizations and individuals must decide what action to pursue. Depending on the severity of the incident, the level of evidence, and their comfort with revealing the incident, they may or not report it to law enforcement.

Generally, investigations begin once an incident is reported to law enforcement. During the preliminary investigation, federal, state, or local law enforcement, along with their respective prosecutors, determine if a crime occurred and if a further investigation is warranted. Also, in some cases, private sector and academic analysts may provide expertise. Among the factors weighed by law enforcement authorities in determining whether to conduct an investigation is whether their agency has jurisdiction over the crime, the number and location of the victims, the expected location of the criminal, the amount of loss, and the agency's investigative priorities and available resources. If it is determined that an investigation will not be pursued, law enforcement may provide advice to victims that may be used to improve their protective measures. When a criminal investigation is pursued, law enforcement investigators have the initial responsibility for leading the evidence-gathering effort and working with cyberforensic investigators and examiners with the technical expertise to analyze the evidence. In cases where evidence is not voluntarily provided, law enforcement can use various subpoena authorities to obtain information needed to perform the investigation.

A key component of cybercrime investigations is the gathering and examination of electronic evidence that can be useful for prosecution. Using cyberforensic tools and techniques,[4] cybercrime investigators and examiners gather and analyze electronic evidence. If available, cyberforensic laboratories may be used to extract the electronic evidence and present it in a court-admissible format. The evidence could entail analysis of terabytes of information on multiple electronic devices, the electronic path taken by a fraudulent e-mail, pornographic images stored on a hard drive, or data stored on a mutilated but later reconstructed CD-ROM. The ability to gather electronic evidence and the assurance that cyberforensic procedures do not compromise the evidence gathered can be key to building a case and prosecuting cybercriminals.

Cybercrime investigations and evidence gathering can also be conducted while a crime is ongoing. If a crime is being investigated while it is still occurring, investigators may use sophisticated techniques to investigate criminal activity that include court-ordered wiretaps. In determining whether and how to gather evidence of information transmitted

[4]Cyberforensics employs electronic tools to extract data from computer media storage without altering the data retrieved. Cyberforensics techniques may also require the reconstruction of media to retrieve digital evidence after attempts to hide, disguise, or destroy it.

electronically, law enforcement may make an application to a court for a wiretap pursuant to the Wiretap Act.[5] To obtain such orders, the application to the court must describe, among other things, the criminal activity and the identity of those involved, if known.

If sufficient evidence is gathered, it can lead to a prosecution. Federal and state prosecutors determine if a prosecution will be pursued based on a number of factors including jurisdiction over the crime, the type and seriousness of the offense, the sufficiency of the evidence, their prosecutorial priorities, and the location and number of the victims. Prosecuting attorneys will also consider the dollar loss and the number of incidents. Some federal prosecuting attorneys may not pursue cybercrime cases because they do not meet the minimum thresholds established for their districts. Thresholds are established by prosecuting attorneys to appropriately focus their limited resources on the most serious crimes that match their district's priorities. For example, if fraud has been committed through the use of a computer, the amount of the dollar loss may need to reach a specific threshold amount for the U.S. Attorney to accept the case. When the U.S. Attorney does not accept a case for prosecution because it does not meet such a threshold, state authorities may decide to accept the case for prosecution.

In addition to criminal remedies, civil remedies are available to address cybercrime activity. The burden of proof in a civil case is not as high as in a criminal case. At the federal level, the FTC investigates activities that could be classified as cybercrime as part of its consumer protection mission and seeks civil injunctions and monetary remedies. In addition, many states have civil statutes that may be applied to cybercrime situations. In the State of Washington, for example, the Attorney General can apply the state's consumer protection statute to cases of cyber-facilitated fraud. Pursuing the case in civil court, the state's Attorney General can seek civil remedies such as the repayment of losses or penalties for wrongdoing or fraud, which could potentially deter future criminal attempts.

[5]In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA"), Pub. L. No. 99-508 (Oct. 21, 1986) which, among others things, extended the prohibitions contained in Title III of the Omnibus Crime and Control and Safe Streets Act of 1968 (the "Wiretap Act"), 18 U.S.C. §§ 2510-2521, to electronic communications that are in transit between machines and contain no aural (human voice) component. The Wiretap Act prohibits installing "sniffer" software to record keystroke and computer traffic of a specific target unless one of the statutory exceptions applies.

Governments Have Enacted Various Laws to Address Cybercrime

Federal and state governments and other nations have enacted laws that apply to cybercrime and the legal recourse or remedies available. In addition, there are international agreements to improve the laws across nations and international cooperation on addressing cybercrime.

Federal Laws

Federal statutes address specific types of cybercrime, while other federal statutes address both traditional crime and cybercrime. Table 3 describes key federal laws used to investigate and prosecute cybercrime activity.

Table 3: Key Federal Laws Used to Investigate and Prosecute Cybercrime

Law (citation)	Description
Computer Fraud and Abuse Act (18 U.S.C. § 1030)	Specifies as a crime the knowing unauthorized access to the computers used by a financial institution, by a federal government entity, or for interstate commerce. Such crimes include knowingly accessing a computer without authorization; damaging a computer by introducing a worm, virus or other attack device; or using unauthorized access to a government, banking, or commerce computer to commit fraud. Violations also include trafficking in passwords for a government computer, a bank computer, or a computer used in interstate or foreign commerce, as well as accessing a computer to commit espionage.
Fraud and related activity in connection with identification documents, authentication features, and information (18 U.S.C. § 1028)	Defines the knowing production, transfer, or possession of false identification documents as a crime. This statute also outlaws the possession of document-making implements such as computer files, hardware, or software.
Aggravated Identity Theft (18 U.S.C. § 1028A)	Adds an additional 2-year term of imprisonment in cases where a defendant "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person" during and in relation to any felony violation of certain enumerated federal offenses.
Fraud and related activity in connection with access devices (18 U.S.C. § 1029)	Outlaws the knowing production, use, or trafficking in counterfeit or unauthorized access devices such as any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service that can be used to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds.
Wire Fraud (18 U.S.C. § 1343)	Prohibits wire fraud. Courts have recognized a variety of means of electronic communications as falling under the wire fraud statute, including facsimile, telex, modem, and Internet transmissions.
Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today (PROTECT) Act of 2003 (18 U.S.C. §§ 1466A, 2251, 2252A, 2423)	Outlaws using computers to generate child pornography, or depicting minors in any obscene or sexual acts. The act enhances tools to protect children and more severely punish those who victimize children.
Certain activities relating to material involving the sexual exploitation of minors (18 U.S.C. § 2252)	Prohibits the transportation, distribution, receipt, and possession, by any means, including a computer, of material involving sexual exploitation of minors.
The Federal Trade Commission Act (15 U.S.C. § 45(a)(1))	The consumer protection provisions of the act declare unfair or deceptive acts or practices in or affecting commerce unlawful.

Law (citation)	Description
Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 (15 U.S.C. § 7701) (18 U.S.C. § 1037)	Sets forth requirements and prohibitions, both criminal and civil, relating to commercial e-mail messages. Contains criminal prohibitions on sending sexually explicit e-mail that does not contain a label or marking designating it as sexually explicit. While DOJ enforces its criminal provisions, the FTC and other regulators enforce its civil provisions, notably requirements to transmit accurate e-mail header information and to provide a functioning opt-out mechanism. The FTC also has promulgated rules under CAN-SPAM, particularly with regard to additional restrictions on unwanted sexually-explicit e-mails.
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (Pub. L. No. 107-56 (Oct. 26, 2001))	Enhances investigatory tools including the authority to intercept electronic communications relating to computer fraud and abuse offenses. It authorizes the Director of the Secret Service to establish nationwide electronic crimes task forces to assist law enforcement, the private sector, and academia in detecting and suppressing computer-based crime, and allows enforcement action to be taken to protect financial payment systems while combating transnational financial crimes directed by terrorists or other criminals.
The Adam Walsh Child Protection and Safety Act (Pub. L. No.109-248 (July 27, 2006))	Prohibits anyone from using innocent or misleading words or images, such as "Barbie" or "Furby," that confuse a minor into viewing a harmful Web site. The law also prohibits knowingly using the Internet to sell or distribute date rape drugs to an unauthorized purchaser or with the intent to commit criminal sexual conduct.

Source: GAO.

Members of Congress have proposed new federal legislation to augment current cybercrime statutes. For example, in February 2007, the Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act (SAFETY) was introduced in the House Judiciary Committee as an anticybercrime bill. Among its various provisions addressing the exploitation of children, the SAFETY Act provides for the promulgation of regulations that would require Internet service providers to retain data such as a subscriber's name and address, user identification, or telephone number to facilitate law enforcement investigations. Also in February 2007, the Securing Adolescents From Exploitation-Online (SAFE) Act of 2007 was introduced in the Senate Committee on the Judiciary. The SAFE Act would include explicit requirements for Internet service providers to report suspected child pornography violations. The House of Representatives passed the Securely Protect Yourself Against Cyber Trespass Act in June 2007. This bill, if signed into law, would prohibit the use of spyware that could take control of a computer or collect user information without permission. The bill would authorize stiff civil penalties against violators.

State and Local Laws

State and local governments have been enacting laws to serve law enforcement efforts in their individual jurisdictions and to enhance cybercrime prevention, investigation, and prosecution efforts. States have also enacted laws against particular types of cybercrime, including laws addressing spamming and spyware. For example, Virginia's Anti-Spam Act

outlaws the use of fraudulent means, such as using a false originating address, to send spam. Further, aggravating factors (such as sending 10,000 spam messages in a 24-hour period or generating more than $1,000 in revenue from a specific spam message) make the crime punishable as a felony under Virginia law. Also, California's Consumer Protection Against Computer Spyware Act makes it illegal for anyone to install software on someone else's computer and use it to deceptively modify settings, including a user's home page, default search page, or bookmarks. It also outlaws the collection, through intentionally deceptive means, of personally identifiable information through keystroke-logging, tracking Web site visits, or extraction of such information from a user's hard drive.

California has also enacted legislation requiring security measures and warnings for wireless network devices. In addition, Westchester County, New York, has taken action to improve the security of wireless networks. Its wireless security law requires that commercial businesses secure their wireless networks or face fines. The law also requires businesses providing wireless Internet access to put up signs advising users of the security risks. Westchester County's enforcement efforts have brought fines against businesses exposing sensitive data over wireless networks.

Other Nations' Laws

Cybercrime laws vary across the international community. Australia enacted its Cybercrime Act of 2001 to address this type of crime in a manner similar to the U.S. Computer Fraud and Abuse Act, discussed above. In addition, Japan enacted the Unauthorized Computer Access Law of 1999 to cover certain basic areas similar to those addressed by the U.S. federal cybercrime legislation. Countries such as Nigeria with minimal or less sophisticated cybercrime laws have been noted sources of Internet fraud and other cybercrime. In response, they have looked to the examples set by industrialized nations to create or enhance their cybercrime legal framework. A proposed cybercrime bill, the Computer Security and Critical Information Infrastructure Protection Bill, is currently before Nigeria's General Assembly for consideration. The bill, if adopted, would mirror similar cybercrime legislation in industrialized nations like the United States, the United Kingdom, Australia, South Africa, and Canada.

Because political or natural boundaries are not an obstacle to conducting cybercrime, international agreements are essential to fighting cybercrime. For example, on November 23, 2001, the United States and 29 other countries signed the Council of Europe's Convention on Cybercrime as a multilateral instrument to address the problems posed by criminal activity on computer networks. Nations supporting this convention agree to have criminal laws within their own nation to address cybercrime, such as

hacking, spreading viruses or worms, and similar unauthorized access to, interference with, or damage to computer systems. It also enables international cooperation in combating crimes such as child sexual exploitation, organized crime, and terrorism through provisions to obtain and share electronic evidence. The U.S. Senate ratified this convention in August 2006. As the 16th of 43 countries to support the agreement, the United States agrees to cooperate in international cybercrime investigations. The governments of European countries such as Denmark, France, and Romania have ratified the convention. Other countries including Germany, Italy, and the United Kingdom have signed the convention although it has not been ratified by their governments. Non-European countries including Canada, Japan, and South Africa have also signed but not yet ratified the convention.

Cybercrime Has Significant Economic Impacts and Threatens U.S. National Security Interests, but Its Precise Magnitude Is Unknown

Cybercrime is a threat to U.S. national economic and security interests. Based on various studies and expert opinion, the direct economic impact from cybercrime is estimated to be in the billions of dollars. The overall loss projection due to computer crime was estimated to be $67.2 billion annually for U.S. organizations, according to a 2005 FBI survey. The estimated losses associated with particular crimes include $49.3 billion in 2006 for identity theft[6] to about $1 billion annually due to phishing.[7] In addition, there is concern about threats that nation-states and terrorists pose to our national security through attacks on our computer-reliant critical infrastructures and theft of our sensitive information. For example, according to the U.S.-China Economic and Security Review Commission report, Chinese strategists are writing about exploiting the vulnerabilities created by the U.S. military's reliance on technologies and attacking key civilian targets.[8] Also, according to FBI testimony, terrorist organizations have used cybercrime to raise money to fund their activities. However, despite the reported loss of money and information and known threats from our nation's adversaries, there remains a lack of understanding about the true magnitude of cybercrime and its impact because it is not always detected or reported.

[6]Javelin Strategy & Research, *2007 Identity Fraud Survey Report: Identity Fraud is Dropping, Continued Vigilance Necessary* (Pleasanton, CA: February 2007).

[7]Department of Homeland Security, Remarks by Assistant Secretary Gregory Garcia at the RSA Conference on IT and Communications Security (San Francisco, CA: February 2007).

[8]U.S.-China Economic and Security Review Commission, *2006 Report to Congress* (Washington, D.C.: November 2006).

Economic Impacts of Cybercrime Are Significant

Based on various studies and expert opinion, the direct economic impact from cybercrime is billions of dollars annually. The overall loss projection due to computer crime was estimated to be $67.2 billion annually for U.S. organizations, according to a 2005 FBI survey. The estimated losses associated with particular crimes include $49.3 billion in 2006 for identity theft and $1 billion annually due to phishing. The studies and experts derive their projected losses based on direct and indirect costs that may include

- actual money stolen,
- estimated cost of intellectual property stolen,
- recovery cost of repairing or replacing damaged networks and equipment, and
- intangible loss due to the opportunity loss from lack of customer confidence in the doing online commerce.

Table 4 shows the economic impact of cybercrime as reported by various studies and reports over the last several years.

Table 4: Economic Impact of Cybercrime

Estimated loss	Methodology	Source
$67.2 billion	Survey projected annual loss to U.S. organizations because of computer crime in 2005.	2005 FBI Computer Crime Survey
$49.3 billion	Survey of 5,000 U.S. adults projected that 8.4 million consumers suffered losses due to identity theft in 2006.	Javelin Strategy & Research 2007
$56.6 billion	Survey of 5,000 U.S. adults projected that 8.9 million consumers suffered losses due to identity theft in 2005.	Javelin Strategy & Research 2006
$8.4 billion	Survey of 2,000 households with Internet access determined U.S. consumers' losses due to viruses, spyware, and phishing in 2004-2005.	Consumer Reports State of the Net 2006
$2.13 billion	Survey of 5,000 U.S. adult Internet users estimated phishing-related losses between April 2003 and May 2005.	Gartner Research
$183.12 million	Over 228,000 complaints were filed; 97,076 were referred to federal, state, and local law enforcement agencies for further consideration in 2005.	Internet Crime Complaint Center (IC3) 2005 Internet Crime Report
$68.14 million ($220 per complaint)	207,449 complaints were filed; 190,143 were referred to law enforcement agencies in 2004.	IC3 2004 Internet Crime Report
$125.6 million ($329 per complaint)	124,509 complaints were filed; 95,064 were referred to law enforcement agencies in 2003.	IC3 2003 Internet Crime Report
$100 billion	Research study estimated the global cost of spam to be $100 billion worldwide, including $35 billion in the United States.	Ferris Research (2007)

Estimated loss	Methodology	Source
$130 million	Survey of 700 organizations identified significant losses due to computer security issues.	2005 Computer Security Institute/FBI Computer Crime and Security Survey
$141million	Survey of 494 organizations identified significant losses due to computer security issues.	2004 Computer Security Institute/FBI Computer Crime and Security Survey
$1 billion	Expert projection of the expected annual direct losses related to phishing.	United States Computer Emergency Readiness Team
$38.4 million	In a survey, 74 percent of the 198 organizations that responded reported being victimized by cybercrime. Nearly two-thirds had been victimized by a computer virus at least once; a quarter had experienced denial of service attacks, such as the degradation of Internet connections due to excessive amounts of incoming information; about a fifth reported that their computer systems had been vandalized or sabotaged.	Bureau of Justice Statistics Pilot Survey (2001)

Source: GAO analysis of government and private sector reports and studies about cybercrime.

Many of the surveys and studies, such as those from IC3 and Computer Security Institute/FBI, are performed at least annually. In addition, the DOJ's Bureau of Justice Statistics has conducted a cybercrime survey of private sector entities to gain a more definitive understanding of cybercrime's economic impact on the United States. As of May 2007, the response rate and results had not been reported.

Individual legal cases also illustrate the financial losses that victims incur due to cybercrime. Examples include the following:

- In February 2007, a defendant was convicted of aggravated identity theft, access device fraud, and conspiracy to commit bank fraud in the Eastern District of Virginia. The defendant, who went by the Internet nickname "John Dillinger," was involved in extensive illegal online "carding" activities. He received e-mails or instant messages containing hundreds of stolen credit card numbers, usually obtained through phishing schemes or network intrusions, from "vendors" who were located in Russia and Romania. In his role as a "cashier" of these stolen credit card numbers, the defendant would then electronically encode these numbers to plastic bank cards, make ATM withdrawals, and return a portion to the vendors. Computers seized from the defendant revealed over 4,300 compromised account numbers and full identity information (i.e., name, address, date of birth, Social Security number, and mother's maiden name) for over 1,600 individual victims.[9]

[9]Statement of Associate Deputy Attorney General before the Subcommittee on Terrorism, Technology and Homeland Security the Committee on the Judiciary (Mar. 21, 2007).

- In September 2005, a Massachusetts juvenile was convicted in connection with approximately $1 million in victim damages. Over a 15-month period, the juvenile hacked into Internet and telephone service providers, stole an individual's personal information and posted it on the Internet, and made bomb threats to high schools in Florida and Massachusetts.[10]

- In October 2004, the Secret Service investigated and shut down an online organization that facilitated losses in excess of $4 million and trafficked in around 1.7 million stolen credit cards and stolen identity information and documents. This high-profile case, known as "Operation Firewall," focused on a criminal organization of some 4,000 members whose Web site functioned as a hub for identity theft activity.[11]

- In July 2003, a man was convicted of causing an aggregate loss of approximately $25 million and hacking into computers in the United States. The defendant pleaded guilty in these proceedings and admitted to numerous charges of conspiracy, computer intrusion, computer fraud, credit card fraud, wire fraud, and extortion. Those charges stemmed from the activities of the defendant and others who operated from Russia and hacked into dozens of computers throughout the United States, stealing usernames, passwords, credit card information, and other financial data, and then extorting money from those victims with the threat of deleting their data and destroying their computer systems.[12]

- In May 2002, a New Jersey man was convicted of causing more than $80 million in damage by unleashing the "Melissa" computer virus in 1999 and disrupting personal computers and computer networks in business and government.[13]

[10]U.S. Attorney's Office District of Massachusetts, Press Release, "Massachusetts Teen Convicted for Hacking into Internet and Telephone Service Providers and Making Bomb Threats to High Schools in Massachusetts and Florida" (Sept. 8, 2005), www.cybercrime.gov/juvenileSentboston.htm (Accessed Mar. 30, 2007).

[11]Department of Justice (DOJ) Criminal Division, Press Release, "Shadowcrew Organization Called 'One-Stop Online Marketplace for Identity Theft'" (Oct. 28, 2004), www.cybercrime.gov/mantovaniIndict.htm (Accessed Mar. 30, 2007).

[12]U.S. Attorney's Office District of Connecticut, Press Release, "Russian Man Sentenced for Hacking into Computers in the United States" (July 25, 2003), www.cybercrime.gov/ivanovSent.htm (Accessed Mar. 30, 2007).

[13]U.S. Attorney's Office District of New Jersey, Press Release, "Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison" (May 1, 2002), www.cybercrime.gov/melissaSent.htm (Accessed Mar. 30, 2007).

Cybercrime Is a Threat to National Security

There is continued concern about the threat that our adversaries pose to our national security through attacks on our computer-reliant critical infrastructures and theft of our sensitive information. Over the last several years, such risks have been described in a variety of reports and testimonies. Table 5 describes the concerns raised.

Table 5: Reports and Testimonies Describing Threats to National Security

Source	Description	Potential attackers
Director of Central Intelligence (1996)[a]	Hackers, terrorists, or other nations could use information warfare techniques as part of a coordinated attack to seriously disrupt electric power distribution, air traffic control, or financial sectors.	A number of countries are developing the doctrine, strategies, and tools to conduct information attacks. International terrorists groups clearly have the capability to attack the information infrastructure of the United States.
Chief of the National Infrastructure Protection Center (NIPC) of the FBI (1998)[b]	Crimes illustrate "the growing problem of cybercrime, the international dimension of the problem, and the increasing threat to our critical infrastructure."	Transnational criminals are rapidly becoming aware of and exploiting the power of cyber tools.
Center for Strategic and International Studies (1999)[c]	Our nation has a "range of enemies today, not only military enemies, but who have the same capabilities to do major damage to the infrastructure upon which we all depend."	Criminals, terrorists, and others
National Communications Systems (NCS), an interagency committee formed to examine communication networks (1999)[d]	Adversaries could disrupt, disable, or collect sensitive data through coordinated attacks on U.S. computer systems.	Organized crime groups are targeting such systems to commit fraud, acquire and exploit proprietary information, and steal funds and securities transmitted through electronic commerce systems.
Director of Central Intelligence (2002)[e]	September 11 attacks demonstrated the nation's dependence on critical infrastructure systems that rely on electronic and computer networks. Further, attacks of this nature would become an increasingly viable option for terrorists as they and other foreign adversaries become more familiar with these targets and the technologies required to attack them.	Terrorist organizations
Institute for Security Technology Studies at Dartmouth College (2003)[f]	Cyber warfare attacks against our critical infrastructure system will become an increasingly viable option.	Nation states and terrorists as they become more familiar with these targets and the required attack technologies
FBI Director (2005)[g]	State actors continue to be a threat to both our national security, as well as our economic security, because they have the technical and financial resources to support advanced network exploitation and attack. The greatest cyber threat is posed by countries that continue to openly conduct computer network attacks and exploitations on American systems.	Foreign governments, terrorist groups, and hackers with the ability and the desire to utilize computers for illegal and harmful purposes

Source: GAO analysis of various reports and testimonies.

[a]Statement for the Record by the Director of Central Intelligence to the U.S. Senate Committee on Governmental Affairs, Permanent Subcommittee on Investigations, "Foreign Information Warfare Programs and Capabilities" (June 25, 1996).

[b]Statement for the Record, Deputy Assistant Director and Chief, National Infrastructure Protection Center, Federal Bureau of Investigation, before the Congressional Joint Economic Committee (Mar. 24, 1998).

[c]The Center for Strategic and International Studies, "Cybercrime, Cyberterrorism, and Cyberwarfare: Averting an Electronic Waterloo" (Dec. 15, 1999).

[d]National Communications System, "The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document," third edition (March 1999).

[e]Statement of the Director of Central Intelligence to the U.S. Senate Select Committee on Intelligence, "Current and Projected National Security Threats to the United States" (Feb. 6, 2002).

[f]Institute for Security Technology Studies at Dartmouth College,"Examining the Cyber Capabilities of Islamic Terrorist Groups" (Hanover, N.H.: March 2004).

[g]Statement of the FBI Director to the U.S. Senate Select Committee on Intelligence, "Current and Projected National Security Threats to the United States" (Feb. 16, 2005).

The risks posed by this increasing and evolving threat are demonstrated by actual and potential attacks and disruptions, such as those cited below.

- DOD officials stated that its information network, representing approximately 20 percent of the entire Internet, receives approximately 6 million probes/scans a day. Further, representatives from DOD stated that between January 2005 and July 2006, the agency initiated 92 cybercrime cases, the majority of which involved intrusions or malicious activities directed against its information network.

- In November 2006, the U.S.-China Economic and Security Review Commission[14] reported that China is actively improving its nontraditional military capabilities. According to the study, Chinese military strategists write openly about exploiting the vulnerabilities created by the U.S. military's reliance on advanced technologies and the extensive infrastructure used to conduct operations. Chinese military writings also refer to attacking key civilian targets such as financial systems. In addition, the report stated that Chinese intelligence services are capable of compromising the security of computer systems. The commission also provided instances of computer network penetrations coming from China. For example, in August and September 2006, attacks on computer systems of the Department of Commerce's Bureau of Industry and Security forced

[14]U.S.-China Economic and Security Review Commission, *2006 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, D.C.: November 2006).

the bureau to replace hundreds of computers and lock down Internet access for 1 month.

- In August 2006, a California man was convicted for conspiracy to intentionally cause damage to a protected computer and commit computer fraud. Between 2004 and 2005, he created and operated a botnet that was configured to constantly scan for and infect new computers. For example, in 2 weeks in February of 2005, the defendant's bots reported more than 2 million infections of more than 629,000 unique addresses (some infected repeatedly). It damaged hundreds of DOD computers worldwide. The DOD reported a total of $172,000 of damage due to a string of computer intrusions at numerous military installations in the United States (including Colorado, Florida, Hawaii, Maryland, South Carolina, and Texas) and around the world (including Germany and Italy). In addition, the botnet compromised computer systems at a Seattle hospital, including patient systems, and damaged more than 1,000 computers in a California school district over the course of several months in 2005. Officials from the California school district reported damages between $50,000 and $75,000 to repair its computers after the botnet struck in February 2005.[15]

- The Central Intelligence Agency has identified two known terrorist organizations with the capability and greatest likelihood to use cyber attacks against our infrastructures.[16]

- In March 2005, security consultants within the electric industry reported that hackers were targeting the U.S. electric power grid and had gained access to U.S. utilities' electronic control systems. Computer security specialists reported that, in a few cases, these intrusions had "caused an impact." While officials stated that hackers had not caused serious damage to the systems that feed the nation's power grid, the constant threat of intrusion has heightened concerns that electric companies may not have

[15]DOJ, United States Attorney for the Western District of Washington, Press Release, *California Man Sentenced for "Botnet" Attack that Implicated Millions: Network of Robot Computers Damaged Military Installations, Northwest Hospital, and California School District* (Seattle, WA: Aug. 25, 2006).

[16]Statement for the Record, Information Operations Issue Manager, Central Intelligence Agency, before the Congressional Joint Economic Committee (Feb. 23, 2000).

adequately fortified their defenses against a potential catastrophic strike.[17]

- Terrorist organizations have used cyberspace and cybercrime to raise money in a number of ways, such as facilitating protection schemes, credit card fraud, and drug smuggling. For example, in a July 2002 testimony, FBI officials stated that Al Qaeda terrorist cells in Spain used stolen credit card information to make numerous purchases.[18] In addition, Indonesian police officials believe the 2002 terrorist bombings in Bali were partially financed through online credit card fraud, according to press reports.[19]

As larger amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that information attacks will threaten vital national interests.

Precise Magnitude of Cybercrime Is Unknown

Despite the large reported impact of cybercrime, the true impact of cybercrime in the United States is unknown because cybercrimes are not always detected or reported. Organizations and individuals do not always detect cybercrimes. The effectiveness of the systems put in place to audit and monitor systems, including intrusion detection systems, intrusion protection systems, security event correlation tools, and computer forensics tools,[20] have limitations that impact their ability to detect a crime

[17]GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (Washington, D.C.: May 26, 2005).

[18]Statement for the Record, Chief, Terrorist Financial Review Group, FBI, before the Senate Judiciary Committee, Subcommittee on Technology, Terrorism and Government Information (July 9, 2002).

[19]*The Washington Post*, *An Indonesian's Prison Memoir Takes Holy War Into Cyberspace* (Dec. 14, 2004).

[20]Intrusion detection systems detect inappropriate, incorrect, or anomalous activity on a network or computer system. Intrusion prevention systems build on intrusion detection systems to detect attacks on a network and take action to prevent them from being successful. Security event correlation tools monitor and document actions on network devices and analyze the actions to determine if an attack is ongoing or has occurred. Computer forensic tools identify, preserve, extract, and document computer-based evidence.

occurring.[21] For example, the effectiveness of intrusion detection systems is limited by their ability to capture accurate baselines or normal network or system activity. Also, these systems are prone to false positives and false negatives and are not as effective in protecting against unknown attacks. In addition, the effectiveness of security event correlation tools is limited by their ability to interface with numerous security products and the quality of the logs they rely upon.

When a cybercrime is detected, companies and individuals can choose not to report the crime. Companies and individuals weigh the cost and impact of the incident with the time and effort needed to support an investigation and prosecution. Cybercrime reporting is discussed further in our challenges section.

Numerous Public and Private Organizations Have Responsibilities to Protect Against, Detect, Investigate, and Prosecute Cybercrime

Federal agencies, state and local law enforcement, private industry, and academia have responsibilities, based on their primary missions or business interests, to protect against, detect, investigate, and prosecute cybercrime. Public and private sector entities are engaged in these efforts individually and through collaborative efforts.

Many Public Entities Have Responsibilities for Addressing Cybercrime

DOJ, DHS, and DOD and the FTC have key roles in addressing cybercrime within the federal government, along with the federal inspectors general. State and local law enforcement organizations also have key responsibilities in addressing cybercrime. Efforts range from fighting cybercrime by investigating and prosecuting it and improving the protection of systems through raising awareness and building relationships.

[21]GAO, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*, GAO-04-321 (Washington, D.C.: May 28, 2004).

Key Department of Justice Organizations

The key agencies within DOJ that focus on enforcing cybercrime violations include the Criminal Division, U.S. Attorneys, and the FBI. Table 6 shows key DOJ organizations, suborganizations, and activities.

Table 6: Department of Justice's Key Organizations and Activities to Mitigate Cybercrime

Organization	Cyber responsibility	Suborganizations and activities
Criminal Division	Implements and supports both the department's Computer Crime Initiative, designed to combat electronic penetrations, data thefts, and cyber attacks on critical information systems, and the department's aggressive battle to protect children from individuals who use computers and the Internet to sexually abuse and exploit them.	**Computer Crimes and Intellectual Property Section (CCIPS):** • Investigates and prosecutes computer crime and intellectual property offenses. • Works with other government agencies, the private sector, academic institutions, and foreign counterparts to prevent, investigate, and prosecute computer crimes. • Provides training to federal, state, and local law enforcement agents; prosecutors; and other government officials on a number of cybercrime-related topics. • Performs public outreach to improve communications and trust between the public and private sectors. • Coordinates closely with the Department of State on international cybercrime initiatives, such as the G-8 High-Tech Crime Subgroup, and negotiation of the Council of Europe's Convention on Cybercrime. • Develops policy and legislation aimed at enhancing the government's ability to combat cybercrime. **Child Exploitation and Obscenity Section (CEOS):** • Leads and coordinates federal law enforcement agencies in effective strategies and policies to combat online child sexual exploitation. • Investigates and prosecutes complex and significant online child sexual exploitation cases. • Provides training, policy, and legislative support for prosecution efforts with U.S. Attorneys and law enforcement partners. • Works with nongovernment organizations such as the National Center for Missing and Exploited Children and with foreign partners to combat online child sexual exploitation. **Fraud Section:** • Investigates and prosecutes fraud offenses involving misuse of computers and the Internet (e.g., Internet fraud, identity theft). • Provides coordination with other departmental components and federal, state, and local law enforcement agencies in investigating and prosecuting Internet fraud. • Provides and coordinates training for federal, state, and local law enforcement agencies on Internet fraud and identity theft. • Participates in multilateral law enforcement meetings on Internet fraud and identity theft, including heading the U.S. delegation to the United Nations Crime Commission Expert Group on Fraud and Identity Theft.

Organization	Cyber responsibility	Suborganizations and activities
U. S. Attorneys' Offices	Coordinate the investigation of, and prosecutes, cybercrime matters.	**Computer Hacking and Intellectual Property (CHIP) units:** 25 units assigned to select U.S. Attorneys' Offices throughout the United States. In addition, the remaining 68 U.S. Attorneys' Offices have at least one full-time equivalent designated to work on CHIP prosecutions. Within their region of jurisdiction, the attorneys • prosecute high-technology offenses, including computer hacking, virus and worm proliferation, Internet fraud, and other attacks on computer systems; • coordinate with CCIPS, FBI, and other agencies to establish good working relationships with the high-technology community and encourage victims to report crimes; • develop and offer regional training programs to increase expertise among federal, state, and local prosecutors; and • provide legal advice to prosecutors and law enforcement officers in their respective districts on the collection of digital evidence, cybercrimes, and intellectual property laws. **Project Safe Childhood Coordinators:** Each U.S. Attorneys' Office has one coordinator trained to prosecute child pornography cases that typically involve the collection and presentation of digital evidence and the use of the Internet.
FBI Cyber Division	Investigates cyber matters and cybercrime as the federal lead agency and as its third strategic priority.	**Computer Intrusion Section:** Agents in FBI headquarters and 56 field offices trained to investigate computer intrusion incidents. These agents • investigate and prevent computer intrusions; • deploy Cyber Action Teams—highly trained teams of FBI agents, analysts, and computer forensics and malicious code experts—to respond to fast-moving cyber threats; and • work with the Computer Analysis Response Teams under the Operations Technology Division, Science and Technology Branch, that conduct cyber forensic analysis and evidence gathering in support of cybercrime investigations. **Cyber Crime Section:** Agents in FBI headquarters and 56 field offices responsible for computer fraud and child exploitation cases. These agents • maintain the Innocent Images National Initiatives unit to conduct undercover operations and investigations of child exploitation cases and cybercrime fraud; • work with public and private entities such as the National Center for Missing and Exploited Children to investigate and share information on child exploitation; and • coordinate with other federal and local law enforcement to combat cybercrime through the Internet Crime Complaint Center and the Cyber Initiative and Resource Fusion Unit. **Information Sharing and Analysis Section:** • Maintains a national-level responsibility for analyzing and disseminating all FBI cyber threat information. • Establishes cyber threat collection requirements, in order to deter, detect, and disrupt cyber threats that affect national security and criminal activity. • Manages the FBI's InfraGard Program.

Organization	Cyber responsibility	Suborganizations and activities
FBI field offices	Investigate cyber matters and cybercrime within their region of responsibility.	**Computer Intrusion Program:** agents in each of the 56 offices assigned to investigate computer intrusion matters in every state and Puerto Rico.
		Computer Crime Task Forces: 93 task forces located throughout the country that combine state-of-the-art technology and the resources of federal, state, and local counterparts to combat all types of cybercrimes.
		Regional Computer Forensics Laboratories: FBI-funded laboratories that provide forensic laboratory services to a geographic area's entire law enforcement community.
		Computer Analysis Response Teams: specialists that gather evidence and perform cyberforensic examinations in support of field-led investigations and gather evidence for the headquarters forensics laboratory.

Sources: GAO and DOJ.

Key Department of Homeland Security Organizations

Three key agencies within DHS have a role in addressing cybercrime issues—the Secret Service, the Cyber Security and Communications Office's National Cyber Security Division, and Immigration and Customs Enforcement. Table 7 shows key DHS organizations, suborganizations, and activities.

Table 7: Department of Homeland Security's Key Organizations and Activities to Mitigate Cybercrime

Organization	Cyber responsibility	Suborganizations and activities
Secret Service	Investigates crimes that are a threat to the country's financial infrastructures and places emphasis on computer fraud, cybercrime, identity theft, and other types of electronic crime.	**Electronic Crimes Special Agents:** Agents assigned to headquarters and over 70 domestic and foreign offices. • Investigate cybercrime and conduct cyberforensics. • Train agents to investigate cybercrime, network intrusions, and Internet-based crime. • Assist other federal, state, and local law enforcement agencies. **Electronic Crimes State and Local Program:** A program to train state and local law enforcement officers to investigate cybercrime. • Trains officers in the areas of basic electronic crimes investigations, network intrusions, and computer forensics. • Creates cybercrime first responders at the state and local level. **Electronic Crimes Task Forces:** A network of 24 task forces creating strategic alliances among federal, state, and local law enforcement agencies and private sector entities. • Prevent, detect, and investigate various forms of electronic crime by increasing resources and sharing information to disrupt criminal activity. • Suppress technology-based criminal activity by building partnerships and sharing information. **Criminal Intelligence Section:** Serves as a central repository for data generated through Secret Service field investigations, open source Internet content, and information obtained through financial and private industry partnerships. • Coordinates, analyzes, and disseminates data in support of Secret Service investigations. • Generates investigative leads based upon criminal intelligence. • Monitors developing technologies and trends in the financial payments industry to prevent and mitigate attacks against the financial infrastructure. **National Computer Forensic Institute:** In collaboration with the State of Alabama, a national cybercrime training facility is being developed to train state and local law enforcement officers, prosecutors, and judges in the areas of basic electronic crimes investigation, network intrusion investigation, and computer forensics.

Organization	Cyber responsibility	Suborganizations and activities
National Cyber Security Division	Serves as the national focal point for addressing cybersecurity issues and coordinating implementation of the nation's cybersecurity strategy.	**Law Enforcement and Intelligence Section:** Serves a liaison function that provides a mechanism for information sharing of cyber-related efforts with the law enforcement and intelligence communities. • Manages the National Cyber Response Coordination Group[a] protection efforts. • Facilitates the coordination of law enforcement and intelligence cyber-related efforts for NCSD. **U.S. Computer Emergency Readiness Team (US-CERT):** A partnership with public and private sector entities to protect the nation's critical Internet infrastructure. • Facilitates information sharing between federal and nonfederal law enforcement and intelligence entities through the National Cyber Security Response System. • Analyzes and reduces cyber threats and vulnerabilities, and disseminates cyber threat warning information. **Cyber Cop Portal:** A secure, Internet-based, information-sharing mechanism that allows members of local, state, and federal government law enforcement organizations to discuss issues related to electronic/cyber crime and threat reduction. **Strategic Initiatives Branch:** Coordinates with public and private sector security partners to understand the cyber threats confronting the nation's critical infrastructure, including cybercrime, and factoring it into risk assessment and management activities.

Organization	Cyber responsibility	Suborganizations and activities
Immigration and Customs Enforcement (ICE)	Investigates and seeks prosecution of domestic and transborder criminal activities occurring on or facilitated by the Internet, primarily within its authority to investigate immigration and customs violations.	**Cyber Crimes Center:** Headquarters center that provides cyber-related technical and investigative services, training, and guidance to ICE headquarters and field office investigators and foreign attachés, as well as other foreign and domestic law enforcement entities. • Develops and coordinates national-level Internet investigations, including online undercover operations, related to crimes investigated by ICE such as: transborder child exploitation, identity and benefit fraud, intellectual property rights, commercial fraud, strategic and national security, financial crimes, and general smuggling investigations. • Performs forensics examination of electronic devices such as personal computers, personal digital assistants, cellular telephones, and other communication devices and operates the ICE National Digital Forensics Laboratory. • Conducts research and development on new and emerging technologies. **ICE Field Offices:** Digital Forensics Agents located in field offices throughout the United States perform forensic examinations of detained and/or seized digital storage devices in field laboratories, assist online field investigators in preparing search warrants targeting digital evidence, and provide expert testimony and support to state and local law enforcement agencies. **ICE Foreign Attachés Offices:** Attachés located in ICE foreign offices coordinate investigative efforts with foreign law enforcement entities.

Sources: GAO and DHS.

[a]The National Cyber Response Coordination Group is a forum of national security, law enforcement, defense, intelligence, and other government agencies that coordinates governmental and public/private preparedness and response to and recovery from national level cyber incidents and physical attacks that have significant cyber consequences.

Key Department of Defense Organizations

Within DOD, the Defense Criminal and Counterintelligence Investigation Organizations conduct all law enforcement investigations and the Defense Cyber Crime Center (DC3) can provide forensics support. Table 8 shows key organizations, suborganizations, and activities.

Table 8: Department of Defense Key Organizations and Activities to Mitigate Cybercrime

Organization	Cyber responsibility	Suborganizations and activities
Defense Criminal and Counterintelligence Investigative organizations[a]	Leading law enforcement agencies in the DOD for investigating computer crimes.	**Department of Defense Criminal Investigative Service (DCIS):** Computer Crime Coordinators (CCCs) and Agents (CCAs) investigating cybercrime and computer intrusions that directly impact DOD. • Establishes policies and procedures for computer crime investigations and computer forensics. • Investigates all computer intrusions and attacks involving DOD and DOD-protected computers. • Maintains six field offices with CCCs to determine the appropriate investigative response for computer crimes and CCAs to investigate and provide computer forensics support. • Manages a Web site to increase awareness about threats children face from the Internet and to provide a Web portal to report suspicious situations. **Air Force Office of Special Investigation (AFOSI):** Special agents and support personnel in AFOSI's Information Operations and Investigations program conduct criminal and counterintelligence investigations in response to cyber crimes and threats directed against the U.S. Air Force and numerous DOD activities. • Provides forensic analysis of digital evidence and other highly specialized investigative support to criminal, fraud, counterintelligence, and counterespionage cybercrime investigations. • Conducts local, national, and international computer network intrusion investigations. **Army Counterintelligence:** • Investigates reported cybercrimes to determine if counterintelligence efforts are warranted. **Naval Criminal Investigative Service (NCIS):** Special agents and computer scientists in NCIS's Cybercrime Department investigate cyber threats against the U.S. Navy and Marine Corps. • Conducts national and local computer network intrusion investigations. • Provides advanced forensic media analysis tools and techniques to support cybercrime investigations. • Collaborates with the Naval Network Warfare Command and Navy Cyber Defense Operations Command on cybercrime investigation, counter intelligence, and operational defense efforts related to Navy networks.

Organization	Cyber responsibility	Suborganizations and activities
DC3	Performs computer forensic investigations for the Defense Criminal and Counterintelligence Investigative organizations.	**Defense Computer Forensics Laboratory:** An accredited laboratory for digital forensic examinations in DOD. • Performs digital forensic examinations on digital evidence from counterintelligence, child pornography, and illegal use of government computer investigations. • Provides services such as digital media restoration. **Defense Computer Investigations Training Program:** A program producing digital forensic examiners and cybercrime investigators. • Trains investigators from the DOD, FBI, Secret Service, and the State Department's Diplomatic Security Services. • Introduces trainees to state-of-the-art equipment and technologies. **Defense Cyber Crime Institute:** A research and development directorate for cyber forensics. • Researches and tests digital forensic hardware and software that includes the preview and testing of vendor products. • Develops and tests digital forensics tools. • Maintains a knowledge management system for digital forensics tactics.
Joint Task Force—Global Network Operations	Protects and detects computer crimes affecting the DOD Global Information Grid.	**Global Network Operations:** A task force of 375 special agents and analysts from each of the Defense Criminal Investigative and Counterintelligence organizations. • Directs the operations and defense of the DOD Global Information Grid. • Continually monitors the grid and notifies its collocated law enforcement and counterintelligence staff of any unusual activity.

Sources: GAO and DOD.

[a]DOD Criminal and Counterintelligence Investigative Organizations include the Air Force Office of Special Investigations, Army Military Intelligence, Army Criminal Investigations Command, Naval Criminal Investigative Service, and Defense Criminal Investigative Service.

Federal Trade Commission

The FTC was created to prevent unfair methods of competition. Its mission expanded over time with additional legislation authorizing it to serve as a protective force for U.S. consumers. The agency has the authority to file civil enforcement actions either in federal district court or administratively. Remedies in these civil actions range from orders to stop the illegal conduct to requiring disgorgement of illegal proceeds or payment of restitution.

FTC's Bureau of Consumer Protection investigates and enforces matters related to activities that may be classified as cybercrime. It has several divisions that focus primarily on different aspects of the FTC's consumer protection mission. According to FTC staff, the Bureau of Consumer Protection is composed of six divisions, which target different substantive areas for enforcement and outreach purposes. The divisions routinely

coordinate initiatives and share resources to most efficiently and effectively further the consumer protection mission. Its resources include headquarter staff and staff located at eight regional offices that investigate and bring a variety of consumer protection and competition cases and engage in outreach efforts. In addition, the Criminal Liaison Unit coordinates for all of the Bureau of Consumer Protection's divisions with criminal law enforcement agencies across the U.S. to encourage the prosecution of criminal fraud.

Federal Inspectors General

Federal Inspectors General have a role in preventing, detecting, and investigating cybercrime within their respective agencies. Specifically, 14 of 19 Inspectors General that provided information to us stated that they handle cybercrime investigations affecting their respective agency within their own capabilities. For example, certain Inspectors General reported having significant efforts in addressing cybercrime, including those for the Departments of Education, Energy, and Transportation and the Environmental Protection Agency. Additionally, 11 of the 19 Inspectors General stated that they perform an education and awareness role within their respective agencies by conducting training, providing presentations, and performing activities mandated by the Federal Information Security Management Act.[22]

State and Local Law Enforcement Organizations

State and local organizations address cybercrime through efforts to share information, improve expertise, and facilitate cybercrime prosecutions both nationally and locally. For example, on a national basis, SEARCH, an organization dedicated to improving state-level law enforcement, has three cybercrime focused programs related to providing high-tech crime training, technical assistance, and research on emerging technology nationwide. In addition, the National Association of Attorneys General has a cybercrime initiative benefiting state prosecutors. It also hosts a cybercrime conference that provides training in cybercrime investigative areas, legislation, case law, and public education tools. The association's executive working group meets quarterly and shares information on criminal issues, including cybercrime.

[22]The Federal Information Security Management Act was enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, to establish clear criteria to improve federal agencies' information security programs. According to the act, information security is defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to maintain their integrity, confidentiality, and availability.

State-level law enforcement entities have implemented initiatives to facilitate the investigation and prosecution of cybercrime in the states. For example, the Commonwealth of Virginia's Office of the Attorney General has a Computer Crime unit dedicated to investigating criminal cases violating the Virginia Computer Crimes Act. In addition, Virginia's Attorney General formed the Virginia Cyber Crime Strike Force that collaborates with the U.S. Attorneys' Offices, the Virginia State Police, the FBI and Virginia's Bedford County Sheriff's Office to investigate and prosecute cybercrime. Other examples of state efforts are the (1) Washington Attorney General's High Tech Crime Unit, which litigates cases of cyberfraud, and pursues civil remedies under the state's broad consumer protection law and (2) Washington State Patrol Computer Crime unit that serves as a first responder to computer crimes affecting state-funded institutions such as state and local governments and public schools and universities.

Private-Sector Entities Focus on Protection and Detection Efforts

The private sector's focus is on the development and implementation of technology systems to protect against computer intrusions, Internet fraud, and spam and, if a crime does occur, to detect it and gather admissible evidence for an investigation. The private entities that focus on these technological efforts include Internet service providers, security vendors, software developers, and computer forensics vendors:

- Internet service providers offer businesses and home users various levels of access to the Internet and other Internet-related services such as customer support and spam and virus protection. Providers also assist law enforcement by monitoring and providing information on selected Internet activities and provide technical expertise to assist with investigations. In addition, providers can pursue civil action against users to punish inappropriate behavior.

- Security vendors such as e-mail security firms can screen electronic messages for harmful data and take action to prevent such data from reaching the intended target. Vendors also assist law enforcement by reporting instances of computer crime, providing technical assistance, and pursuing civil action against inappropriate behavior.

- Software developers are improving the quality and security of operating system programs to detect and block malicious code.

- Computer forensics vendors provide private companies with computer forensics investigative services to detect the theft of trade secrets and

intellectual property, detect employee fraud, locate and recover previously inaccessible documents and files, provide reports on all user activity, and access password-protected files. In addition, computer forensic vendors develop tools used by law enforcement to investigate cybercrime. These tools allow for the analysis of digital media and the gathering of evidence that is admissible in court.

Numerous Public and Private Partnerships Work to Address Cybercrime

Numerous partnerships have been established between public sector entities, between public and private sector entities, and internationally to collaborate and implement effective cybercrime strategies. Each of their strategies includes information sharing activities and consumer awareness efforts. Table 9 gives brief descriptions of key partnerships, their purposes, and primary stakeholders.

Table 9: Key Partnerships Established to Address Cybercrime

Organization	Cybercrime purpose	Primary stakeholders
Internet Crime Complaint Center	A partnership between the FBI and the National White Collar Crime Center[a] that serves as a means to receive Internet-related criminal complaints, further research and development, and refer criminal complaints to law enforcement and government agencies.	Federal, state, local, or international law enforcement and/or regulatory agencies
InfraGard	An information sharing and analysis effort established by the FBI to protect physical and cyber-based critical infrastructure assets.	Federal, state, and local law enforcement agencies, academia, private industry, and other government agencies
The National Cyber Security Alliance	A partnership established by the federal government to provide cybersecurity awareness and education resources for the home user, small business, and education audience.	DHS, FTC, and private-sector corporations and organizations
National Cyber Forensics and Training Alliance	A partnership established by the FBI, the National White Collar Crime Center, and Carnegie Mellon and West Virginia Universities to provide a venue to share critical confidential information about cyber incidents and share resources.	Industry, academia, and law enforcement
Electronic Crimes Task Forces	As discussed earlier, established by the Secret Service to create strategic alliances among various stakeholders.	Federal, state, and local law enforcement agencies and private-sector entities

Organization	Cybercrime purpose	Primary stakeholders
Cyber Initiative and Resource Fusion Unit	A spin-off of the IC3 that follows the early investigative trail in some complex technical cases. Center analysts eliminate false leads and refine a case before it is referred to a local or international law enforcement agency or task force. The center is supported by online organizations and merchants. Federal agents and analysts from industry and academia work together to find out where the crime originates, who is behind it, and how to fight it. They identify Internet crime trends and technologies, develop significant cases, and help law enforcement agencies worldwide identify and combat Internet crimes.	Federal, state, and local law enforcement agencies, academia, private industry, and other government agencies
Anti-Phishing Working Group	An association focused on eliminating fraud and identity theft that result from phishing, pharming, and e-mail spoofing of all types.	Private industry, academic institutions, and law enforcement agencies
SEARCH	A nonprofit membership organization that has developed extensive programs to assist justice and public safety agencies. Their cybercrime efforts support law enforcement by providing a High-Tech Crime Training Program, technical assistance, and research into emerging technology issues.	State and local law enforcement agencies, first responders, and prosecutors
The Business Software Alliance	A nonprofit trade association dedicated to promoting a safe and legal digital world. It is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce.	Commercial software and computer hardware industry
Cybercrime Institute	A collaborative venture in Georgia with Kennesaw State University and the FBI, the Georgia Bureau of Investigation, the State Attorney General's Office, the Georgia Technology Authority, and the National White Collar Crime Agency to provide education and training in the fight against cybercrime.	Professionals in governmental agencies, law enforcement, corporations, universities, and colleges

Source: GAO analysis of various reports and documents.

[a]The National White Collar Crime Center provides a nationwide support system for agencies involved in the prevention, investigation, and prosecution of economic and high-tech crimes and to support and partner with other appropriate entities in addressing homeland security initiatives, as they relate to economic and high-tech crimes. Through a combination of training and critical support services, they equip state and local law enforcement agencies with skills and resources they need to tackle emerging economic and cybercrime problems.

Public and Private Sectors Face Challenges in Addressing Cybercrime

Numerous challenges impede the efforts of public and private entities to mitigate cybercrime (see table 10) including (1) reporting cybercrime, (2) ensuring adequate law enforcement analytical and technical capabilities, (3) working in a borderless environment with laws of multiple jurisdictions, and (4) implementing information security practices and raising awareness.

Table 10: Challenges to Addressing Cybercrime

Challenge	Description
Reporting cybercrime.	Accurately reporting cybercrime to law enforcement.
Ensuring adequate law enforcement analytical and technical capabilities.	Obtaining and retaining investigators, prosecutors, and cyberforensics examiners. Keeping up-to-date with current technology and criminal techniques.
Working in a borderless environment with laws of multiple jurisdictions.	Investigating and prosecuting cybercrime that transcends borders with laws and legal procedures of multiple jurisdictions.
Implementing information security practices and raising awareness.	Protecting information and information systems. Raising awareness about criminal behavior.

Source: GAO.

Reporting Cybercrime

Although surveys and studies show that the nation potentially loses both billions of dollars annually and sensitive information as a result of cybercrime, definitive data on the amount of cybercrime is not available. Understanding the impact of cybercrime in the United States is a challenge because reporting of cybercrime is limited.

When a cybercrime is detected, entities and individuals can choose to report it to law enforcement or not. They weigh the cost and impact of the incident with the time and effort needed to support an investigation and prosecution. In addition, our work and findings of the Congressional Research Service related to information sharing have shown that businesses do not always want to report problems because there is a perception that their information will be disclosed publicly, which could,

in turn, cause harm to their business.[23] Reasons for not reporting a crime to law enforcement include the following:

- *Financial market impacts.* The stock and credit markets and bond rating firms react negatively to security breach announcements, which could raise the cost of capital to reporting firms. Even firms that are privately held and are not active in public securities markets can be adversely affected if banks and other lenders judge them to be more risky than previously thought.

- *Reputation or confidence effects.* Negative publicity damages a reporting firm's reputation or brand, and could cause customers to lose confidence, giving commercial rivals a competitive advantage.

- *Litigation concerns.* If an organization reports a security breach, investors, customers, or other stakeholders can use the courts to seek recovery of damages. If the organization has been open in the past about previous incidents, plaintiffs may allege a pattern of negligence.

- *Signal to attackers.* A public announcement alerts hackers that an organization's cyber-defenses are weak and can inspire further attacks.

- *Inability to share information.* Some private-sector entities want to share information about an incident with law enforcement and other entities; however, once the information becomes part of an ongoing investigation, their ability to share information may be limited.

- *Job security.* IT personnel fear for their jobs after an incident and seek to conceal the breach from senior management.

- *Lack of law enforcement action.* According to private sector officials, law enforcement entities have failed to investigate cases reported to them, which is a disincentive for them reporting crimes in the future.

To improve the reporting of cybercrime, the numerous public/private partnerships (e.g., the National Cyber Forensics and Training Alliance, InfraGard, and the Electronic Crimes Task Forces), as well as the

[23]GAO, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24 (Washington, D.C.: Oct. 15, 2001) and GAO, *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, GAO-03-233 (Washington, D.C.: Feb. 28, 2003); Congressional Research Service, *The Economic Impact of Cyber Attacks*, RL 32331 (Washington, D.C.: Apr. 1, 2004).

awareness and outreach efforts of law enforcement discussed earlier, are methods for building better relationships and understanding between the public and private sectors. These efforts may increase trust between the public and private sector and encourage better reporting of cybercrimes when they occur.

Ensuring Adequate Law Enforcement Analytical and Technical Capabilities

Efforts by law enforcement to investigate and prosecute cybercrime require individuals with specialized skills and tools. According to federal, state, and local law enforcement and private sector officials, it is a challenge to recruit such individuals from a limited pool of available talent, retain them in the face of competing offers, and train them to stay up to date with changing technology and increasingly sophisticated criminal techniques.

Obtaining and Retaining Investigators, Prosecutors, and Cyberforensics Examiners

Federal and state law enforcement organizations face challenges in having the appropriate number of skilled investigators, forensic examiners, and prosecutors. According to federal and state law enforcement officials, the pool of qualified candidates is limited because individuals involved in investigating or examining cybercrime are highly trained specialists requiring both law enforcement and technical skills, including knowledge of various IT hardware and software and forensic tools. According to Defense Cyber Crime Center officials, once an investigator or examiner specializes in cybercrime, it can take up to 12 months for those individuals to become proficient enough to fully manage their own investigations. Further, according to state officials, state and local law enforcement agencies do not have the resources needed to hire the investigators with adequate technical knowledge required to address cybercrime.

Law enforcement organizations also find it difficult to retain highly skilled cyberforensic investigators and examiners. According to federal and state officials, the private sector demands individuals with the same skills and successfully attracts them away from their government positions with much higher salaries and better benefits. For example, according to an Assistant U.S. Attorney, several cybercrime experts, including attorneys, federal and state law enforcement agents, and cyberforensic examiners, have left their government positions due to the higher salaries and benefits offered by the private sector.

The available pool of experienced federal cybercrime investigators is also impacted by FBI and Secret Service rotation policies. For example, according to FBI officials, new FBI agents, not initially assigned to one of the 15 largest field offices, are required to rotate to one of the these large

offices after 3 years in order to have diversified experiences. According to FBI headquarters and field agents, when cybercrime investigators rotate out under this policy, they are not necessarily reassigned to cybercrime investigations in their new field office, and so their extensive cyber background is underutilized. In addition, the agents who rotate in to replace experienced cybercrime investigators may have little or no cybercrime experience or background. Further, according to FBI officials, the pool of experienced senior managers is impacted by the FBI's current policy that senior field supervisory agents are limited to 5-year terms in their positions and then most move to seek further career advancement. This can include the movement of experienced cybercrime investigators out of senior cybercrime positions. Similarly, according to Secret Service officials, most Secret Service agents, including those with technical, cybercrime investigation expertise, rotate to a protective assignment, which focuses on the protection of the President, Vice President, and others and not on the investigation of cybercrime. In addition, officials stated that there is an investigative career track that allows agents to continue doing investigations, including those related to cybercrime; however, protective assignments are perceived as higher profile and could lead to greater career advancement. FBI and Secret Service officials acknowledged that the rotation policies have at times resulted in these agencies underutilizing staff with cyber expertise.

Keeping Up to Date with Current Technology and Criminal Techniques

The rapid evolution of technology and cybercrime techniques means that law enforcement agencies must continuously upgrade technical equipment and software tools. Such equipment and tools are expensive, and agencies' need for them does not always fall into the typical federal replacement cycle. For example, in order for investigators to perform cyberforensic examinations and gather the evidence required to support a prosecution, the examiners and investigators must, in some cases, store and analyze huge amounts of digital data. According to federal law enforcement officials, the amount of data being collected is growing exponentially. However, according to law enforcement officials, state and local law enforcement agencies do not always have the resources to obtain the equipment necessary to analyze large amounts of data.

Law enforcement organizations also find that maintaining a current understanding of new criminal techniques and technologies can be difficult. For example, law enforcement agents are required to extract forensic data from IT devices that have only been on the market for months. They also must keep up with innovative criminal techniques and approaches. For example, techniques for assembling and controlling botnets are becoming increasingly sophisticated and difficult to trace,

making it difficult to identify certain spamming and phishing schemes. In addition, criminals are increasing their use of encryption techniques.[24] This requires law enforcement to continue to research and develop appropriate countermeasures. Training can help to keep investigators' skills current, but relevant courses are limited, costly, and time-consuming, and take agents away from the cases that they are investigating.

Federal and state law enforcement organizations are taking steps to improve their analytic and technical capabilities. For example, the Secret Service has developed training programs for federal, state, and local law enforcement and DOD's Defense Cyber Crime Center has a cyberforensic training program for DOD investigators and other law enforcement officials. Further, the FBI's Cyber Action Teams rapidly provide technical expertise to cybercrime investigations worldwide, when needed. To overcome shortfalls in equipment and electronic storage, the FBI is sponsoring regional computer forensics laboratories to serve the needs of an entire region's law enforcement. In addition, public/private partnerships, like the FBI's Infragard and National Cyber Forensics Training Alliance and the Secret Service's Electronic Crimes Task Forces, provide ways to share expertise between law enforcement, the private sector, and academia. Although it will continue to be a challenge to keep current with the rapid evolution of technology and cybercrime techniques, these DOD, FBI, and Secret Service efforts are positive steps to attempt to keep up with techniques and technology for investigations.

Working in a Borderless Environment with Laws of Multiple Jurisdictions

Law enforcement organizations face the challenge of investigating and prosecuting cybercrime that crosses national and state borders, and working with laws, legal procedures, and law enforcement entities from multiple jurisdictions. Working in this environment complicates most cyber investigations.

Private sector, individual, and law enforcement efforts are complicated by the borderless nature of cybercrime. As discussed earlier, cybercriminals are not hampered by physical proximity or regional, national, or international borders. Cybercriminals can be physically located in one nation or state, direct their crime through computers in multiple nations or states, and store evidence of the crime on computers in yet another nation

[24]Encryption is the process of encoding a message so that it can be read only by the sender and the intended recipient.

or state. This makes it difficult to trace the cybercriminals to their physical location. In addition, cybercriminals can take steps to remain anonymous, making it difficult, if not impossible, to attribute a crime to them.

Similar to efforts addressing traditional crime, efforts to investigate and prosecute cybercrime are complicated by the multiplicity of laws and procedures that govern in the various nations and states where victims may be found, and the conflicting priorities and varying degrees of expertise of law enforcement authorities in those jurisdictions. Laws used to address cybercrime differ across states and nations. For example, not all U.S. states have antispam laws or antispyware laws. In addition, an act that is illegal in the United States may be legal in another nation or not directly addressed in the other nation's laws. Developing countries, for example, may lack cybercrime laws and enforcement procedures.

Further, jurisdictional boundaries can limit the actions that federal, state, and local law enforcement can take to investigate cybercrime that crosses local, regional, and national borders. For example, state and local officials may be unable to pursue investigations outside of their jurisdiction, so when a cybercrime goes beyond their jurisdiction, they may need to rely upon officials of other jurisdictions to further investigate the crime. Additionally, extradition between states can be complicated depending on the laws of the state where the suspect is located and the knowledge of the states' law enforcement and judiciary regarding cybercrime. In addition, the United States does not have extradition arrangements with all nations, which makes it impossible to extradite a cybercriminal from certain nations. Extradition from nations having an extradition agreement with the United States can be complicated or impossible if the nation's laws do not make the action illegal or its magistrate is not knowledgeable about cybercrime. Also, state and local officials are unable to extradite persons from other nations without federal law enforcement assistance.

Conflicting priorities also complicate cybercrime investigations and prosecutions. Cybercrime can occur without physical proximity to the victim, and thus a cybercriminal can operate without victimizing a citizen in the jurisdiction or federal judicial district in which the crime originated. With no negative impact on the citizens in that district, there may be no incentive for the local citizens to press their law enforcement officers to investigate the crime. According to state officials, it is difficult to commit resources to crimes where the victims are outside their state or jurisdiction, although the suspected cybercriminal may be prosecuted in the jurisdiction where the victim is located.

Federal and state law enforcement organizations are taking steps to help them work in the borderless environment within which cybercriminals operate. For example, federal, state, and local law enforcement organizations participate in cybercrime task forces that combine a region's law enforcement capabilities to investigate and prosecute cybercrime in the most advantageous way. To address transnational jurisdiction, investigation, and prosecution issues, DOJ and the State Department have established agreements with more than 40 nations through the G-8 High Tech Crime Working Group to address cybercrime cooperatively. The Council of Europe's Cybercrime Convention is a similar international effort. These and other efforts are essential to addressing the transborder nature of cybercrime and enhancing the ability of law enforcement to capture, prosecute, and punish cybercriminals.

Implementing Information Security Practices and Raising Awareness

A major challenge in mitigating cybercrime is improving information security practices on the part of organizations and individual Internet users. Raising awareness about criminal behavior and the need to protect information and systems is a key activity in addressing cybercrime.

Protecting Information and Information Systems

Criminals often take advantage of poor computer security practices, which makes maintaining a strong information security posture vital to efforts to stop cybercrime. However, individuals allow easy access for criminals to their personal computers and electronic devices by not enabling security on those devices. Without adequate information security, critical systems and sensitive data are more susceptible to criminal access, theft, modification, and destruction. Further, our audits have shown that federal agencies do not adequately protect the information systems that the government relies upon to deliver services to its customers. In addition, over the last several years, we have identified the challenges associated with the federal government's efforts to coordinate public and private sector efforts to protect the computer systems that support our nation's critical infrastructures. As a result, federal information security has been on GAO's list of high-risk areas since 1997 and cyber critical infrastructure protection since 2003.[25] In addition, we have made numerous recommendations to enhance the security of federal information systems and cyber critical infrastructure protection efforts. Implementation of these recommendations is essential to protecting federal information systems.

[25]GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

Raising Awareness about Criminal Behavior

A major challenge is educating the public in how to recognize cybercrime when it is occurring. Criminals prey on people's ignorance and susceptibility to ruses. For example, attackers create e-mail and Web sites that appear legitimate, often copying images and layouts of actual Web sites. Some cybercrime techniques also take advantage of combinations of vulnerabilities. For example, phishing entices users to provide the sensitive information desired. However, phishers also use technical methods to exploit software and system vulnerabilities to reinforce users' perceptions that they are on a legitimate Web site.

Despite efforts by public and private entities to raise awareness about the importance of information security and the techniques used by criminals, users continue to not understand the need for protecting their personal information and to recognize unusual requests that could be criminal activity. The types of cybercrime that the media highlight, such as child pornography cases and major companies being hacked, do not tend to undermine people's trust in the Internet. For example, there continue to be reports of people falling victim to well-known scams such as the Nigerian 4-1-9 fraud.[26] In addition, even as awareness grows, practices are not easily changed. Further, the issues of adequate awareness apply to law enforcement. State and local law enforcement may not be aware of the cybercrime problem that could be impacting their citizens.

There are numerous steps being taken to improve security of information systems and raise user awareness. For example, as discussed earlier, information security vendors provide software and services; software developers are attempting to improve the quality and security of their products; public and private entities are working together to identify and mitigate risks, including criminal activities; and federal organizations, such as the FBI, the Secret Service, FTC, and DHS, sponsor programs and organizations to raise user awareness about securing their information and not becoming a victim of cybercrime. These are positive steps to improve security and raise awareness.

Conclusions

The actual and potential harms that result from cybercrime attacks in the United States are significant. Although the precise amount of economic

[26]The Nigerian 4-1-9 fraud is an advance fee scam where criminals deceive victims into the payment of a fee by persuading them that they will receive a very large benefit in return. Through the Internet, businesses and individuals around the world have been, and continue to be, targeted by perpetrators of this scam.

loss due to cybercrime is unknown, its impact is likely billions of dollars. In addition, nation-state and terrorist adversaries are seeking ways to attack our nation's critical infrastructures and steal our sensitive information.

While numerous public and private entities—federal agencies, state and local law enforcement, industry, and academia—have responsibilities to address these threats, they face challenges in protecting against, detecting, investigating, and prosecuting cybercrimes. These challenges include reporting cybercrime, ensuring adequate law enforcement analytical and technical capabilities, working in a borderless environment with laws of multiple jurisdictions, and implementing information security practices and raising awareness.

Public and private entities are working to address these challenges by expanding public/private partnerships to increase the trust between entities, to improve the quality and quantity of shared information, and to leverage resources and technologies across public and private boundaries. In addition, law enforcement organizations have formed task forces and international agreements to foster working in a borderless environment with laws from multiple jurisdictions. Continued expansion of these efforts is essential. Additionally, more can be done to assure an adequate pool of individuals with the skills needed to effectively combat cybercrime. Although law enforcement agencies must be sensitive to a number of organizational issues and objectives in their human capital programs, current staff rotation policies at key law enforcement agencies may negatively impact the agencies' analytical and technical capabilities to combat cybercrime.

Recommendation for Executive Action

We recommend that the Attorney General direct the FBI Director and the Secretary of Homeland Security direct the Director of the Secret Service to assess the impact of the current rotation approach on their respective law enforcement analytical and technical capabilities to investigate and prosecute cybercrime and to modify their approaches, as appropriate.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from the FBI (see app. II). In the response, the Deputy Assistant Director from the FBI's Cyber Division stated that the FBI Director had approved rotational policies after careful consideration of the viable alternatives provided by analysis and study conducted by the Human Resources Division. Further, he stated that the FBI Director had endorsed the establishment of five

distinct career paths for both new and veteran special agents, including a specific designation for cyber matters. According to the Assistant Director, this career path will ensure the FBI recruits, trains, and deploys special agents with the critical cyber skill set required to maintain the FBI on the cutting edge of computer technology and development, and positioned to counter the constantly evolving cyber threat. Despite these efforts to assess and expand analytical and technical capabilities, the current rotational policies may adversely affect the FBI's use of staff with cyber expertise; therefore, it is important to continually reassess the rotational policies that impact the FBI's ability to address the cyber threat.

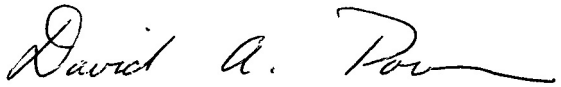
In addition, we received written comments on a draft of this report from the Secret Service (see app. III). In the response, the Assistant Director, Office of Inspection, stated that agents who complete the Electronic Crimes Special Agent Program's computer forensics training course are required to serve a minimum of four years in the program. In addition, he stated that the Secret Service is expanding its Electronic Crimes Special Agent Program and will have approximately 770 trained and active agents by the end of fiscal year 2007. He also stated that the rotation of the Electronic Crimes Special Agent Program agents does not have a detrimental impact on the agency's cyber investigative capabilities because Secret Service field offices send additional agents through the program prior to a trained agent's departure, and because the Electronic Crimes Task Forces allow the agency to draw on state and local law officials trained in cyber investigations and computer forensics. While we agree that expanding the Electronic Crimes Special Agent Program and leveraging the relationships and capabilities of the Electronic Crimes Task Forces is important to adequately addressing cybercrime, the current rotational policy may adversely affect the Secret Service's use of staff with cyber expertise; therefore, it is important for the Secret Service to continually reassess the rotational policies that impact its ability to address the cyber threat.

DOD, DOJ, DHS, state and local government, and other officials also provided technical corrections that have been incorporated in this report as appropriate.

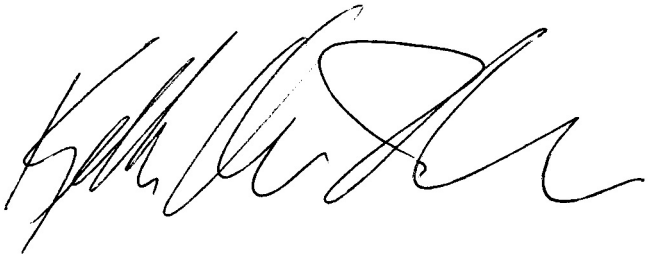
As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to interested congressional committees, the Attorney General, the Secretaries of Defense and Homeland Security, the Chairman of the Federal Trade

Commission, and other interested parties. We also will make copies available to others upon request. In addition, this report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you or your staff has any questions about this report, please contact David Powner at (202) 512-9286, or pownerd@gao.gov; or Keith Rhodes at (202) 512-6412, or rhodesk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Major contributors to this report are listed in appendix IV.



David A. Powner
Director, Information Technology Management Issues



Keith A. Rhodes
Chief Technologist
Director, Center for Technology and Engineering

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) determine the impact of cybercrime on our nation's economy and security; (2) describe key federal entities, as well as nonfederal and private-sector entities, responsible for addressing cybercrime; and (3) determine challenges being faced in addressing cybercrime.

To determine the impact of cybercrime on the U.S. economy and security, we analyzed various government and private-sector reports, surveys, and statistics related to cybercrime and conducted interviews with experts from law enforcement, academia, and information technology and security companies to verify, clarify, and gain a greater understanding of cybercrime's impact. Further, we interviewed officials and staff at key federal agencies, including the Departments of Defense, Justice, and Homeland Security; and the Federal Trade Commission; and obtained, through structured interview questions, information from 19 federal Office of Inspectors General about the number and frequency of cybercrimes experienced at their respective agencies and the subsequent cost associated with addressing these incidents, among other things.

To identify the key public and private-sector entities that work to mitigate and investigate computer crime and prosecute cyber criminals, we analyzed reports, surveys, and studies related to cybercrime. In addition, we held interviews with cybercrime experts from government and the private sector to identify entities and verify the entities identified as being important. To verify information and determine relevant activities, we performed document analysis, held site visits, conducted structured interviews, and received written responses to structured interview questions. The entities contacted during the course of our work include the following:

- *Department of Justice:* Computer Crime and Intellectual Property Section; Bureau of Justice Statistics; United States Attorneys, including the Pittsburgh and Seattle Computer Hacking and Intellectual Property units; FBI's Cyber Division, including the Computer Intrusion Section and the Innocent Images National Initiative unit; FBI's National Cyber Forensics and Training Alliance; FBI's Cyber Initiative and Resource Fusion Unit; FBI's Internet Crime Complaint Center; and FBI's Pittsburgh and Seattle Field Office units.

- *Department of Homeland Security:* Special Agent in Charge of the Secret Service's Criminal Investigative Division; the National Cyber Security Division's Deputy Director of the Law Enforcement and Intelligence

Section and Deputy Director of the United States Computer Emergency Readiness Center.

- *Department of Defense:* Defense Cyber Crime Center; Joint Task Force for Global Network Operations; Defense Criminal Investigative Service; Air Force Office of Special Investigation, Army Military Intelligence, and the Naval Criminal Investigative Service.

- *Federal Trade Commission:* Officials from the Divisions of Advertising Practices, Enforcement, and Marketing Practices. In addition, members of the team attended sessions of a Federal Trade Commission sponsored conference that focused attention on cybercrime.

- *Office of Inspectors General:* Department of Education's Computer Crime Division/Office of Inspector General; written responses from structured interview questions from officials from the Inspectors General of the Small Business Administration, Department of Defense, Nuclear Regulatory Commission, Health and Human Services, National Science Foundation, Department of Veterans Affairs, General Services Administration, Department of Labor, Department of Transportation, Agency for International Development, Office of Personnel Management, Department of the Treasury, Department of Justice, Housing and Urban Development, Social Security Administration, Department of Energy, Department of the Interior.

- *Private Sector:* Counterpane Internet Security; Cyber Security Industry Alliance; CypherTrust; Guidance Software; InfraGard; Information Technology-Information Sharing and Analysis Center; Microsoft; Postini; SEARCH; Symantec; and other cybercrime experts.

- *State and Local Entities:* Office of the Attorney General of Washington; Washington State Highway Patrol's Computer Crime Unit; Office of the Attorney General of Virginia—Computer Crime Unit; and the National Association of Attorneys General.

We also met with representatives from the State Department to discuss the department's role in addressing cybercrime. However, after meeting with representatives from the department's Bureau of Resource Management, Political-Military Affairs, International Narcotics and Law Enforcement, and others, we determined that the department's cybercrime responsibilities were outside the scope of our engagement. In addition, State Department representatives stated that they work closely with the Department of Justice's Computer Crime and Intellectual Property Section on cybercrime issues and that Justice officials would be a better source to

determine the impact of cybercrime on the United States and international efforts to address cybercrime.

To determine the challenges being faced in addressing cybercrime, we gathered and analyzed relevant documents, interviewed key government and private-sector officials regarding challenges to fighting cybercrime, and conducted Internet and media research. Based on the information received and our knowledge of the issues, we determined the major challenges impeding efforts to address cybercrime.

To observe operations of cybercrime related entities and interview relevant federal, state, and local government and private-sector officials, we performed our work between June 2006 and May 2007 in the Washington, D.C., metropolitan area; Pittsburgh, Pennsylvania; Seattle, Washington; and Fairmont, West Virginia; in accordance with generally accepted government auditing standards.

Appendix II: Comments from the Federal Bureau of Investigation

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

June 13, 2007

Mr. David A. Powner
Director
Information Technology
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: GAO 07-705

Dear Mr. Powner:

Thank you for the opportunity to review the Government Accountability Office (GAO) draft report entitled "Cybercrime - Public and Private Entities Face Challenges in Addressing Cyber Threats." The draft report has been reviewed by the Federal Bureau of Investigations's (FBI) Cyber Division (CyD) and the Human Resource Division (HRD). This letter constitutes the formal FBI comments to the draft report and it is requested that it be included in GAO's final report.

I have reviewed your recommendation concerning the assessment of the impact of the current rotation policies affecting both newly hired Special Agents (SA) and senior field Supervisory Special Agents. The FBI Director, Robert S. Mueller III, has approved rotational policies in these matters after careful consideration of the viable alternatives provided by analysis and study conducted by the HRD. Further, the Director has endorsed the establishment of five distinct career paths for both new and veteran SAs, including a specific designation for cyber matters. This career path will ensure the FBI recruits, trains, and deploys SAs with the critical cyber skill set required to maintain the FBI on the cutting edge of computer technology and development, and positioned to counter the constantly evolving cyber threat.

Mr. David A. Powner

Thank you for the opportunity to comment on your report.

Sincerely yours,

Shawn Henry
Deputy Assistant Director
Cyber Division

Appendix III: Comments from the U.S. Secret Service

U.S. Department of Homeland Security
UNITED STATES SECRET SERVICE
Washington, D.C. 20223

June 8, 2007

MEMORANDUM FOR NORMAN J. RABKIN
MANAGING DIRECTOR
HOMELAND SECURITY AND JUSTICE
U.S. GOVERNMENT ACCOUNTABILITY OFFICE

FROM: George D. Rogers
Assistant Director
Office of Inspection
U.S. Secret Service

SUBJECT: Cybercrime (Job Code 310820)

The U.S. Secret Service is transmitting its response to the recommendation included in the Government Accountability Office draft report entitled, "Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats (GAO-07-705)."

GAO Recommendation

Recommendation that the Attorney General direct the FBI Director and the Secretary of Homeland Security direct the Director of the U.S. Secret Service to assess the impact of the current rotation approach on their respective law enforcement analytical and technical capabilities to investigate and prosecute cybercrime, and to modify their approaches as appropriate.

Response

The Secret Service trains agents in cyber investigations through our Electronic Crimes Special Agent Program (ECSAP). Agents who complete the computer forensics training course are required to serve a minimum of four years in this program. The Secret Service is currently expanding the ECSAP program. By the end of FY 2007, we will have approximately 770 trained and active ECSAP agents assigned to Secret Service offices throughout the world.

While ECSAP agents may rotate to a different type of assignment after serving their four year requirement, this does not have a detrimental impact on our cyber investigative capabilities. In most instances, field offices send additional agents through ECSAP training prior to a trained agent's departure. As part of the Computer Security Protection Initiative ECSAP agents assigned to protective details continue to use their skills. Each ECSAP agent must undergo a yearly recertification. As the ECSAP program expands, the Secret Service will have multiple ECSAP agents assigned to each office.

Additionally, the Secret Service maintains 24 Electronic Crimes Task Forces located in metropolitan regions across the country. These task forces combine the resources of state and local police, as well as academia and private industry. The Secret Service trains state and local law enforcement officers in cyber investigations and computer forensics through the Electronic Crimes State and Local Program (ECSLP). These state and local law enforcement officers are often assigned to their regional Secret Service task force. In this manner, the task force model allows the Secret Service to maintain investigative capabilities even as personnel rotate to other protective or investigative assignments.

I appreciate your interest in the U.S. Secret Service. If I may be of further assistance, please contact the Office of Inspection at 202/406-5766.

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

David A. Powner, (202) 512-9286, or pownerd@gao.gov
Keith A. Rhodes, (202) 512-6412, or rhodesk@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Barbara Collier, Neil Doherty, Michael Gilmore, Steve Gosewehr, Barbarol James, Kenneth A. Johnson, Kush K. Malhotra, Amos Tevelow, and Eric Winter made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548