United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Thursday, June 28, 2012

INFORMATION SECURITY

Cyber Threats Facilitate Ability to Commit Economic Espionage

Statement of Gregory C. Wilshusen, Director
Information Security Issues

June 28, 2012

INFORMATION SECURITY

Cyber Threats Facilitate Ability to Commit Economic Espionage

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-876T, a testimony before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The threat of economic espionage—the theft of U.S. proprietary information, intellectual property (IP), or technology by foreign companies, governments, or other actors—has grown. Moreover, dependence on networked information technology (IT) systems has increased the reach and potential impact of this threat by making it possible for hostile actors to quickly steal massive amounts of information while remaining anonymous and difficult to detect. To address this threat, federal agencies have a key role to play in law enforcement, deterrence, and information sharing. Consistent with this threat, GAO has designated federal information security as a governmentwide high-risk area since 1997 and in 2003 expanded it to include protecting systems and assets vital to the nation (referred to as critical infrastructures). GAO was asked to testify on the cyber aspects of economic espionage. Accordingly, this statement discusses (1) cyber threats facing the nation's systems, (2) reported cyber incidents and their impacts, (3) security controls and other techniques available for reducing risk, and (4) the responsibilities of key federal entities in support of protecting IP. To do this, GAO relied on previously published work in this area, as well as reviews of reports from other federal agencies, media reports, and other publicly available sources.

What GAO Recommends

In prior reports, GAO has made hundreds of recommendations to better protect federal systems, critical infrastructures, and intellectual property.

View GAO-12-876T. For more information, contact Gregory C. Wilshusen (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The nation faces an evolving array of cyber-based threats arising from a variety of sources. These sources include criminal groups, hackers, terrorists, organization insiders, and foreign nations engaged in crime, political activism, or espionage and information warfare. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. Moreover, potential threat actors have a variety of attack techniques at their disposal, which can adversely affect an organization's computers or networks and be used to intercept or steal valuable information. The magnitude of the threat is compounded by the ever-increasing sophistication of cyber attack techniques, such as attacks that may combine multiple techniques. Using these techniques, threat actors may target individuals and businesses, resulting in, among other things, loss of sensitive personal or proprietary information.

These concerns are highlighted by reports of cyber incidents that have had serious effects on consumers and businesses. These include the compromise of individuals' sensitive personal data such as credit- and debit-card information and the theft of businesses' IP and other proprietary information. While difficult to quantify monetarily, the loss of such information can result in identity theft; lower-quality counterfeit goods; lost sales or brand value to businesses; and lower overall economic growth and declining international trade.

To protect against these threats, a variety of security controls and other techniques are available. These include technical controls such as those that manage access to systems, ensure system integrity, and encrypt sensitive data. But they also include risk management and strategic planning that organizations undertake to improve their overall security posture and reduce their exposure to risk. Further, effective public-private partnerships are a key element for, among other things, sharing information about threats.

Multiple federal agencies undertake a wide range of activities in support of IP rights. Some of these agencies include the Departments of Commerce, Justice, and Homeland Security, among others. For example, components within the Justice Department and the Federal Bureau of Investigation are dedicated to fighting computer-based threats to IP. In addition, both Congress and the Administration have established interagency mechanisms for better coordinating the protection of IP. Ensuring effective coordination will be critical for better protecting the economic security of America's businesses.

Chairman Meehan, Ranking Member Higgins, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's hearing on the threat of economic espionage facing U.S. businesses.

The threat of economic espionage[1] is not new. In April 1992, we testified that the theft of U.S. proprietary information or technology by foreign companies has long been a part of the competitive business environment.[2] We also testified that the unauthorized acquisition of U.S. proprietary or other information by foreign governments to advance their countries' economic position was growing.

Today, this threat continues to grow. According to the Federal Bureau of Investigation (FBI), the theft of intellectual property (IP)[3]—products of human intelligence and creativity—is a growing threat which is heightened by the rise of the use of digital technologies.[4] The increasing dependency upon information technology (IT) systems and networked operations pervades nearly every aspect of our society. In particular, increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While bringing significant benefits, this dependency can also create

[1]According to the Office of the National Counterintelligence Executive, economic espionage occurs when an actor, knowing or intending that his or her actions will benefit any foreign government, instrumentality or agent, knowingly: (1) steals, or without authorization appropriates, carries away, conceals, or obtains by deception or fraud a trade secret; (2) copies, duplicates, reproduces, destroys, uploads, downloads, or transmits that trade secret without authorization; or (3) receives a trade secret knowing that the trade secret had been stolen, appropriated, obtained or converted without authorization. See *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011* (October 2011).

[2]GAO, *Economic Espionage: The Threat to U.S. Industry*, Testimony before the Subcommittee on Economic and Commercial Law, Committee on the Judiciary, House of Representatives, GAO/T-OSI-92-6 (April 29, 1992).

[3]Intellectual property is a category of legal rights that grants owners certain exclusive rights to intangible assets or products of the human intellect, such as inventions; literary and artistic works; and symbols, names, images, and design.

[4]See the FBI's website on cybercrime and intellectual property theft at http://www.fbi.gov/about-us/investigate/cyber/ipr/ipr.

vulnerabilities to cyber-based threats. Cyber attacks are one way that threat actors—whether nations, companies, or criminals—can target the intellectual property and other sensitive information of federal agencies and American businesses. According to the Office of the National Counterintelligence Executive, sensitive U.S. economic information and technology are targeted by intelligence services, private sector companies, academic and research institutions, and citizens of dozens of countries.[5] To help address this threat, federal agencies have a key role to play in law enforcement, deterrence, and information sharing. Underscoring the importance of this issue, we have designated federal information security as a high-risk area since 1997 and in 2003 expanded this area to include protecting computerized systems supporting our nation's critical infrastructure.[6]

In my testimony today, I will describe (1) cyber threats facing the nation's systems, (2) reported cyber incidents and their impacts, (3) security controls and other techniques available for reducing risk, and (4) the responsibilities of key federal entities in support of improving the protection of intellectual property. In preparing this statement in June 2012, we relied on our previous work in these areas. (Please see the related GAO products in appendix II.) These products contain detailed overviews of the scope and methodology we used. We also reviewed relevant reports from the Department of Justice and Office of the National Counterintelligence Executive, and information on security incidents, including those involving economic espionage, from the U.S. Computer Emergency Readiness Team (US-CERT), media reports, and other publicly available sources. The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

[5]Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace.*

[6]See, most recently, GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

Background

As computer technology has advanced, both government and private entities have become increasingly dependent on computerized information systems to carry out operations and to process, maintain, and report essential information. Public and private organizations rely on computer systems to transmit sensitive and proprietary information, develop and maintain intellectual capital, conduct operations, process business transactions, transfer funds, and deliver services. In addition, the Internet has grown increasingly important to American business and consumers, serving as a medium for hundreds of billions of dollars of commerce each year.

Consequently, ineffective information security controls can result in significant risks, including

- loss or theft of resources, including money and intellectual property;
- inappropriate access to and disclosure, modification, or destruction of sensitive information;
- use of computer resources for unauthorized purposes or to launch attacks on other computers systems;
- damage to networks and equipment;
- loss of business due to lack of customer confidence; and
- increased costs from remediation.

The Nation Faces an Evolving Array of Cyber-Based Threats

Cyber-based threats are evolving and growing and arise from a wide array of sources. These sources include business competitors, corrupt employees, criminal groups, hackers, and foreign nations engaged in espionage and information warfare. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. Table 1 shows common sources of cyber threats.

Table 1: Sources of Cybersecurity Threats

Threat source	Description
Bot-network operators	Bot-net operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks).
Business competitors	Companies that compete against or does business with a target company may seek to obtain sensitive information to improve their competitive advantage in various areas, such as pricing, manufacturing, product development, and contracting.

Threat source	Description
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft, online fraud, and computer extortion.
Hackers	Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking, monetary gain, and political activism, among other reasons. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled or corrupt organization insider is a source of computer crime including economic espionage. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
International corporate spies	International corporate spies pose a threat to the United States through their ability to conduct economic and industrial espionage[a] and large-scale monetary theft and to hire or develop hacker talent.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities, including economic espionage directed against U.S businesses. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. In his January 2012 testimony, the Director of National Intelligence stated that, among state actors, China and Russia are of particular concern.
Phishers	Individuals or small groups execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware or malware to accomplish their objectives.
Spammers	Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (e.g., a denial of service).
Spyware or malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several notable destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, National Institute of Standards and Technology, and the Software Engineering Institute's CERT® Coordination Center.

[a]According to the Office of the National Counterintelligence Executive, industrial espionage, or theft of trade secrets, occurs when an actor, intending or knowing that his or her offense will injure the owner of a trade secret of a product produced for or placed in interstate or foreign commerce, acts with the intent to convert that trade secret to the economic benefit of anyone other than the owner. See Foreign Spies Stealing U.S. Economic Secrets in Cyberspace.

These sources of cyber threats make use of various techniques, or exploits, to adversely affect an organization's computers, software, or networks, or to intercept or steal valuable or sensitive information. Table 2 provides descriptions of common types of cyber exploits.

Table 2: Types of Cyber Exploits

Type of exploit	Description
Cross-site scripting	An attack that uses third-party web resources to run script within the victim's web browser or scriptable application. This occurs when a browser visits a malicious website or clicks a malicious link. The most dangerous consequences occur when this method is used to exploit additional vulnerabilities that may permit an attacker to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, and remotely access and control the victim's machine.
Denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial-of-service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Logic bombs	A piece of programming code intentionally inserted into a software system that will cause a malicious function to occur when one or more specified conditions are met.
Phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
Structured Query Language (SQL) injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a useful program that a user would likely execute.
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer– sometimes with a powerful antenna–searching for unsecured wireless networks.
Worm	A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread itself. Unlike computer viruses, worms do not require human involvement to propagate.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed timeframe between public discoveries of both makes it difficult to defend against.

Source: GAO analysis of data from the National Institute of Standards and Technology, United States Computer Emergency Readiness Team, and industry reports.

Cyberspace—where much business activity and the development of new ideas often take place—amplifies these threats by making it possible for malicious actors to quickly steal and transfer massive quantities of data while remaining anonymous and difficult to detect.[7] For example, cyber attackers do not need to be physically close to their victims, technology allows attacks to easily cross state and national borders, attacks can be carried out at high speed and directed at a number of victims simultaneously, and cyber attackers can more easily remain anonymous. Moreover, the use of these and other techniques is becoming more sophisticated, with attackers using multiple or "blended" approaches that combine two or more techniques. Using such techniques, threat actors may target individuals, resulting in loss of privacy or identity theft; businesses, resulting in the compromise of proprietary information or intellectual property; critical infrastructures, resulting in their disruption or destruction; or government agencies, resulting in the loss of sensitive information and damage to economic and national security.

Reported Cyber-Incidents Illustrate Serious Risk to the Security of Intellectual Property and Other Sensitive Economic Information

Reports of cyber incidents affecting both public and private institutions are widespread. The U.S. Computer Emergency Readiness Team (US-CERT) receives computer security incident reports from federal agencies, state and local governments, commercial enterprises, U.S. citizens, and international computer security incident response teams. In its fiscal year 2011 report to Congress on implementation of the Federal Information Security Management Act of 2002, the Office of Management and Budget reported that US-CERT received over 100,000 total incident reports in fiscal year 2011. Over half of these (about 55,000) were phishing exploits; other categories of incidents included virus/Trojan horse/worm/logic bombs; malicious websites; policy violations; equipment theft or loss; suspicious network activity; attempted access; and social engineering.

Private sector organizations have experienced a wide range of incidents involving data loss or theft, economic loss, computer intrusions, and privacy breaches, underscoring the need for improved security practices. The following examples from news media and other public sources illustrate that a broad array of information and assets remain at risk.

[7]Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace*.

- In March 2012, it was reported that a security breach at Global Payments, a firm that processed payments for Visa and Mastercard, could compromise the credit- and debit-card information of millions of Americans. Subsequent to the reported breach, the company's stock fell more than 9 percent before trading in its stock was halted. Visa also removed the company from its list of approved processors.
- In March 2012, it was reported that Blue Cross Blue Shield of Tennessee paid out a settlement of $1.5 million to the U.S. Department of Health and Human Services arising from potential violations stemming from the theft of 57 unencrypted computer hard drives that contained protected health information of over 1 million individuals.
- In April 2011, Sony disclosed that it suffered a massive breach in its video game online network that led to the theft of personal information, including the names, addresses, and possibly credit card data belonging to 77 million user accounts.
- In February 2011, media reports stated that computer hackers had broken into and stolen proprietary information worth millions of dollars from the networks of six U.S. and European energy companies.
- A retailer reported in May 2011 that it had suffered a breach of its customers' card data. The company discovered tampering with the personal identification number (PIN) pads at its checkout lanes in stores across 20 states.
- In mid-2009 a research chemist with DuPont Corporation reportedly downloaded proprietary information to a personal e-mail account and thumb drive with the intention of transferring this information to Peking University in China and also sought Chinese government funding to commercialize research related to the information he had stolen.
- Between 2008 and 2009, a chemist with Valspar Corporation reportedly used access to an internal computer network to download secret formulas for paints and coatings, reportedly intending to take this proprietary information to a new job with a paint company in Shanghai, China.
- In December 2006, a product engineer with Ford Motor Company reportedly copied approximately 4,000 Ford documents onto an external hard drive in order to acquire a job with a Chinese automotive company.

These incidents illustrate the serious impact that cyber threats can have on, among other things, the security of sensitive personal and financial information and proprietary information and intellectual property. While these effects can be difficult to quantify monetarily, they can include any of the following:

- For consumers or private citizens: identity theft or compromise of personal and economic information and costs associated with lower-quality counterfeit or pirated goods.
- For business: lost sales, lost brand value or damage to public image, cost of intellectual property protection, and decreased incentive to invest in research and development.
- For the economy as a whole: lower economic growth due to reduced incentives to innovate and lost revenue from declining U.S. trade with countries that have weak IP rights regimes.

Security Controls and Other Techniques Can Reduce Vulnerability to Cyber-Based Attacks

The prevalence of cyber threats and the risks they pose illustrate the need for security controls and other actions that can reduce organizations' vulnerability to such attacks. As we have reported, there are a number of cybersecurity technologies that can be used to better protect systems from cyber attacks, including access control technologies, system integrity technologies, cryptography, audit and monitoring tools, and configuration management and assurance technologies.[8] In prior reports, we have made hundreds of recommendations to federal agencies to better protect their systems and cyber-reliant critical infrastructures. Table 3 summarizes some of the common cybersecurity technologies, categorized by the type of security control they help to implement.

Table 3: Common Cybersecurity Technologies

Category	Technology	What it does
Access control		
Boundary protection	Firewalls	Control access to and from a network or computer.
Authentication	Biometrics	Uses human characteristics, such as fingerprints, irises, and voices, to establish the identity of the user.
Authorization	User rights and privileges	Allow or prevent access to data and systems and actions of users based on the established policies of an organization.
System integrity	Antivirus software	Provides protection against malicious code, such as viruses, worms, and Trojan horses.

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

Category	Technology	What it does
Cryptography	Digital signatures and certificates	Use public key cryptography to provide (1) assurance that both the sender and recipient of a message or transaction will be uniquely identified, (2) assurance that the data have not been accidentally or deliberately altered, and (3) verifiable proof of the integrity and origin of the data.
	Virtual private networks	Allow organizations or individuals in two or more physical locations to establish network connections over a shared or public network, such as the Internet, with functionality that is similar to that of a private network using cryptography.
Audit and monitoring	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.
	Computer forensics tools	Identify, preserve, extract, and document computer-based evidence.
Configuration management and assurance	Policy enforcement applications	Enable system administrators to engage in centralized monitoring and enforcement of an organization's security policies.
	Network management	Allow for the control and monitoring of networks, including management of faults, configurations, performance, and security.
	Scanners	Analyze computers or networks for security vulnerabilities.
	Continuity of operations tools	Provide a complete backup infrastructure to maintain availability in the event of an emergency or during planned maintenance.
	Patch management	Acquires, tests, and applies multiple patches to one or more computer systems.

Source: GAO analysis.

In addition, the use of an overall cybersecurity framework can assist in the selection of technologies to protect an organization against cyber attacks. Such a framework includes

- determining the business requirements for security;
- performing risk assessments;
- establishing a security policy;
- implementing a cybersecurity solution that includes people, process, and technology to mitigate identified security risks; and
- continuously monitoring and managing security.

Risk assessments, which are central to this framework, help organizations determine which assets are most at risk and to identify

countermeasures to mitigate those risks. Risk assessment is based on a consideration of threats and vulnerabilities that could be exploited to inflict damage.

Even with such a framework, there often are competing demands for cybersecurity investments. For example, for some companies, mitigating physical risks may be more important than mitigating cyber risks. Further, investing in cybersecurity technologies needs to make business sense. It is also important to bear in mind the limitations of some cybersecurity technologies and to be aware that their capabilities should not be overstated. Technologies do not work in isolation. Cybersecurity solutions make use of people, process, and technology. Cybersecurity technology must work within an overall security process and be used by trained personnel. We have also emphasized the importance of public-private partnerships for sharing information and implementing effective cybercrime prevention strategies.[9]

Similarly, the Office of the National Counterintelligence Executive has identified a series of "best practices in data protection strategies and due diligence for corporations."[10] These include developing an information strategy; insider threat programs and awareness; effective data management; network security, auditing, and monitoring; and contingency planning.

Key Federal Agencies Have Responsibilities for Protecting Intellectual Property

Multiple federal agencies undertake a wide range of activities in support of IP rights. Some of these agencies are the Departments of Commerce (including the U.S. Patent and Trademark Office), State, Justice (including the FBI), Health and Human Services, and Homeland Security; the U.S. Trade Representative; the U.S. Copyright Office; and the U.S. International Trade Commission. In many cases, IP-related efforts represent a small part of the agencies' much broader missions.

A smaller number of agencies and their components are involved in investigating IP violations and enforcing U.S. IP laws. For example, the

[9]GAO, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07-705 (Washington, D.C.: June 22, 2007).

[10]Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace*.

Department of Justice's (DOJ) U.S. attorneys offices, Criminal Division, and the FBI investigate and prosecute federal IP crimes. DOJ established the Computer Hacking and Intellectual Property program, which consists of specially trained assistant U.S. attorneys to pursue IP cases. Each of the 93 U.S. attorneys offices throughout the country have assistant U.S. attorneys designated as Computer Hacking and Intellectual Property coordinators, who are available to work on IP cases. In addition, DOJ has created Computer Hacking and Intellectual Property units in 25 U.S. attorney's offices with histories of large IP case loads. DOJ's Computer Crime and Intellectual Property Section—based in Washington, D.C.—consists of prosecutors devoted to enforcing computer crime and IP laws. Computer Crime and Intellectual Property Section attorneys prosecute cases, assist prosecutors and other investigative agents in the field, and help develop and implement an overall criminal enforcement strategy. The FBI's Cyber Division oversees the bureau's IP enforcement efforts; though not all of its IP investigations are cyber-related.

Over the years, Congress and the administration have created interagency mechanisms to coordinate federal IP law enforcement efforts. These include the National Intellectual Property Law Enforcement Coordination Council (NIPLECC), created in 1999 to coordinate U.S. law enforcement efforts to protect and enforce IP rights in the United States and abroad and the Strategy for Targeting Organized Piracy initiative, created by the President in 2004 to target cross-border trade in tangible goods and strengthen U.S. government and industry IP enforcement action. In December 2004, Congress passed legislation to enhance NIPLECC's mandate and created the position of the Coordinator for International Intellectual Property Enforcement, located within the Department of Commerce, to lead NIPLECC. In November 2006 we reported that NIPLECC continued to face persistent difficulties, creating doubts about its ability to carry out its mandate.[11] We also noted that while the Strategy for Targeting Organized Piracy had brought attention and energy to IP efforts within the U.S. government, it had limited usefulness as a tool to prioritize, guide, implement, and monitor the combined efforts of multiple agencies.

[11]GAO, *Intellectual Property: Strategy for Targeting Organized Piracy (STOP) Requires Changes for Long-term Success,* GAO-07-74 (Washington, D.C.: Nov. 8, 2006).

In 2008, Congress passed the Prioritizing Resources and Organization for Intellectual Property Act (PRO-IP Act), which, among other things, created the position of the Intellectual Property Enforcement Coordinator (IPEC) to serve within the Executive Office of the President. The duties of the coordinator outlined in the act include specific efforts to enhance interagency coordination, such as the development of a comprehensive joint strategic plan. The act also required the Attorney General to devote additional resources to IP enforcement and undertake other IP-enforcement-related efforts. In October 2010, we noted that DOJ and FBI officials and Office of the IPEC staff reported taking many actions to implement the requirements of the PRO-IP Act.[12] Moreover, the IPEC coordinated with other federal entities to deliver the 2010 Joint Strategic Plan on Intellectual Property Enforcement to Congress and the public. We reported that the plan addressed the content requirements of the act, but that enhancements were needed, such as identifying responsible departments and entities for all action items and estimates of resources needed to carry out the plan's priorities. Accordingly, we recommended that the IPEC take steps to ensure that future strategic plans address these elements. IPEC staff generally concurred with our findings and recommendations.

In summary, the ongoing efforts to steal U.S. companies' intellectual property and other sensitive information are exacerbated by the ever-increasing prevalence and sophistication of cyber-threats facing the nation. Recently reported incidents show that such actions can have serious impact not only on individual businesses, but on private citizens and the economy as a whole. While techniques exist to reduce vulnerabilities to cyber-based threats, these require strategic planning by affected entities. Moreover, effective coordination among federal agencies responsible for protecting IP and defending against cyber-threats, as well as effective public-private partnerships, are essential elements of any nationwide effort to protect America's businesses and economic security.

[12]GAO, *Intellectual Property: Agencies Progress in Implementing Recent Legislation, but Enhancements Could Improve Future Plans*, GAO-11-39 (Washington, D.C.: Oct. 13, 2010).

Chairman Meehan, Ranking Member Higgins, and Members of the Subcommittee, this concludes my statement. I would be happy to answer any questions you have at this time.

Appendix I: Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this statement include Michael Gilmore and Anjalique Lawrence (Assistant Directors), Bradley Becker, Kush Malhotra, and Lee A. McCracken.

Appendix II: Related GAO Products

Cybersecurity: Threats Impacting the Nation. GAO-12-666T. Washington, D.C.: April 24, 2012

IT Supply Chain: National Security-Related Agencies Need to Better Address Risks. GAO-12-361. Washington, D.C.: March 23, 2012.

Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use. GAO-12-92. Washington, D.C.: December 9, 2011.

Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure. GAO-11-865T. Washington, D.C.: July 26, 2011.

High-Risk Series: An Update. GAO-11-278. Washington, D.C.: February 2011.

Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed. GAO-11-117. Washington, D.C.: January 12, 2011.

Intellectual Property: Agencies Progress in Implementing Recent Legislation, but Enhancements Could Improve Future Plans. GAO-11-39. Washington, D.C.: October 13, 2010.

Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed. GAO-10-628. Washington, D.C.: July 15, 2010.

Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance. GAO-10-606. Washington, D.C.: July 2, 2010.

Cybersecurity: Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats. GAO-10-834T. Washington, D.C.: June 16, 2010.

Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods. GAO-10-423. Washington, D.C.: April 12, 2010.

Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative. GAO-10-338. Washington, D.C.: March 5, 2010.

Intellectual Property: Enhancements to Coordinating U.S. Enforcement Efforts. GAO-10-219T. Washington, D.C.: December 9, 2009.

National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture. GAO-09-432T. Washington, D.C.: March 10, 2009.

Intellectual Property: Federal Enforcement Has Generally Increased, but Assessing Performance Could Strengthen Law Enforcement Efforts. GAO-08-157. Washington, D.C.: March 11, 2008.

Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats. GAO-07-705. Washington, D.C.: June 22, 2007.

Intellectual Property: Strategy for Targeting Organized Piracy (STOP) Requires Changes for Long-term Success. GAO-07-74. Washington, D.C.: November. 8, 2006.