

May 2005

CRITICAL
INFRASTRUCTURE
PROTECTION

Department of
Homeland Security
Faces Challenges in
Fulfilling
Cybersecurity
Responsibilities



G A O

Accountability * Integrity * Reliability



Highlights of [GAO-05-434](#), a report to congressional requesters

CRITICAL INFRASTRUCTURE PROTECTION

Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities

Why GAO Did This Study

Increasing 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, this widespread interconnectivity also poses significant risks to our nation's computer systems and, more importantly, to the critical operations and infrastructures they support. The Homeland Security Act of 2002 and federal policy established DHS as the focal point for coordinating activities to protect the computer systems that support our nation's critical infrastructures. GAO was asked to determine (1) DHS's roles and responsibilities for cyber critical infrastructure protection, (2) the status and adequacy of DHS's efforts to fulfill these responsibilities, and (3) the challenges DHS faces in fulfilling its cybersecurity responsibilities.

What GAO Recommends

GAO is making recommendations to the Secretary of Homeland Security to strengthen the department's ability to implement key cybersecurity responsibilities by completing critical activities and resolving underlying challenges. In written comments on a draft of this report, DHS agreed with our recommendation to engage stakeholders to prioritize its responsibilities, but disagreed with and sought clarification on recommendations to resolve its challenges.

www.gao.gov/cgi-bin/gettrpt?GAO-05-434.

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

What GAO Found

As the focal point for critical infrastructure protection (CIP), the Department of Homeland Security (DHS) has many cybersecurity-related roles and responsibilities that we identified in law and policy (see table below for 13 key responsibilities). DHS established the National Cyber Security Division to take the lead in addressing the cybersecurity of critical infrastructures.

While DHS has initiated multiple efforts to fulfill its responsibilities, it has not fully addressed any of the 13 responsibilities, and much work remains ahead. For example, the department established the United States Computer Emergency Readiness Team as a public/private partnership to make cybersecurity a coordinated national effort, and it established forums to build greater trust and information sharing among federal officials with information security responsibilities and law enforcement entities. However, DHS has not yet developed national cyber threat and vulnerability assessments or government/industry contingency recovery plans for cybersecurity, including a plan for recovering key Internet functions.

DHS faces a number of challenges that have impeded its ability to fulfill its cyber CIP responsibilities. These key challenges include achieving organizational stability, gaining organizational authority, overcoming hiring and contracting issues, increasing awareness about cybersecurity roles and capabilities, establishing effective partnerships with stakeholders, achieving two-way information sharing with these stakeholders, and demonstrating the value DHS can provide. In its strategic plan for cybersecurity, DHS identifies steps that can begin to address the challenges. However, until it confronts and resolves these underlying challenges and implements its plans, DHS will have difficulty achieving significant results in strengthening the cybersecurity of our critical infrastructures.

DHS's Key Cybersecurity Responsibilities

<ul style="list-style-type: none"> • Develop a national plan for critical infrastructure protection, including cybersecurity. • Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector. • Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities. • Develop and enhance national cyber analysis and warning capabilities. • Provide and coordinate incident response and recovery planning efforts. 	<ul style="list-style-type: none"> • Identify and assess cyber threats and vulnerabilities. • Support efforts to reduce cyber threats and vulnerabilities. • Promote and support research and development efforts to strengthen cyberspace security. • Promote awareness and outreach. • Foster training and certification. • Enhance federal, state, and local government cybersecurity. • Strengthen international cyberspace security. • Integrate cybersecurity with national security.
--	---

Source: GAO analysis of law and policy.

Contents

Letter

Results in Brief	1
Background	2
DHS's Roles and Responsibilities for Cybersecurity in Support of Critical Infrastructure Protection Are Many and Varied	4
DHS Has Initiated Efforts That Begin to Address Its Responsibilities, but More Work Remains	18
DHS Continues to Face Challenges in Establishing Itself as a National Focal Point for Cyberspace Security	28
Conclusions	55
Recommendations for Executive Action	59
Agency Comments and Our Evaluation	60
	61

Appendixes

Appendix I: Objectives, Scope, and Methodology	65
Appendix II: DHS Organizations with Cyber-Related Roles	67
Appendix III: Comments from the Department of Homeland Security	70
Appendix IV: GAO Contact and Staff Acknowledgments	73

Tables

Table 1: Sources of Emerging Cybersecurity Threats	5
Table 2: Likely Sources of Cyber Attacks, According to Respondents to the CSI/FBI 2003 Computer Crime and Security Survey	7
Table 3: Types of Cyber Attacks	8
Table 4: Federal Government Actions in Developing CIP Policy	16
Table 5: Infrastructure Sectors Identified by the National Strategy for Homeland Security and HSPD-7	20
Table 6: Thirteen DHS Cybersecurity Responsibilities	22
Table 7: DHS Partnership and Information-Sharing Initiatives	31
Table 8: DHS Initiatives to Enhance Analytical Capabilities	35
Table 9: Incident Response and Recovery Initiatives	37
Table 10: DHS Cybersecurity Awareness and Outreach Initiatives	48
Table 11: Key Initiatives in Cybersecurity Education	49
Table 12: DHS's Intergovernmental Cybersecurity Initiatives	51
Table 13: International Cybersecurity Initiatives	53

Figures

Figure 1: Security Vulnerabilities, 1995-2004	11
Figure 2: NCSD Organization Chart	24

Abbreviations

CERT/CC	CERT® Coordination Center
CIP	critical infrastructure protection
DHS	Department of Homeland Security
HSPD	Homeland Security Presidential Directive
ISAC	information sharing and analysis center
IT	information technology
NCSD	National Cyber Security Division
NIPP	National Infrastructure Protection Plan
US-CERT	United States-Computer Emergency Response Team

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, D.C. 20548

May 26, 2005

Congressional Requesters:

Since the early 1990s, 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 the benefits have been enormous, this widespread interconnectivity also poses significant risks to the government’s and our nation’s computer systems and, more importantly, to the critical operations and infrastructures they support. The speed and accessibility that create the enormous benefits of the computer age, if not properly controlled, allow unauthorized individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. Recent terrorist attacks and threats have further underscored the need to manage and bolster the cybersecurity of our nation’s critical infrastructures.

Federal law and policy call for critical infrastructure protection (CIP) activities that are intended to enhance the cyber and physical security of both the public and private infrastructures that are essential to national security, national economic security, and national public health and safety.¹ Federal policy recognizes the importance of building public/private partnerships and identifies several critical infrastructure sectors as well as federal agencies to work with the sectors to coordinate efforts to strengthen the security of the nation’s public and private, computer-dependent critical infrastructure. In addition, it establishes the Department of Homeland Security (DHS) as the focal point for the security of cyberspace—including analysis, warning, information sharing, vulnerability reduction, mitigation, and recovery efforts for public and private critical infrastructure information systems. To accomplish this mission, DHS is to work with the federal agencies, state and local governments, and the private sector.

In response to your request, we determined (1) DHS’s roles and responsibilities for cyber critical infrastructure protection and national information security, as established in law and policy, and the specific organizational structures DHS has created to fulfill them; (2) the status of

¹This includes the Homeland Security Act of 2002, Homeland Security Presidential Directive 7, and the *National Strategy to Secure Cyberspace*.

DHS's efforts to protect the computer systems that support the nation's critical infrastructures and to strengthen information security—both inside and outside the federal government—and the extent to which such efforts adequately address its responsibilities; and (3) the challenges DHS faces in fulfilling its cybersecurity roles and responsibilities. To accomplish these objectives, we reviewed relevant law, policy, directives, and documents and interviewed officials from DHS, other federal agencies, and the private sector who are involved in efforts to enhance the cybersecurity of critical infrastructures. Appendix I provides further details on our objectives, scope, and methodology. We performed our work from July 2004 to April 2005 in accordance with generally accepted government auditing standards.

Results in Brief

As the focal point for critical infrastructure protection, DHS has many cybersecurity-related roles and responsibilities that are called for in law and policy. These responsibilities include developing plans, building partnerships, and improving information sharing, as well as implementing activities related to the five priorities in the national cyberspace strategy: (1) developing and enhancing national cyber analysis and warning, (2) reducing cyberspace threats and vulnerabilities, (3) promoting awareness of and training in security issues, (4) securing governments' cyberspace, and (5) strengthening national security and international cyberspace security cooperation. To fulfill its cybersecurity role, in June 2003, DHS established the National Cyber Security Division to serve as a national focal point for addressing cybersecurity and coordinating the implementation of cybersecurity efforts.

While DHS has initiated multiple efforts, it has not fully addressed any of the 13 key cybersecurity-related responsibilities that we identified in federal law and policy, and it has much work ahead in order to be able to fully address them. For example, DHS (1) has recently issued the *Interim National Infrastructure Protection Plan*, which includes cybersecurity elements; (2) operates the United States Computer Emergency Readiness Team to address the need for a national analysis and warning capability; and (3) has established forums to foster information sharing among federal officials with information security responsibilities and among various law enforcement entities. However, DHS has not yet developed national threat and vulnerability assessments or developed and exercised government and government/industry contingency recovery plans for cybersecurity, including a plan for recovering key Internet functions. Further, DHS continues to have difficulties in developing partnerships—as called for in

federal policy—with other federal agencies, state and local governments, and the private sector.

DHS faces a number of challenges that have impeded its ability to fulfill its cyber CIP responsibilities. Key challenges include achieving organizational stability; gaining organizational authority; overcoming hiring and contracting issues; increasing awareness about cybersecurity roles and capabilities; establishing effective partnerships with stakeholders (other federal agencies, state and local governments, and the private sector); achieving two-way information sharing with these stakeholders; and demonstrating the value DHS can provide. In its strategic plan for cybersecurity, DHS has identified steps that can begin to address these challenges. However, until it effectively confronts and resolves these underlying challenges, DHS will have difficulty achieving significant results in strengthening the cybersecurity of our nation's critical infrastructures, and our nation will lack the strong cybersecurity focal point envisioned in federal law and policy.

We are making recommendations to the Secretary of Homeland Security to strengthen the department's ability to implement key cybersecurity responsibilities by completing critical activities and resolving underlying challenges.

DHS provided written comments on a draft of this report (see app. III). In brief, DHS agreed that strengthening cybersecurity is central to protecting the nation's critical infrastructures and that much remains to be done. In addition, DHS concurred with our recommendation to engage stakeholders in prioritizing its key cybersecurity responsibilities. However, DHS did not concur with our recommendations to identify and prioritize initiatives to address the challenges it faces, or to establish performance metrics and milestones for these initiatives. Specifically, DHS reported that its strategic plan for cybersecurity already provides a prioritized list, performance measures, and milestones to guide and track its activities. The department sought additional clarification of these recommendations. While we agree with DHS that its plan identifies activities (along with some performance measures and milestones) that will begin to address the challenges, this plan does not include specific initiatives that would ensure that the challenges are addressed in a prioritized and comprehensive manner. For example, the strategic plan for cybersecurity does not include initiatives to help stabilize and build authority for the organization. Further, the strategic plan does not identify the relative priority of its initiatives and does not consistently identify performance measures for completing its initiatives.

As DHS moves forward in identifying initiatives to address the underlying challenges it faces, it will be important to establish performance measures and milestones for fulfilling these initiatives.

DHS officials (as well as others who were quoted in our report) also provided detailed technical corrections, which we have incorporated in this report as appropriate.

Background

Critical Infrastructure Protection (CIP) involves activities that enhance the cyber and physical security of the public and private infrastructures that are critical to national security, national economic security, and national public health and safety. Because a large percentage of the nation's critical infrastructures is owned and operated by the private sector, public/private partnerships are crucial for successful critical infrastructure protection. Recent terrorist attacks and threats have further underscored the need to encourage and manage CIP activities. Vulnerabilities are being identified on a more frequent basis and, if these vulnerabilities are exploited, several of our nation's critical infrastructures could be disrupted or disabled.

Sources of Potential Cyber Attacks on Critical Infrastructures Are Proliferating

Several types of organizations and individuals are capable of conducting attacks on our nation's critical infrastructures. Historically, attacks on our infrastructures could be conducted only by a relatively small number of entities. However, with critical infrastructures' increasing reliance on computers and networks, more organizations and individuals can cause harm using cyber attacks. Further, U.S. authorities are becoming increasingly concerned about the prospect of combined physical and cyber attacks, which could have devastating consequences. Table 1 lists sources of threats that have been identified by the U.S. intelligence community and others.

Table 1: Sources of Emerging Cybersecurity Threats

Threat	Description
Bot-network operators	Bot-network operators are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing ^a schemes, spam, and malware ^b attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam or phishing attacks, etc.).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of U.S. citizens across the country.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking 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 organization insider is a principal source of computer crime. 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 also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
Phishers	Individuals, or small groups, that execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Individuals or organizations that distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several 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 U.S. 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 Federal Bureau of Investigation, Central Intelligence Agency, and the Software Engineering Institute's CERT® Coordination Center.

^aPhishing involves the creation and use of e-mails and Web sites that are designed to look like those of well-known legitimate businesses or government agencies, in order to deceive Internet users into disclosing their personal data for criminal purposes, such as identity theft and fraud.

^bMalware is software designed with malicious intent, such as a virus.

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent—such as crime, terrorism, foreign intelligence gathering, and acts of war. For example, in February 2005, the Federal Bureau of Investigation Director testified before the Senate Select Committee on Intelligence about current threats—including cyber threats—to the United States.² He stated that the cyber threat to the United States is serious, and the number of actors with both the ability and the desire to use computers for illegal and harmful purposes continues to rise. The Director added that individuals or groups from foreign states, including foreign governments, continue to pose threats to our national and economic security because they have the resources to support advanced network exploitation and attack. In addition, he stated that “terrorists show a growing understanding of the critical role of information technology in the day-to-day operations of our economy and national security and have expanded their recruitment to include people studying math, computer science and engineering.” The Director further stated that although individual hackers do not pose a great threat, hackers intent on stealing information or motivated by money are a concern—adding that “if this pool of talent is utilized by terrorists, foreign governments or criminal organizations, the potential for a successful cyber attack on our critical infrastructures is greatly increased.”

²Testimony of Robert S. Mueller, III, Director, Federal Bureau of Investigation, before the Senate Select Committee on Intelligence (Feb. 16, 2005).

Analyses by various organizations have also demonstrated the increasing threats that are faced by critical infrastructure sectors in the United States. For example, in May 2004, the E-Crime Watch™ survey of security and law enforcement executives found that 43 percent of the respondents reported “an increase in electronic crimes and intrusions over the previous year and 70 percent reported at least one electronic crime or intrusion being committed against their organization.” Regarding the source of the electronic crime or intrusion, 70 percent of respondents reported that they knew the source. The respondents most frequently identified hackers (40 percent), followed by current and former employees and contractors (31 percent), as the greatest threats to cybersecurity.³ Similarly, respondents to the 2003 Computer Security Institute and Federal Bureau of Investigation Computer Crime and Security Survey identified independent hackers as the most likely source of cyber attacks, as shown in table 2.⁴

Table 2: Likely Sources of Cyber Attacks, According to Respondents to the CSI/FBI 2003 Computer Crime and Security Survey

Potential source	Percentage of respondents
Independent hackers	82%
Disgruntled employees	77%
U.S. competitors	40%
Foreign governments	28%
Foreign corporations	25%

Source: 2003 CSI/FBI Computer Crime and Security Survey.

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.

³CSO magazine, “2004 E-Crime Watch—Survey Shows Significant Increase in Electronic Crime” (Framingham, MA: May 25, 2004).

⁴Computer Security Institute, *2003 CSI/FBI Computer Crime and Security Survey* (2003).

Types of Attacks Are Expanding and Tools Are Readily Available

According to the Federal Bureau of Investigation, terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping programs (“sniffers”) that can deny access, degrade the integrity of, intercept, or destroy data (see table 3).

Table 3: Types of Cyber Attacks

Type of attack	Description
Denial of service	A method of attack from a single source that denies system access to legitimate users by overwhelming the target computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems or use the Internet.
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.
Exploit tools	Publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Logic bombs	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer’s employment.
Phishing	The creation and use of e-mails and Web sites—designed to look like those of well-known legitimate businesses, financial institutions, and government agencies—in order to deceive Internet users into disclosing their personal data, such as bank and financial account information and passwords. The phishers then take that information and use it for criminal purposes, such as identity theft and fraud.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Trojan horse	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.
Virus	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. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate.
War dialing	Simple programs that dial consecutive telephone numbers looking for modems.
War driving	A method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adaptor that involves patrolling locations to gain unauthorized access.
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.

Source: GAO analysis of reports by the Department of Justice and GAO.

Viruses and worms are commonly used to launch denial-of-service attacks, which generally flood targeted networks and systems by transmitting so much data that regular traffic is either slowed or stopped. Such attacks have been used ever since the groundbreaking Morris worm, which brought 10 percent of the systems connected to the Internet to a halt in November 1988. In 2001, the Code Red worm used a denial-of-service attack to affect millions of computer users by shutting down Web sites, slowing Internet service and disrupting business and government operations.⁵

As the number of individuals with computer skills has increased, intrusion tools have become more readily available and relatively easy to use. Frequently, skilled hackers develop exploitation tools and post them on Internet hacking sites. These tools are then readily available for others to download, allowing even inexperienced programmers to create a computer virus or to literally point and click to launch an attack. According to the National Institute of Standards and Technology, 30 to 40 new attack tools are posted on the Internet every month.⁶ Experts also agree that there has been a steady advance in the sophistication and effectiveness of attack technologies. Intruders quickly develop attacks to exploit vulnerabilities that have been discovered in products, use these attacks to compromise computers, and share them with other attackers. In addition, they can combine these attacks with other forms of technology to develop programs that automatically scan the network for vulnerable systems, attack them, compromise them, and use them to spread the attack even further.

Cyber Vulnerabilities Have Increased

In addition to the growing threat from terrorists, transnational criminals, foreign intelligence services, and hackers, there has been a growing number of software vulnerabilities. Flaws in software code that could cause a program to malfunction generally result from programming errors that occur during software development. The increasing complexity and size of software programs contribute to an increase in software flaws. For example, Microsoft Windows 2000 reportedly contains about 35 million lines of code, compared with about 15 million lines for Windows 95. As

⁵GAO, *Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures*, [GAO-01-1073T](#) (Washington, D.C.: Aug. 29, 2001).

⁶GAO, *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk*, [GAO-01-751](#) (Washington, D.C.: Aug. 13, 2001).

reported by the National Institute of Science and Technology, based on studies of code inspections, there can be as many as 20 flaws per thousand lines of software code. While most flaws do not create security vulnerabilities,⁷ the potential for these errors reflects the difficulty and complexity of delivering trustworthy code.⁸ By exploiting software vulnerabilities, hackers and others who spread malicious code can cause significant damage, ranging from defacing Web sites to taking control of entire systems and thereby being able to read, modify, or delete sensitive information; disrupt operations; launch attacks against other organizations' systems; or destroy systems.

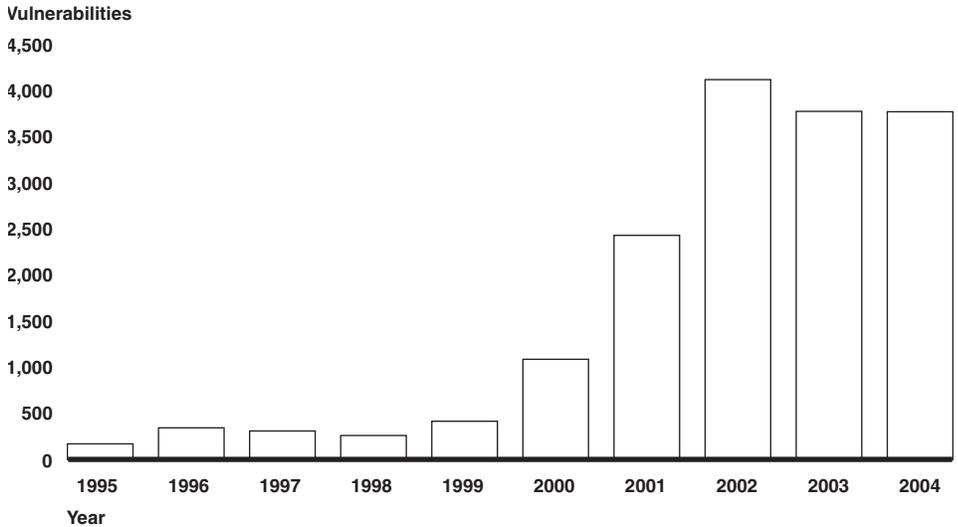
Between 1995 and 2004, the Software Engineering Institute's CERT® Coordination Center (CERT/CC)⁹ reported that 16,726 security vulnerabilities had resulted from software flaws. Figure 1 illustrates the increase in security vulnerabilities over these years.

⁷A vulnerability is a flaw or weakness in hardware or software that can be exploited, resulting in a violation of an implicit or explicit security policy.

⁸National Institute for Standards and Technology, *Procedures for Handling Security Patches: Recommendations of the National Institute of Standards and Technology*, National Institute of Science and Technology Special Publication 800-40 (Gaithersburg, MD: August 2002).

⁹The CERT/CC is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by the Carnegie Mellon University. CERT and CERT® Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

Figure 1: Security Vulnerabilities, 1995-2004



Source: GAO analysis based on CERT/CC data.

Taking Advantage of Vulnerabilities, Attackers Are Able to Cause Serious Consequences

The growing number of known vulnerabilities increases the potential number of attacks. As vulnerabilities are discovered, attackers attempt to exploit them. Attacks can be launched against specific targets or widely distributed through viruses and worms. The risks posed by this increasing and evolving threat are demonstrated in media and other reports of actual and potential attacks and disruptions, such as those cited below.

- 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 adequately fortified their defenses against a potential catastrophic strike.
- In January 2005, a major university reported that a hacker had broken into a database containing 32,000 student and employee Social Security numbers, potentially compromising their finances and identities. In

similar incidents during 2003 and 2004, it was reported that hackers had attacked the systems of other universities, exposing the personal information of over 1.8 million people.

- On August 11, 2003, the Blaster worm was launched, and it infected more than 120,000 computers in its first 36 hours. The worm was programmed to launch a denial-of-service attack against Microsoft's Windows Update Web site, and it affected a wide range of systems and caused slowdowns and disruptions in users' Internet services. For example, the Maryland Motor Vehicle Administration was forced to shut down its computer systems.
- In June 2003, the U.S. government issued a warning concerning a virus that specifically targeted financial institutions. Experts said the BugBear.b virus was programmed to determine whether a victim had used an e-mail address for any of the roughly 1,300 financial institutions listed in the virus's code. If a match was found, the software attempted to collect and document user input by logging keystrokes and then provide this information to a hacker, who could use it in attempts to break into the banks' networks.
- In May 2004, we reported that according to a preliminary study coordinated by the Cooperative Association for Internet Data Analysis, on January 25, 2003, the SQL Slammer worm (also known as "Sapphire" and "SQL Hell") infected more than 90 percent of vulnerable computers worldwide within 10 minutes of its release on the Internet.¹⁰ As the study reports, exploiting a known vulnerability for which a patch had been available since July 2002, Slammer doubled in size every 8.5 seconds and achieved its full scanning rate (55 million scans per second) after about 3 minutes, causing considerable harm through network outages. Further, the study emphasized that the effects would likely have been more severe had Slammer carried a malicious payload, exploited a more widespread vulnerability, or targeted a more popular service. Despite its lack of malicious payload, Slammer caused significant damage, exacting a toll on several large companies and municipalities that found their internal networks deluged with data from the virus. Major financial institutions reported problems; for example, one reported that a majority of its automatic teller machines were unable to process

¹⁰GAO, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*, GAO-04-321 (Washington, D.C.: May 28, 2004).

customer transactions for several hours. The attack disrupted operations for several hours at a 911 call center that served two suburban police departments and at least 14 fire departments. A commercial airline had flights delayed or canceled because of online ticketing and electronic check-in problems.

- In November 2002, a British computer administrator was indicted on charges that he accessed and damaged 98 computers in 14 states between March 2001 and March 2002, causing some \$900,000 in damage. These networks belonged to the Department of Defense, the National Aeronautics and Space Administration, and private companies. The indictment alleges that the attacker was able to gain administrative privileges on military computers, copy password files, and delete critical system files. The attacks rendered the networks of the Earle Naval Weapons Station in New Jersey and the Military District of Washington inoperable.

The CERT/CC has noted that attacks that once took weeks or months to propagate over the Internet now take just hours—or even minutes—because automated tools are now available. For instance, while Code Red achieved an infection rate of over 20,000 systems within 10 minutes in July 2001, about a year and a half later, in January 2003, the Slammer worm successfully attacked at least 75,000 systems, infecting more than 90 percent of vulnerable systems within 10 minutes.

According to CERT/CC, due to the widespread use of automated tools that have made attacks against Internet-connected systems so commonplace, it no longer publishes the number of incidents that are reported. For historical perspective, the number of computer security incidents reported to CERT/CC rose from just under 10,000 in 1999 to over 52,000 in 2001, to about 82,000 in 2002, and to 137,529 in 2003—when CERT/CC stopped reporting the number of incidents. Moreover, the Director of the CERT Centers stated that he estimates that as much as 80 percent of security incidents go unreported, in most cases because (1) the organization was unable to recognize that its systems had been penetrated or there were no indications of penetration or attack or (2) the organization was reluctant to report.

Concerns Regarding the Impact of Cyber Threats on Infrastructure Control Systems Are Growing

Since September 11, 2001, the critical link between cyberspace and physical space has been increasingly recognized. In July 2002, the National Infrastructure Protection Center reported that the potential for compound cyber and physical attacks, referred to as “swarming attacks,” is an emerging threat to our nation’s critical infrastructures. Swarming attacks can slow down or complicate the response to a physical attack. For instance, a cyber attack that disabled the water supply or the electrical system, in conjunction with a physical attack, could deny emergency services the necessary resources to manage the consequences of the physical attack—such as controlling fires, coordinating actions, and generating light.

There is a general consensus—and increasing concern—among government officials and experts on control systems, about potential cyber threats to the control systems that govern our critical infrastructures. In his November 2002 congressional testimony, the Director of the CERT Centers at Carnegie Mellon University noted that supervisory control and data acquisition systems and other forms of networked computer systems had been used for years to control power grids, gas and oil distribution pipelines, water treatment and distribution systems, hydroelectric and flood control dams, oil and chemical refineries, and other physical infrastructure systems.¹¹ These control systems are increasingly being connected to communications links and networks to enhance performance and to reduce operational costs by supporting remote maintenance, remote control, and remote update functions. They are potential targets for individuals intent on causing massive disruption and physical damage. The use of commercial-off-the-shelf technologies for these systems—without adequate security enhancements—can significantly limit available approaches to protection and may increase the number of potential attackers.

¹¹Testimony of Richard D. Pethia, Director, CERT Centers, Software Engineering Institute, Carnegie Mellon University, before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations (November 19, 2002).

As components of control systems increasingly make critical decisions that were once made by humans, the potential effect of a cyber attack becomes more devastating. For example, a failed control system was a contributing factor in the widespread east coast electrical blackout of August 2003. While investigations later found that this incident was not the result of a deliberate attack, DHS officials stated that the significant involvement of a control system highlighted the fact that a physical system or location could be accessed through a cyber connection. Another example occurred in August 2003; the Nuclear Regulatory Commission confirmed that earlier that year the Slammer worm had infected a private computer network at a nuclear power plant, disabling a safety monitoring system for nearly 5 hours. The plant's process computer failed, and it took about 6 hours for it to become available again. The worm reportedly also affected communications on the control networks of at least five other utilities by propagating so quickly that control system traffic was blocked. Looking ahead, 66 percent of the technology experts and scholars who responded to a 2004 survey on the future of the Internet believe that at least one devastating cyber attack will occur on the networked information infrastructure or the country's power grid within the next 10 years.¹²

In March 2004, we reported on the significant challenges of securing controls systems, including technical limitations, perceived lack of economic justification, and conflicting organizational priorities.¹³ We recommended that the Secretary of DHS develop and implement a strategy for coordinating with the private sector and other government agencies to improve the security of control systems. This strategy was issued in December 2004.

Critical Infrastructure Protection Policy Has Continued to Evolve Since the Mid-1990s

Over the years, the federal government and critical infrastructure representatives have sponsored working groups, written reports, issued policies, and created organizations to address CIP. To provide a historical perspective, table 4 summarizes the key developments in federal CIP policy since 1997.

¹²Pew Internet and American Life Project, "The Future of the Internet: In a survey, technology experts and scholars evaluate where the network is headed in the next 10 years." (Washington, D.C.: January 9, 2005)

¹³GAO, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, GAO-04-354 (Washington, D.C.: March 15, 2004).

Table 4: Federal Government Actions in Developing CIP Policy

Policy action	Date	Description
<i>Critical Foundations: Protecting America's Infrastructures^a</i>	Oct. 1997	Described the potentially devastating effects of poor information security on the nation and recommended measures to achieve a higher level of CIP that included industry cooperation and information sharing, a national organizational structure, a revised program of research and development, a broad program of awareness and education, and a reconsideration of related laws.
Presidential Decision Directive 63	May 1998	Established CIP as a national goal and presented a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. Established government agencies to coordinate and support CIP efforts. Identified lead federal agencies to work with coordinators in eight infrastructure sectors and five special functions. Encouraged the development of information-sharing and analysis centers. Required every federal department and agency to be responsible for protecting its own critical infrastructures, including both cyber-based and physical assets. Superseded by HSPD-7 (see details on HSPD-7 below).
<i>National Plan for Information Systems Protection^b</i>	Jan. 2000	Provided a vision and framework for the federal government to prevent, detect, and respond to attacks on the nation's critical cyber-based infrastructure and to reduce existing vulnerabilities by complementing and focusing existing federal computer security and information technology requirements.
Executive Order 13228	Oct. 2001	Established the Office of Homeland Security, within the Executive Office of the President, to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks. Established the Homeland Security Council to advise and assist the President with all aspects of homeland security and to ensure coordination among executive departments and agencies.
Executive Order 13231	Oct. 2001	Established the President's Critical Infrastructure Protection Board to coordinate cyber-related federal efforts and programs associated with protecting our nation's critical infrastructures and to recommend policies and coordinating programs for protecting CIP-related information systems.
<i>National Strategy for Homeland Security^c</i>	July 2002	Identified the protection of critical infrastructures and key assets as a critical mission area for homeland security. Expanded the number of critical infrastructures from the 8 identified in Presidential Decision Directive 63 to 13 and identified lead federal agencies for each.
Homeland Security Act of 2002 ^d	Nov. 2002	Created the Department of Homeland Security and assigned it the following CIP responsibilities: (1) developing a comprehensive national plan for securing the key resources and critical infrastructures of the United States; (2) recommending measures to protect the key resources and critical infrastructures of the United States in coordination with other groups; and (3) disseminating, as appropriate, information to assist in the deterrence, prevention, and preemption of or response to terrorist attacks.

(Continued From Previous Page)

Policy action	Date	Description
<i>The National Strategy to Secure Cyberspace</i> ^e	Feb. 2003	Provided the initial framework for both organizing and prioritizing efforts to protect our nation's cyberspace. Provided direction to federal departments and agencies that have roles in cyberspace security and identified steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity.
<i>The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets</i> ^f	Feb. 2003	Provided a statement of national policy to remain committed to protecting critical infrastructures and key assets from physical attacks. Built on Presidential Decision Directive 63 with its sector-based approach and called for expanding the capabilities of information sharing and analysis centers. Outlined three key objectives: (1) identifying and assuring the protection of the most critical assets, systems, and functions; (2) assuring the protection of infrastructures that face an imminent threat; and (3) pursuing collaborative measures and initiatives to assure the protection of other potential targets.
Executive Order 13286	Feb. 2003	Superseded Executive Order 13231 but maintained the same national policy statement regarding the protection against disruption of information systems for critical infrastructures. Dissolved the President's Critical Infrastructure Protection Board and eliminated the board's chair, the Special Advisor to the President for Cyberspace Security. Designated the National Infrastructure Advisory Council to continue to provide the President with advice on the security of information systems for critical infrastructures supporting other sectors of the economy through the Secretary of Homeland Security.
Homeland Security Presidential Directive 7	Dec. 2003	Superseded Presidential Decision Directive 63 and established a national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attack. Defined roles and responsibilities for the Department of Homeland Security and sector-specific agencies to work with sectors to coordinate CIP activities. Established a CIP Policy Coordinating Committee to advise the Homeland Security Council on interagency CIP issues.

Source: GAO analysis of documents listed above.

^aPresident's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, D.C.: October 1997).

^bThe White House, *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to Dialogue* (Washington, D.C.: January 2000).

^cThe White House, Office of Homeland Security, *National Strategy for Homeland Security*.

^dHomeland Security Act of 2002, Public Law 107-296 (November 25, 2002).

^eThe White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

^fThe White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*.

DHS's Roles and Responsibilities for Cybersecurity in Support of Critical Infrastructure Protection Are Many and Varied

While policies and strategies for protecting our nation's critical infrastructures have evolved over recent years, three key documents (a law, a national policy, and a national strategy) currently guide federal and nonfederal cybersecurity-related CIP efforts. The law establishes DHS's responsibilities for critical infrastructure protection, a role that includes strengthening the security of our nation's information infrastructure. The policy and strategy are consistent with the law, and reinforce and expand on it. Together, the three guiding documents contain numerous and varied requirements levied on DHS, of which 13 key responsibilities address cybersecurity. To fulfill its cybersecurity roles and responsibilities, DHS has established the National Cyber Security Division (NCSA).

Federal Law and Policies Guide Critical Infrastructure Protection and Cybersecurity

Federal law and policies establish CIP as a national goal and describe a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems that are essential to the minimum operations of the economy and the government. These include (1) the Homeland Security Act of 2002, (2) Homeland Security Presidential Directive-7 (HSPD-7), and (3) the *National Strategy to Secure Cyberspace*. A discussion of each follows.

The Homeland Security Act of 2002 Created the Department of Homeland Security

The Homeland Security Act of 2002, signed by the President on November 25, 2002, established DHS and gave it lead responsibility for preventing terrorist attacks in the United States, reducing the vulnerability of the United States to terrorist attacks, and minimizing the damage and assisting in recovery from attacks that do occur. To help DHS accomplish its mission, the act establishes, among other entities, five under secretaries with responsibility over directorates for management, science and technology, information analysis and infrastructure protection, border and transportation security, and emergency preparedness and response.

The act also assigns the department a number of CIP responsibilities, including (1) developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States; (2) recommending measures to protect the key resources and critical infrastructure of the United States in coordination with other federal agencies and in cooperation with state and local government agencies and authorities, the private sector, and other entities; and (3) disseminating, as appropriate, information analyzed by the department—both within the department and to other federal, state, and local government agencies and

private-sector entities—to assist in the deterrence, prevention, preemption of, or response to terrorist attacks.

Homeland Security Presidential Directive 7 Defines Federal CIP Responsibilities

In December 2003, the President issued HSPD-7, which superseded Presidential Decision Directive-63 and established a national policy for federal departments and agencies to identify and prioritize critical infrastructures and key resources and to protect them from terrorist attack. HSPD-7 defines responsibilities for DHS, sector-specific federal agencies that are responsible for addressing specific critical infrastructure sectors, and other departments and agencies. These responsibilities are briefly discussed below.

DHS—HSPD-7 requires, among other things, that the Secretary of Homeland Security

- coordinate the national effort to enhance CIP;
- identify, prioritize, and coordinate the protection of critical infrastructure, emphasizing protection against catastrophic health effects or mass casualties;
- establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors;
- serve as the focal point for securing cyberspace, including analysis, warning, information sharing, vulnerability reduction, mitigation, and recovery efforts for critical infrastructure information systems; and
- produce a comprehensive and integrated national plan for critical infrastructure and key resources protection that outlines national goals, objectives, milestones, and key initiatives.

Sector-specific agencies—HSPD-7 designated certain federal agencies as lead federal points of contact for the critical infrastructure sectors identified in the *National Strategy for Homeland Security* (see table 5). These agencies are responsible for infrastructure protection activities in their assigned sectors and are to coordinate and collaborate with relevant federal agencies, state, and local governments, and the private sector to carry out related responsibilities.

Table 5: Infrastructure Sectors Identified by the National Strategy for Homeland Security and HSPD-7

Sector	Description	Lead agency
Agriculture	Provides for the fundamental need for food. The infrastructure includes supply chains for feed and crop production.	Department of Agriculture
Banking and finance	Provides the financial infrastructure of the nation. This sector consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions, including clearing and settlement.	Department of the Treasury
Chemicals and hazardous materials	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical industry produces more than 70,000 products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.	Department of Homeland Security
Commercial facilities	Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.	Department of Homeland Security
Dams	Comprises approximately 80,000 dam facilities, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.	Department of Homeland Security
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.	Department of Defense
Drinking water and water treatment systems	Sanitizes the water supply with the use of about 170,000 public water systems. These systems depend on reservoirs, dams, wells, treatment facilities, pumping stations, and transmission lines.	Environmental Protection Agency
Emergency services	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.	Department of Homeland Security
Energy	Provides the electric power used by all sectors, including critical infrastructures, and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.	Department of Energy
Food	Carries out the post-harvesting of the food supply, including processing and retail sales.	Department of Agriculture and Department of Health and Human Services
Government	Ensures national security and freedom and administers key public functions.	Department of Homeland Security
Government facilities	Includes the buildings owned and leased by the federal government for use by federal entities.	Department of Homeland Security
Information technology and telecommunications	Provides communications and processes to meet the needs of businesses and government.	Department of Homeland Security
National monuments and icons	Includes key assets that are symbolically equated with traditional American values and institutions or U.S. political and economic power.	Department of the Interior

(Continued From Previous Page)

Sector	Description	Lead agency
Nuclear reactors, materials, and waste	Includes 104 commercial nuclear reactors; research and test nuclear reactors; nuclear materials; and the transportation, storage, and disposal of nuclear materials and waste.	Department of Homeland Security working with the Nuclear Regulatory Agency and Department of Energy
Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The U.S. Postal Service and other carriers provide the services of this sector.	Department of Homeland Security
Public health and healthcare	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. The sector consists of health departments, clinics, and hospitals.	Department of Health and Human Services
Transportation systems	Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.	Department of Homeland Security in collaboration with the Department of Transportation

Source: GAO analysis based on the President's National Strategy documents and HSPD-7.

Other federal agencies—HSPD-7 instructs all federal departments and agencies to identify, prioritize, and coordinate the protection of their own critical infrastructures in order to prevent, deter, and mitigate the effects of attacks. In addition, this national policy recognizes that certain other federal entities have special functions related to critical infrastructure and key resources protection, such as the Department of Justice's law enforcement function, the State Department's foreign affairs function, and the Executive Office of the President's Office of Science and Technology's research and development policy-setting function.

The *National Strategy to Secure Cyberspace* Provides an Initial Framework for Cybersecurity

The *National Strategy to Secure Cyberspace* (cyberspace strategy), a national policy issued in February 2003, provides a framework for both organizing and prioritizing efforts to protect our nation's cyberspace. It also provides direction to federal departments and agencies that have roles in cyberspace security and identifies steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity. In addition, the cyberspace strategy identifies DHS as the central coordinator for cyberspace security efforts. As such, DHS is responsible for coordinating and working with other federal and nonfederal entities that are involved in cybersecurity.

The cyberspace strategy is organized according to five national priorities, and it identifies major actions and initiatives for each. The five priorities are (1) providing national cyber analysis, warning, and incident response; (2) reducing cyberspace threats and vulnerabilities; (3) promoting awareness and training; (4) securing governments' cyberspace; and (5)

strengthening national security and international cyberspace security cooperation.

DHS Has 13 Key Cybersecurity Responsibilities

Among the many CIP roles and responsibilities established for DHS identified in federal law and policy are 13 key cybersecurity-related responsibilities. These include general CIP responsibilities that have a cyber element (such as developing national plans, building partnerships, and improving information sharing) as well as responsibilities that relate to the five priorities established by the cyberspace strategy. Table 6 provides a description of each responsibility.

Table 6: Thirteen DHS Cybersecurity Responsibilities

DHS cybersecurity responsibilities	
General CIP responsibilities with a cyber element	Description
Develop a national plan for critical infrastructure protection that includes cybersecurity.	Developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including information technology and telecommunications systems (including satellites) and the physical and technological assets that support such systems. This plan is to outline national strategies, activities, and milestones for protecting critical infrastructures.
Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector.	Fostering and developing public/private partnerships with and among other federal agencies, state and local governments, the private sector, and others. DHS is to serve as the “focal point for the security of cyberspace.”
Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities.	Improving and enhancing information sharing with and among other federal agencies, state and local governments, the private sector, and others through improved partnerships and collaboration, including encouraging information sharing and analysis mechanisms. DHS is to improve sharing of information on cyber attacks, threats, and vulnerabilities.
Responsibilities related to the cyberspace strategy’s five priorities	
Develop and enhance national cyber analysis and warning capabilities.	Providing cyber analysis and warnings, enhancing analytical capabilities, and developing a national indications and warnings architecture to identify precursors to attacks.
Provide and coordinate incident response and recovery planning efforts.	Providing crisis management in response to threats to or attacks on critical information systems. This entails coordinating efforts for incident response, recovery planning, exercising cybersecurity continuity plans for federal systems, planning for recovery of Internet functions, and assisting infrastructure stakeholders with cyber-related emergency recovery plans.
Identify and assess cyber threats and vulnerabilities.	Leading efforts by the public and private sector to conduct a national cyber threat assessment, to conduct or facilitate vulnerability assessments of sectors, and to identify cross-sector interdependencies.

(Continued From Previous Page)

DHS cybersecurity responsibilities

General CIP responsibilities with a cyber element	Description
Support efforts to reduce cyber threats and vulnerabilities.	Leading and supporting efforts by the public and private sector to reduce threats and vulnerabilities. Threat reduction involves working with the law enforcement community to investigate and prosecute cyberspace threats. Vulnerability reduction involves identifying and remediating vulnerabilities in existing software and systems.
Promote and support research and development efforts to strengthen cyberspace security.	Collaborating and coordinating with members of academia, industry, and government to optimize cybersecurity related research and development efforts to reduce vulnerabilities through the adoption of more secure technologies.
Promote awareness and outreach.	Establishing a comprehensive national awareness program to promote efforts to strengthen cybersecurity throughout government and the private sector, including the home user.
Foster training and certification.	Improving cybersecurity-related education, training, and certification opportunities.
Enhance federal, state, and local government cybersecurity.	Partnering with federal, state, and local governments in efforts to strengthen the cybersecurity of the nation's critical information infrastructure to assist in the deterrence, prevention, preemption of, and response to terrorist attacks against the United States.
Strengthen international cyberspace security.	Working in conjunction with other federal agencies, international organizations, and industry in efforts to promote strengthened cybersecurity on a global basis.
Integrate cybersecurity with national security.	Coordinating and integrating applicable national preparedness goals with its National Infrastructure Protection Plan.

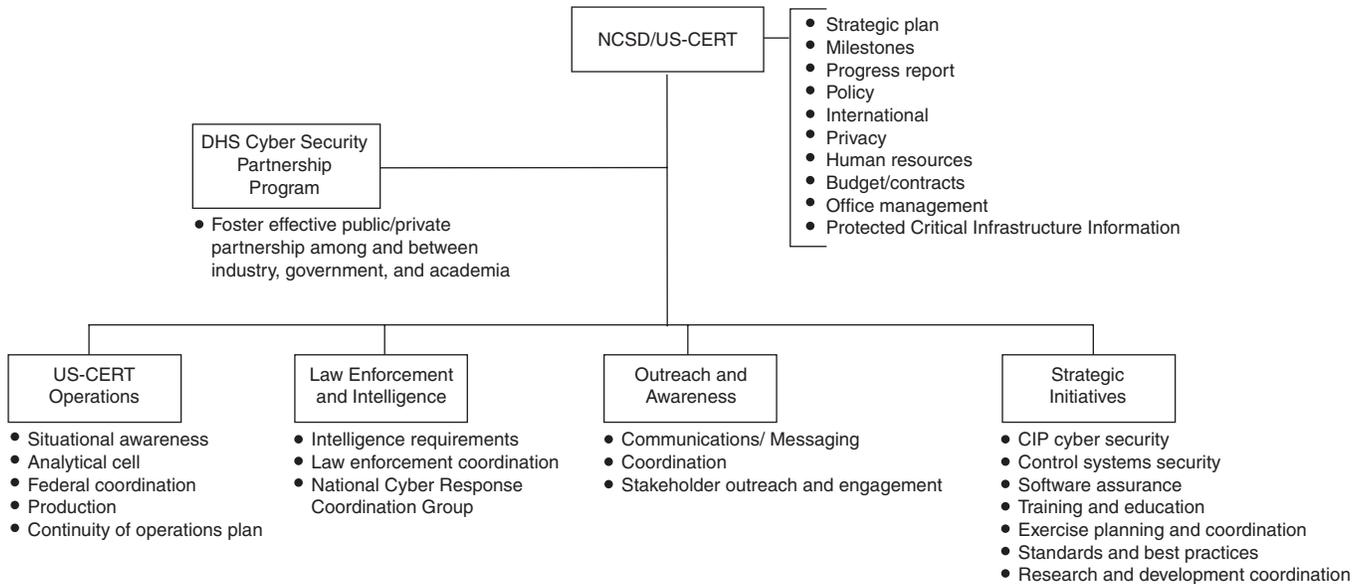
Source: GAO analysis of the Homeland Security Act of 2002, the Homeland Security Presidential Directive-7, and the *National Strategy to Secure Cyberspace*.

DHS Has Established an Organizational Structure to Fulfill Its Cybersecurity Requirements

In June 2003, DHS established the National Cyber Security Division (NCSA), under its Information Analysis and Infrastructure Protection Directorate, to serve as a national focal point for addressing cybersecurity issues and to coordinate implementation of the cybersecurity strategy. NCSA also serves as the government lead on a public/private partnership supporting the U.S. Computer Emergency Response Team (US-CERT) and as the lead for federal government incident response.

NCSA is headed by the Office of the Director and includes a cybersecurity partnership program as well as four branches: US-CERT Operations, Law Enforcement and Intelligence, Outreach and Awareness, and Strategic Initiatives. Table 7 displays the NCSA organization chart and the major functions of each organization; it is followed by a brief description of each organization's roles and responsibilities.

Figure 2: NCSO Organization Chart



Source: DHS.

NCSO/US-CERT Director

The NCSO/US-CERT Director is responsible for issues related to the operation of the NCSO, such as human resources, policy, and budget, as well as international coordination efforts. The director is responsible for managing US-CERT—which is a partnership between NCSO and the public and private sectors to make cybersecurity a coordinated, national effort; increase public awareness of cyber threats and vulnerabilities; and improve computer security preparedness and response to cyber threats.

DHS Cyber Security Partnership Program

This program is to foster effective public/private partnership among and between industry, government, and academia. It is intended to facilitate and leverage stakeholder collaboration to drive measurable progress in addressing cybersecurity issues and mitigating cyber vulnerabilities. Under the auspices of the partnership program, DHS works jointly with software developers, academic institutions, researchers, and communities of interest—including the information sharing and analysis centers (ISAC)—

as well as with DHS's federal, state, local, and international government counterparts.

US-CERT Operations Branch

NCSD's US-CERT Operations branch focuses on situational awareness, analytical cells, and federal coordination. It is to provide capabilities to US-CERT and coordinate all cyber incident warnings and responses across both the government and the private sector through US-CERT. A key component of US-CERT is the National Cyber Security Response System (Response System), which provides a nationwide, real-time collaborative information-sharing network to enable communication and collaboration among DHS and federal, state, local, and international government and law enforcement entities. Components of the Response System include the following:

- The US-CERT Operations Center serves as a 24-hour-a-day/7-day-a-week, real-time focal point for cybersecurity, conducting daily conference calls with U.S.-based watch and warning centers to share classified and unclassified security information.
- The US-CERT Portal provides a Web-based collaborative system that allows US-CERT to share sensitive cyber-related information with members of government and industry.
- The US-CERT Control Systems Security Center serves as an operational and strategic component of US-CERT's capability to address the complex security issues associated with the use of control systems.
- The US-CERT public Web site provides government, the private sector, and the public with information they need to improve their ability to protect their information systems and infrastructures.
- The National Cyber Alert System is to deliver targeted, timely, and actionable information to Americans to allow them to secure their computer systems.

-
- The National Cyber Response Coordination Group brings together officials from federal agencies to coordinate public/private cyber preparedness and incident response.¹⁴
 - The Government Forum of Incident Response and Security Teams is a community of government response teams that are responsible for securing government information technology systems. This forum works to understand and handle computer security incidents and to encourage proactive and preventative security practices.

Law Enforcement and Intelligence Branch

The Law Enforcement and Intelligence branch of NCSA has two primary responsibilities: managing the National Cyber Response Coordinating Group and facilitating the coordination of law enforcement and intelligence cyber-related efforts for NCSA. This branch provides a mechanism for information sharing among the components concerned with cyber issues of law enforcement, intelligence, and the private sector. This information sharing includes all levels of information (classified, law enforcement sensitive, and unclassified). The branch coordinates clearing classified information of its sensitive content and shares it with private sector partners.

Outreach and Awareness Branch

NCSA's Outreach and Awareness branch is responsible for outreach, awareness, and messaging. The branch promotes cybersecurity awareness among the general public and within key communities, maintains relationships with governmental cybersecurity professionals to coordinate and share information about cybersecurity initiatives, and develops partnerships to promote public/private coordination and collaboration on cybersecurity issues.

The branch is organized into three functional areas: Stakeholder Outreach, Communications and Messaging, and Coordination. The Stakeholder Outreach team serves to build and maintain relationships among and

¹⁴This group, operating under the authority granted by the Cyber Annex to the National Response Plan, is a forum of national security, law enforcement, defense, intelligence, and other government agencies that coordinates intragovernment and public/private preparedness and response to and recovery from national level cyber incidents and physical attacks that have significant cyber consequences.

between industry, government, and academia in order to raise cybersecurity awareness and secure cyberspace. The Communications and Messaging team focuses on coordination of internal and external communications. The Coordination team works to ensure collaboration on events and activities across NCSA and with other DHS entities, including the public affairs, legislative affairs, and private-sector offices and others, as appropriate. In addition, the team works to foster the department's role as a focal point and coordinator for securing cyberspace and implementing the *National Strategy to Secure Cyberspace*.

Strategic Initiatives Branch

NCSA's Strategic Initiatives branch is organized into six teams with different responsibilities, as follows:

- The CIP Cybersecurity team is jointly responsible (with DHS's National Communications System) for developing a CIP plan for the Information Technology (IT) Sector, including the Internet, that will identify critical assets and vulnerabilities, map interdependencies, and promote cyber awareness throughout other federal sector plans.
- The Control Systems team is responsible for facilitating control system incident management and security awareness, establishing an assessment capability for vulnerability reduction and incident response, creating a self-sustaining security culture within the control systems community, focusing attention on the protection of legacy control systems, and making strategic recommendations for the future of control systems and security products.
- The Software Assurance initiative presents a framework for promoting and coordinating efforts to improve the security, reliability, and safety of software.
- The Training and Education team is responsible for promoting the development of an adequate number of effective cybersecurity professionals, enhancing cybersecurity capability within the federal workforce by identifying the skills and abilities necessary for specific job tasks, and working with other organizations to develop content standards for training products and for certifications.
- The Exercise Plans and Programs team is charged with improving the nation's ability to respond to cyber incidents by creating, sponsoring,

and learning from international, national, regional, and interagency exercises. The team is responsible for planning and coordinating cybersecurity exercises with internal and external DHS stakeholders.

- The Standards and Best Practices/Research and Development Coordination team works to encourage technology innovation efforts. The team is responsible for identifying cybersecurity research and development requirements and cybersecurity standards issues and for assembling and distributing information on best practices.

NCSD Collaborates with Other DHS Entities to Accomplish Its Mission

DHS has additional directorates, branches, and offices with CIP responsibilities. In its role as the cybersecurity focal point, NCSD collaborates with these other DHS entities, including the Infrastructure Coordination Division, which runs the Protected Critical Infrastructure Information program to encourage sharing of sensitive information (including cybersecurity-related information), and the National Communications System, a federal interagency group, which is responsible for, among other things, improving the effectiveness of the management and use of national telecommunications resources to support the federal government during emergencies. In appendix II, we discuss other DHS entities with responsibilities for CIP-related activities that impact cybersecurity.

DHS Has Initiated Efforts That Begin to Address Its Responsibilities, but More Work Remains

DHS has initiated efforts that begin to address each of its 13 key responsibilities for cybersecurity; however, the extent of progress varies among these responsibilities, and more work remains to be done on each. For example, DHS (1) has recently issued an interim plan for infrastructure protection that includes cybersecurity plans, (2) is supporting a national cyber analysis and warning capability through its role in US-CERT, and (3) has established forums to build greater trust and to encourage information sharing among federal officials with information security responsibilities and among various law enforcement entities. However, DHS has not yet developed national cyber threat and vulnerability assessments or developed and exercised government and government/industry contingency recovery plans for cybersecurity, including a plan for recovering key Internet functions. The department also continues to have difficulties in developing partnerships, as called for in federal policy, with other federal agencies, state and local governments, and the private sector. Without such partnerships, it is difficult to develop the trusted, two-way information sharing that is essential to improving homeland security.

We discuss below the steps that DHS has taken related to each of the department's 13 key responsibilities and the steps that remain.

DHS Recently Issued National Plan For Improving Critical Infrastructure Protection That Includes Cybersecurity, but This Plan Is Not Yet Comprehensive and Complete

In February 2005, DHS issued a national plan for critical infrastructure protection that includes cybersecurity-related initiatives. This plan, the Interim National Infrastructure Protection Plan (Interim NIPP), addresses many of the requirements identified in federal law and policy, but it does not yet comprise a comprehensive and complete plan.

Specifically, the Interim NIPP provides a strategy for protecting critical infrastructures by integrating physical security and cybersecurity in its goals, objectives, and planned actions. Key actions include developing and implementing sector-specific and cross-sector protection plans; conducting cross-sector interdependency analysis; conducting and updating vulnerability assessments at the asset, sector, and cross-sector levels; and establishing performance metrics. In addition, the Interim NIPP establishes a national organizational structure to provide effective partnerships, communications, and coordination between DHS and infrastructure stakeholders.

However, the plan does not yet comprise the comprehensive national plan envisioned in federal law and policy, for several reasons, including the following.

- **The Interim NIPP lacks sector-specific cybersecurity plans.** This plan does not yet include detailed plans for addressing cybersecurity in the infrastructure sectors. Agency officials acknowledge that many of the detailed plans for addressing cybersecurity will be included in the sector-specific annexes that are to be provided in the next version of the plan. To ensure that cybersecurity will be appropriately and consistently addressed in the next version of the plan, NCSA has provided guidance to sector-specific agencies regarding the inclusion of cybersecurity issues in their respective sector-specific plans. In addition, NCSA continues to review and provide feedback on the sector-specific plans, which will become annexes to the next NIPP.
- **The Interim NIPP is not yet a final plan.** The development of this plan is an ongoing, evolving process that requires the participation of key stakeholders, including other federal agencies, state and local governments, the private sector, foreign countries, and international

organizations. DHS expects to obtain and incorporate stakeholder comments and to issue a more complete NIPP in November 2005.

- **The Interim NIPP lacks required milestones.** Specifically, this plan does not include any national-level milestones for completing efforts to enhance the security of the nation's critical infrastructures. According to a DHS official, these milestones will be incorporated in the sector-specific plans.

DHS acknowledges the need to address these issues with the Interim NIPP and plans to do so in subsequent versions. According to DHS officials, as the NIPP evolves and as the sector-specific plans are developed, the level of specificity will increase to include key initiatives and milestones.

DHS Has Taken Positive Steps Toward Building Partnerships and Improving Information Sharing, but Additional Work Is Needed

DHS has undertaken numerous initiatives to foster partnerships and enhance information sharing with other federal agencies, state and local governments, and the private sector about cyber attacks, threats, and vulnerabilities; but more work is needed to address underlying barriers to sharing information.

DHS and NCSD have multiple initiatives under way to enhance partnerships and information sharing. Descriptions of selected initiatives are provided in table 7.

Table 7: DHS Partnership and Information-Sharing Initiatives

Initiative	Description
National Cyber Response and Coordination Group	<ul style="list-style-type: none"> Facilitates coordination of intragovernmental and public/private preparedness and operations in order to respond to and recover from incidents that have significant cyber consequences. Brings together officials from national security, law enforcement, defense, intelligence, and other government agencies that maintain significant cybersecurity responsibilities and capabilities.
National Cyber Security Response System	<ul style="list-style-type: none"> Provides a nationwide, real-time, collaborative information-sharing network that enables state and local government officials, federal agencies, the private sector, international counterparts, and law enforcement entities to communicate and collaborate with DHS and each other about cyber issues. Includes a number of different mechanisms for sharing information between and among federal and nonfederal entities, including the US-CERT operations center, the US-CERT portal, the US-CERT Control Systems Security Center, the US-CERT public Web site, and the National Cyber Alert System.
Expanded use of Cyber Warning Information Network	<ul style="list-style-type: none"> Expands DHS's use of the Cyber Warning Information Network, a private communications network (voice and data) with no logical dependency on the Internet or the public switched network in order to provide a backup mechanism for information sharing.
Government Forum of Incident Response and Security Teams	<ul style="list-style-type: none"> Brings together technical and tactical practitioners from government agency security response teams. Forum members work together to understand and handle computer security incidents reported by federal agencies and to encourage proactive and preventative security practices. Shares specific technical details regarding incidents within a trusted U.S. government environment on an agency-to-peer level.
Chief Information Security Officers Forum	<ul style="list-style-type: none"> Brings together federal officials responsible for the information security of their respective agencies and provides a trusted venue for them to collaborate; leverage each other's experiences, capabilities and programs, and lessons learned; and address and discuss particularly problematic or challenging areas.
DHS Cyber Security Partnership Program	<ul style="list-style-type: none"> Develops and enhances strategic partnerships with 32 industry associations and hundreds of small, medium, and large enterprises, establishing an outreach channel of over 1 million constituents. Facilitates improved information sharing, including the interchange of lessons learned and best practices.
ISAC partnerships	<ul style="list-style-type: none"> Enhances partnerships with the ISACs—including the ISACs for electricity, telecommunications, and states, and with information technology vendors. DHS officials reported that all of the critical infrastructure sectors' ISACs are part of the US-CERT portal and that they participate in information sharing exercises—including regularly scheduled daily or biweekly meetings.
US-CERT Control Systems Security Center Outreach	<ul style="list-style-type: none"> Fosters public/private collaboration to improve the security of critical infrastructure control systems. NCSO reports that it has established relationships with more than 25 potential partners for future participation in the center.
Internal DHS collaboration	<ul style="list-style-type: none"> Entails NCSO collaborating with the Protected Critical Infrastructure Information program office to establish procedures for the private sector to electronically submit critical infrastructure information. These offices have developed a process for companies and other entities to use to facilitate sharing protected information on a continual basis.

Source: GAO analysis based on DHS information.

Although NCSID has taken steps to develop partnerships and information-sharing mechanisms, the organization has not effectively leveraged its partnerships to increase the sharing of information. For example, although the Multi-State ISAC and US-CERT have established an effective working relationship, according to officials from both organizations, their ability to share classified information has been hindered by ISAC members' lack of security clearances. Further, DHS officials reported that only limited information has been shared by the private sector under the Protected Critical Infrastructure Information program¹⁵ because of private sector concerns about what information DHS would share with other federal agencies.

Additionally, key stakeholders in NCSID partnerships have expressed concerns about information sharing. For example, while officials from several CIP-related federal agencies found the Chief Information Security Officers forum to be valuable, officials from one agency stated that it had been largely ineffective in improving communications among federal agencies. Regarding NCSID's efforts with the private sector, one ISAC reported publicly that its information sharing with DHS was disintegrating. Further, a representative from that ISAC stated that DHS had abruptly stopped sending notices to ISAC managers and no longer called the ISAC about new terrorism activity. Further, an ISAC official stated that when the ISAC recently contacted DHS's Homeland Security Operations Center about rumors of a dirty bomb during a national event, ISAC officials were told to obtain the information from the media.

¹⁵The Protected Critical Infrastructure Information program was established to encourage private industry to share sensitive and proprietary business information about its critical infrastructures with the government with the assurance that the information would be protected from public disclosure, in accordance with the Critical Infrastructure Information Act of 2002.

Issues related to the development of partnerships and of appropriate information-sharing relationships are not new. In July 2004, we recommended actions to improve the effectiveness of DHS's information-sharing efforts.¹⁶ We recommended that officials within the Information Analysis and Infrastructure Protection Directorate (1) proceed with and establish milestones for developing an information-sharing plan and (2) develop appropriate DHS policies and procedures for interacting with ISACs, sector coordinators (groups or individuals designated to represent their respective infrastructure sectors' CIP activities), and sector-specific agencies and for coordination and information sharing within the Information Analysis and Infrastructure Protection Directorate and other DHS components. Moreover, we recently designated establishing appropriate and effective information-sharing mechanisms to improve homeland security as a new high-risk area.¹⁷ We reported that the ability to share security-related information can unify the efforts of federal, state, and local government agencies and the private sector in preventing or minimizing terrorist attacks.

In its strategic plan for cybersecurity, DHS acknowledges the need to build better partnerships and information-sharing relationships. Among the actions that DHS identified are enhancing the US-CERT Operations Center's capabilities and increasing participation in information-sharing mechanisms such as the National Cyber Alert System. For the nonfederal sector, DHS's strategic plan for cybersecurity includes actions to develop effective public/private partnerships through associations, ISACs, Internet service providers, and improved international partnerships. For federal agency information security, the strategic plan identifies efforts to improve government mechanisms, such as the National Cyber Response Coordination Group and the Government Forum of Incident Response and Security Teams. In addition, the Interim NIPP acknowledges as a goal, the importance of building partnerships among stakeholders to implement critical infrastructure protection programs and identifies related objectives, including establishing mechanisms for coordination and information exchange among partners.

¹⁶GAO, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, [GAO-04-780](#) (Washington, D.C.: July 9, 2004).

¹⁷GAO, *High-Risk Series: An Update*, [GAO-05-207](#) (Washington, D.C.: January 2005).

DHS Provides National Cyber Analysis and Warning Capabilities but Has Not Yet Developed an Architecture to Support Strategic Capabilities, and Analytical Tools Require Further Maturity

DHS has collaborated on, developed, and is working to enhance tools and communication mechanisms for providing analysis and warning of occurring and potential cyber incidents, but it has not yet developed the indications and warning architecture required by HSPD-7, and important analytical tools are not yet mature.

Through NCSA's involvement in US-CERT, DHS provides cyber analysis and warning capabilities by providing continuous operational support in monitoring the status of systems and networks. When a new vulnerability or exploit is identified, US-CERT evaluates its severity; determines what actions should be taken and what message should be disseminated; and provides information through NCSA's multiple communications channels, including its daily telephone call with other U.S.-based watch and warning centers, the US-CERT portal, the US-CERT public Web site, and the National Cyber Alert System. It produces the following types of warnings:

- **Technical cybersecurity alerts**—provide real-time information about current security issues, vulnerabilities, and exploits.
- **Cybersecurity bulletins**—provide technical audiences with weekly summaries of security issues and new vulnerabilities.
- **Cybersecurity alerts**—provide nontechnical audiences with real-time information about current issues, vulnerabilities, and exploits and include steps and actions that nontechnical users can take.
- **Cybersecurity tips**—describe common security issues and offer advice for nontechnical users.
- **Vulnerability notes**—provide warnings about vulnerabilities that do not meet the severity threshold required to issue an alert.

Additionally, when a situation warrants direct contact with a federal agency, an infrastructure sector, or a nonfederal entity, NCSA contacts the entity and provides relevant information prior to making public announcements about the situation. This includes collaborating with relevant software vendors on a particular vulnerability or exploit.

DHS is also involved in several initiatives to enhance cyber analytical capabilities. Key initiatives are identified in table 8.

Table 8: DHS Initiatives to Enhance Analytical Capabilities

Initiative	Description
Intelligence sharing	US-CERT serves as a conduit for sharing information from the intelligence and law enforcement communities to the civilian federal and nonfederal communities. According to an NCSD official, its law enforcement and intelligence branch works to share declassified information about threats, malicious activities, or vulnerabilities with US-CERT members. In addition, US-CERT can share information with the law enforcement and intelligence communities that might not reach these groups by other means.
Situational awareness tools	NCSD's US-CERT Einstein Program, which is currently in pilot testing at the Department of Transportation, is to obtain network flow data from federal agencies and analyze the traffic patterns and behavior. This information is to be combined with other relevant data to (1) detect potential deviations and identify how Internet activities are likely to affect federal agencies and (2) provide insight into the health of the Internet and suspicious activities.
Malicious Code Analysis Program	This program includes (1) a laboratory for analyzing malicious code and developing countermeasures and (2) a common vulnerabilities and exposures dictionary system to correlate information across vendor products.
Cyber-incident repository	NCSD officials are collaborating with multiple partners (including the Department of Defense, the intelligence community, law enforcement, academia, private industry, and the public) to develop a repository for cyber-related intelligence data.

Source: GAO analysis based on DHS information.

Despite its progress in providing analysis and warning capabilities, DHS has not yet developed or deployed a national indications and warning architecture for infrastructure protection that would identify the precursors to a cyber attack, and NCSD's analytical capabilities are still evolving and are not yet robust. For example, the US-CERT Einstein program, identified in table 8, is in the early stages of deployment and is currently being pilot tested at one agency. In addition, NCSD officials acknowledge that the program's current analytical capabilities are not expected to provide national-level indicators and precursors to a cyber attack, as called for in HSPD-7's requirement that DHS provide an indications and warning architecture.

DHS is still facing the same challenges in developing strategic analysis and warning capabilities that we reported on 4 years ago during a review of NCSD's predecessor, the National Infrastructure Protection Center. In 2001, we reported on the analysis and warnings efforts within the center and identified several challenges that were impeding development of an effective strategic analysis and warning capability.¹⁸ We reported that a

¹⁸GAO, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, GAO-01-323 (Washington, D.C.: Apr. 25, 2001).

generally accepted methodology for analyzing strategic cyber-based threats did not exist. Specifically, there was no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. We also reported that the Center did not have the industry-specific data on factors such as critical systems components, known vulnerabilities, and interdependencies.

We therefore recommended that the responsible executive-branch officials and agencies establish a capability for strategic analysis of computer-based threats, including developing a methodology, acquiring expertise, and obtaining infrastructure data. However, officials have taken little action to establish this capability, and therefore our recommendations remain open today.

In its strategic plan for cybersecurity, DHS acknowledges that it has more to do to enhance its analytical capability and to leverage existing capabilities. Specifically, it establishes objectives and activities to

- enhance the US-CERT Operations Center capability,
- expand the US-CERT Einstein Program pilot to a total of six agencies,
- promote consistency across federal civilian incident-response teams,
- develop a vulnerability assessment methodology and compile vulnerability information, and
- improve its coordinated cyber intelligence capability.

DHS Has Improved Its Ability to Coordinate Incident Response, but More Recovery Planning and Exercises Are Needed

DHS has improved its ability to coordinate a response to cyber attacks with federal, state, and local governments and private-sector entities through the communications capabilities that it has developed for US-CERT, the continued expansion of backup communication capabilities, and the establishment of collaboration mechanisms. However, DHS's plans and exercises for recovering from attacks are not yet complete and comprehensive.

As a partnership between DHS and the public and private sectors to make cybersecurity a coordinated national effort, US-CERT is an essential mechanism for coordinating information and activity on a real-time basis. US-CERT's Operations Center, secure portal, public Web site, and National

Cyber Alert System not only provide means for disseminating alerts and warnings—as discussed above—but they also support incident response and recovery efforts.

Additionally, DHS is expanding its incident response and recovery capabilities through the use of the Critical Infrastructure Warning Information Network, a survivable communications network that does not rely on public telecommunications networks or the Internet. DHS has installed these network terminals in key government network operations centers, in several private industry network operations centers, and in the United Kingdom’s National Infrastructure Security Coordination Centre. In addition, it is considering placing additional network nodes at critical government agencies, companies, and trusted foreign partners.

Additional initiatives to expand incident response and recovery capabilities, including mechanisms for collaboration, are identified in table 9.

Table 9: Incident Response and Recovery Initiatives

Initiative	Description
National Cyber Response Coordination Group	<p>The National Cyber Response Coordination Group was formalized in the Cyber Annex of the <i>National Response Plan</i> and is cochaired by NCSD, the Department of Justice’s Computer Crime and Intellectual Property Section, and the Department of Defense. In the event of a significant incident (including cyber incidents and physical incidents that affect cyber networks), this group would play a major role in coordinating responses and recovery planning. Specifically, it is expected to develop and provide a strategic assessment of the impact on the information infrastructure and a coordinated response, through its close association with others in private industry, academia, and international and local governments.</p> <p>The National Cyber Response Coordination Group brings together officials from all agencies that have a statutory responsibility for cybersecurity and the sector-specific agencies identified in HSPD-7. The group meets monthly and is developing cyber preparedness and response plans that will help it support the overarching mission of the DHS Interagency Incident Management Group. To date, the group has conducted two exercises to test its concept of operations and communications mechanisms and has held a workshop to analyze the thresholds for convening the group.</p>

(Continued From Previous Page)

Initiative	Description
National Exercise Program Office	<p>DHS established the National Exercise Program Office to improve response planning and coordination between public and private incident response and recovery capabilities by having them undertake exercises.</p> <p>To date, NCSD has sponsored several exercises that test cyber readiness in various geographic locations and critical infrastructure sectors across the nation. In September and October 2004, regional exercises were held in Seattle and New Orleans. Both exercises highlighted dependencies between cyber and physical infrastructures and interdependencies among critical infrastructures. These exercises also identified and tested the coordination and cooperation among federal, state, and local governments and the private sector that would be necessary in the case of attacks (both physical and cyber) on the critical infrastructures in those regions of the United States. According to NCSD officials, these regional exercises have pointed out the importance of regional response capabilities and have spurred activity in both regions to develop working groups to improve response capabilities within those regions.</p> <p>NCSD, along with DHS's Office of Domestic Preparedness, sponsored two cyber-focused tabletop exercises^a in Connecticut and New Jersey. According to NCSD officials, these tabletop exercises offered an opportunity for key state agencies, including information technology, emergency preparedness, and law enforcement, to address cybersecurity issues and increase coordination within their state governments as well as with the federal government. In addition, NCSD prepared the cyber-related portion for the Top Officials 3 exercise, referred to as TOPOFF 3, that occurred in March and April 2005. This exercise tested not only response to attacks, but also continuity of government and operations; emergency response at the state, regional, and local levels; and containment and mitigation of chemical, nuclear, and other attacks.</p> <p>Further, according to NCSD officials, the NCSD Exercise Team is working closely with the National Cyber Response Coordination Group to sponsor a series of four tabletop exercises in fiscal year 2005 that are intended to mature and refine the interagency body's Concept of Operations and to accelerate the development of detailed procedures under the <i>Cyber Annex to the National Response Plan</i>.</p> <p>The lessons learned from these and other exercises will form the building blocks for an NCSD-sponsored National Cyber Exercise, CYBER STORM, planned for November 2005, which is expected to include private-sector, as well as state government, participation.</p>
US-CERT Control Systems Security Center	<p>NCSD established the US-CERT Control Systems Security Center to reduce vulnerabilities and to respond to threats to control systems. The center compiled a list of the control system technologies in use, including the underlying platforms, so that the US-CERT could rapidly identify the impact of cyber vulnerabilities on control systems.</p>
Internet Disruption Working Group	<p>In order to coordinate cybersecurity contingency plans, including a plan for recovering key Internet functions, DHS formed the Internet Disruption Working Group. Among other things, this group is to determine the operational dependency of critical infrastructure sectors on the Internet, assess the consequences of the loss of Internet functionality, and work with stakeholders to identify and prioritize short-term protective measures and reconstitution measures to be used in the event of a major disruption.</p>

Source: GAO analysis of DHS information.

^aA tabletop exercise is a focused practice activity that places the participants in a simulated situation requiring them to function in the capacity that would be expected of them in a real event. Its purpose is to promote preparedness by testing policies and plans and by training personnel.

While DHS has made clear progress in planning for incident response, key steps remain to be taken in order to fulfill requirements for exercising continuity plans for federal systems and for coordinating the development of government/industry contingency recovery plans for cybersecurity—as recommended in the cyberspace strategy. Specifically, DHS does not yet have plans (or associated performance measures or milestones) for testing federal continuity plans, for recovering key Internet functions, or for providing technical assistance to both private-sector and other government entities as they develop their own emergency recovery plans. Without continuity planning exercises, federal agencies will not be able to coordinate efforts to ensure that the critical functions provided by federal systems would continue during a significant event and that recovery from such an event would occur in an effective and timely manner. In addition, without plans to address the recovery of key Internet functions, it is unclear how recovery would be performed and how federal capabilities could be used to assist with recovery.

In commenting on a draft of this report, NCSD officials stated that although the division is not currently sponsoring any exercises to test other department and agencies' continuity plans or plans for recovering key Internet functions, they are participating in and offering cybersecurity expertise to already existing department and agency exercises that test continuity of operations and plans for recovery.

DHS Has Begun Efforts to Identify and Assess Threats and Vulnerabilities, but Much Remains to Be Done to Complete These Assessments

DHS has participated in national efforts to identify and assess cyber threats and has begun taking steps to facilitate sector-specific vulnerability assessments, but it has not yet completed the comprehensive cyber threat and vulnerability assessments—or the identification of cross-sector interdependencies—that are called for in the cyberspace strategy.

In late 2003 and early 2004, DHS assisted in coordinating the cyber-related issues for the *National Intelligence Estimate of Cyber Threats to the U.S. Information Infrastructure*. The resulting classified document issued in February 2004 details actors (nation-states, terrorist groups, organized criminal groups, hackers, etc.), capabilities, and, where known, associated intent. National intelligence estimates provide America's highest integrated national threat assessment and are used throughout the defense, intelligence, and homeland security communities.

Regarding ongoing threat identification, DHS's Infrastructure Protection Office, Information Analysis Office, and NCSD coordinate efforts on a daily

basis. For example, NCSA works closely with the Information Analysis Office to coordinate the exchange of threat information, discussions of the potential threat to critical infrastructures based on reported information, and the creation of cyber-based intelligence requirements to gather additional information. In addition, as discussed earlier, information is shared between the private sector and the intelligence community through US-CERT. According to NCSA officials, because there are restrictions on the ability of some parts of the intelligence communities to collect information within the United States, information properly shared through US-CERT could help the intelligence community to develop better situational awareness.

DHS has also taken a number of foundational steps toward developing the comprehensive vulnerability assessment mandated by HSPD-7. Three key initiatives are discussed below:

- **Development of a Baseline Methodology for Vulnerability Assessment**—As the designated entity for fulfilling DHS’s responsibility as the sector-specific agency for the IT infrastructure sector, NCSA is currently identifying the IT sector’s critical assets and developing a baseline methodology for performing vulnerability assessments within the sector. To do so, NCSA is studying existing vulnerability assessment methodologies with the idea of developing a flexible baseline methodology that can be used by members of the IT sector who do not yet have established methodologies. An NCSA official stated that a secondary use for this methodology would be as baseline guidance for cyber assessments across the other critical infrastructures, to be carried out by the sector-specific agencies and their sectors.
- **Development of a Cyber Assessment Template**—NCSA is assisting DHS’s Information Analysis and Infrastructure Protection Directorate’s Protective Security Division by developing a cyber assessment template for their “site assistance visits” to be used to assess the security of critical infrastructure facilities. The cyber-related segment of these visits includes an assessment of process control systems, including supervisory control and data acquisition, and business information technology. According to NCSA officials, they have developed the process control template and are currently developing the business information technology template.
- **Development of Sector Guidance**—As the subject matter expert for the cyber aspects of the National Infrastructure Protection Plan and

associated sector-specific plans, NCSD has developed and distributed guidance to assist sector-specific agencies in addressing the cyber components of their sectors.

While NCSD's plans are focused on important issues, it has not yet completed the national cyber threat assessment and the sector vulnerability assessments—or the identification of cross-sector interdependencies—that are called for in the cyberspace strategy. Further, its assessment efforts are still in early stages. For example, according to an NCSD official, efforts to develop a vulnerability assessment methodology for the IT Sector are in early development. As part of its next steps, NCSD plans to involve the private sector in completing the methodology and then give a larger group of stakeholders in the IT Sector an opportunity to review and comment on it. NCSD also plans to assist the IT sector in conducting its cybersecurity-related vulnerability assessment. Once these assessments are complete, NCSD plans to coordinate a thorough analysis of the impact that interdependencies have on sectors and entities within the sectors.

The Interim NIPP and DHS's strategic plan for cybersecurity acknowledge that much remains to be done in the areas of threat and vulnerability assessment. The Interim NIPP recognizes that DHS is responsible for analyzing specific threats, providing threat warnings, and conducting general threat assessments. It also reports that the Information Analysis and Infrastructure Protection Directorate's Office of Infrastructure Protection will conduct vulnerability assessments for a number of purposes, including investigating interdependencies, filling selected gaps, and testing new methodologies. Additionally, one of NCSD's strategic goals is to work with the public and private sectors to reduce vulnerabilities and to minimize the severity of cyber attacks. As part of this goal, NCSD plans to define and execute methodologies to identify critical assets and to identify and assess vulnerabilities. It established a milestone of developing a vulnerability assessment methodology for the IT Sector by the third quarter of fiscal year 2005. However, neither DHS nor NCSD has defined plans, performance measures, or milestones for completing the required national cyber-related threat and sector vulnerability assessments, or for identifying cross-sector interdependencies.

In commenting on a draft of this report, NCSD officials noted that because of the IT sector's recent formation and its complexity, NCSD has not set strict milestones or performance measures for completing plans. NCSD officials noted, however, that milestones have been set for (1) defining the

sector, (2) creating a public/private collaboration mechanism, and (3) developing methodologies for identifying assets and vulnerability assessments. NCSO officials stated that these steps must be fulfilled in order to ensure accurate assessments and to identify cross-sector interdependences.

Performing infrastructure sector-level vulnerability assessments and developing related remedial plans have been long-standing issues that were identified as requirements in Presidential Decision Directive 63 in 1998. From a planning perspective, it is important to perform comprehensive vulnerability assessments of all of our nation's critical infrastructures because such assessments can enable authorities to evaluate the potential effects of an attack on a given sector and then invest accordingly to protect that sector. Without a vulnerability assessment and remedial plan, it will be difficult to know with any certainty that those vulnerabilities that could cause the greatest harm—or are most likely to be exploited— have been addressed. In September 2001, we reported that substantive, comprehensive analysis of infrastructure sector vulnerabilities and the development of remedial plans had not yet been performed because sector coordinators were still establishing the necessary relationships, identifying critical assets and entities, and researching and identifying appropriate methodologies.¹⁹ In May 2004, we reported that some sectors had taken steps to perform sector-wide vulnerability assessments or to require individual entities to perform vulnerability assessments for their facilities and operations.²⁰ However, others—including the IT sector—still have not taken such actions. Until a comprehensive threat assessment and sector-specific vulnerability assessments are completed and cross-sector dependencies are identified, DHS cannot ensure that all threats and vulnerabilities have been identified and addressed.

In commenting on a draft of this report, NCSO officials stated that because of the IT sector's recent formation and its complexity, NCSO and the sector face challenges in defining the sector, developing effective partnerships, and identifying critical assets. The officials also stated that significant progress has been made in developing methodologies to identify assets and assess vulnerabilities in the IT sector; however, continued collaborative

¹⁹GAO, *Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-822 (Washington, D.C.: Sept. 20, 2001).

²⁰GAO-04-321.

efforts are necessary to ensure that all threats and vulnerabilities are identified and addressed.

DHS Has Several Threat and Vulnerability Reduction Efforts Under Way, but More Action Is Needed

DHS has initiated efforts to reduce threats by enhancing its collaboration with the law enforcement community and to reduce vulnerabilities by shoring up guidance on software and system security, but much remains to be done.

To support efforts to reduce cyber threats, NCSD has restructured its organization to improve its coordination with the law enforcement community and has initiated numerous outreach initiatives. Specifically, NCSD restructured its organization to establish a law enforcement and intelligence branch. It currently has representatives from the cyber components of five different agencies: the National Security Agency, U.S. Immigration and Customs Enforcement, U.S. Secret Service, Federal Bureau of Investigation, and Central Intelligence Agency. This branch provides an information-sharing mechanism among the intelligence, law enforcement, and network security communities. For example, there have been at least two instances where the intelligence community had discovered cyber-related issues that it wanted to report to the public, but it was unable to do so because it would potentially reveal sources and methods, according to an NCSD official. In those cases, NCSD and the intelligence community collaborated to develop and release a public alert that conveyed the threat without revealing sensitive information. In addition, the law enforcement and intelligence branch has provided information from the law enforcement community to the intelligence community. For example, according to an NCSD official, in August 2004, the organization received information about a potential software vulnerability from a law enforcement partner that it shared with the intelligence community.

Additionally, NSCD's law enforcement and intelligence branch has taken steps to improve its domestic and international outreach efforts to support threat reduction; and, according to an NCSD official, the interaction and coordination among the branch and other agencies on cyber-related issues have been effective. Key outreach initiatives include the following:

- Within the federal government, NCSD's law enforcement and intelligence branch has developed a relationship with other law enforcement entities, including entities within the Departments of Energy and Defense and the federal inspector general community.

-
- DHS supports the Cybercop Portal, which is 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. At the time of our review, according to an NCSD official, there were over 6,000 members from the 50 states, most government agencies, and over 40 countries.
 - According to an NCSD official, NCSD has entered into a partnership with the Department of Justice's Bureau of Justice Statistics to conduct a joint survey to study the amount and scope of cyber crime in the United States. The survey will be distributed to 36,000 businesses, including small businesses covering all critical infrastructure sectors.
 - NCSD is reviewing the possibility of enhancing the U.S. computer crime statute (18 U.S.C. 1030). Specifically, according to NCSD officials, it is trying to determine the effect of criminalizing the development and possession (with criminal intent) of malicious computer code, such a change would provide law enforcement with a proactive mechanism to address certain cyber crimes. NCSD has entered into preliminary discussions with the Department of Justice's Computer Crimes and Intellectual Property Section and with other federal, state, and local law enforcement agencies. In addition, NCSD has solicited opinions from the private sector and from academia.

To reduce vulnerabilities, NCSD is encouraging the development of better quality and more secure software. It has established a plan targeting four areas: (1) people (including software developers and users), (2) processes (including best practices and practical software development guidelines), (3) software evaluation tools, and (4) acquisition—creating software security improvements through acquisition specifications and guidelines. To accomplish its plans, NCSD has undertaken the following initiatives:

- NCSD has hosted and cohosted various forums and workshops that focused on topics such as developing a common body of knowledge for software assurance and improving the quality, reliability, and dependability of software. For example:
 - NCSD has hosted three workshops, with subject matter experts from academia and the private sector, to begin the process of developing a common body of knowledge on software assurance that could be used by educators across the country to develop curricula for

academic programs in software engineering, information assurance, and various other disciplines.

- DHS and the Department of Defense have cosponsored two Software Assurance Forums to bring together representatives from industry, government, and academia to address the challenges in software security and quality.
- NCSA is inventorying existing software assurance-related efforts in public and private industry to develop and publish practical guidance, reference materials, and best practices for training software developers.
- NCSA is conducting a software assurance security tools evaluation to support and promote the development of technological advances in software assurance. In coordination with the National Institute of Science and Technology, NCSA has created a set of studies and experiments to measure the effectiveness of various tools and classes of tools.
- NCSA is working with the Department of Defense and other government agencies to examine successful models and to develop and publish best practices for acquisition language and evaluation. NCSA also is working to develop and publish common or sample statement of work/procurement language, which includes provisions on liability, for federal acquisition managers.
- According to an NCSA official, the organization has also formed a working group to address the issue of preventing a major disruption on the Internet. The working group is composed of federal agencies with an interest in preventing a major interruption on the Internet. These agencies are the Department of the Treasury, the Department of Defense, the National Communication System, and NCSA (including US-CERT and CERT/CC). The working group has also tried to include key private-sector individuals. The group's initiatives include efforts to (1) create various scenarios for disruptions in order to determine whom to work with to solve the problem, how to respond and what to do, and what protective measures should be put in place; and (2) determine what infrastructure sectors are functionally dependent on the Internet.

While NCSA has many efforts under way to coordinate threat reduction activities, it is limited in what it can do on vulnerability reduction until the cyber-related vulnerability assessments (discussed in the previous section)

are completed. Since DHS is now planning a methodology for conducting vulnerability assessments, it will likely be some time before stakeholders can conduct the assessments—and even longer before they are able to develop a comprehensive plan for reducing vulnerabilities.

In its strategic plan for cybersecurity, DHS acknowledges that there is more to do to coordinate both threat and vulnerability reduction efforts. Specifically, NCSA has established a strategic goal to coordinate with the intelligence and law enforcement communities to identify and reduce threats to cyberspace. As part of this goal, NCSA identified a number of actions to improve the available information on cyber incidents, publish the results of the planned cyber incident survey, improve the Cybercop Portal, and reach out to other law enforcement entities. Regarding vulnerability reduction, NCSA has established a goal to reduce vulnerabilities and a list of action items, including actions to improve the security within the IT infrastructure sector; to address cybersecurity issues for control systems; to improve software assurance efforts; and to promote cybersecurity standards and best practices.

DHS Is Collaborating on Cybersecurity Research and Development, but a Comprehensive Plan and Associated Milestones are Not Yet in Place

DHS is collaborating with the Executive Office of the President's Office of Science and Technology Policy and with many other federal departments and agencies, including the Departments of Agriculture, Commerce, Defense, and Energy, to develop a national research and development plan for CIP, including cybersecurity. However, a complete plan is not yet in place, and the milestones for key activities under this plan have not yet been developed.

NCSA coordinates with DHS's Science and Technology Directorate to develop (1) the Cyber Security Research and Development Portfolio and (2) the CIP Portfolio that targets process control system security and includes some research and development projects. Research programs include efforts to develop operational analysis tools to enhance the security of domain name systems, establish secure routing protocols, and improve Internet security. In addition, NCSA participates in the Critical Information Infrastructure Protection Interagency Working Group, which is cochaired by the Executive Office of the President's Office of Science and Technology Policy and DHS's Science and Technology Directorate, to identify critical cyber research and development requirements for inclusion in the federal research and development effort. As part of this requirement identification process, NCSA determines where the private sector has already done research and development, in order to minimize overlap and

wasted effort. An NCSO official reports that requirements come from software developers and from the agency's work with industry, academia, and other government agencies.

Although DHS is working to identify cyber research requirements and to support and coordinate cybersecurity-related research and development projects, the working group cochaired by DHS and the Executive Office of the President's Office of Science and Technology Policy that was required to lead the effort to issue a national research and development plan for CIP (including cybersecurity) has not yet developed a comprehensive plan. Also, while the Interim NIPP acknowledges the importance of research and development to a variety of cybersecurity initiatives—including improving Internet security protocols and developing a next generation security architecture featuring autonomic, self-aware, and self-healing systems—it does not identify goals or milestones associated with developing a prioritized plan for these initiatives.

In commenting on a draft of this report, DHS Science and Technology Directorate officials stated that the first public version of the national research and development plan supporting CIP had recently been released.²¹ They acknowledged, however, that this is a baseline plan and does not include an investment plan and road map that are to be added next year. In addition, these officials commented that milestones have not yet been established because planning activities are in progress.

DHS Has Made Progress in Implementing an Awareness and Outreach Strategy, but More Remains to Be Done

DHS has made progress in increasing cybersecurity awareness by implementing numerous awareness and outreach initiatives, but the effectiveness of its activities is unclear because many CIP stakeholders are still uncertain of DHS's cybersecurity roles. Table 10 identifies key DHS awareness and outreach initiatives.

²¹The Executive Office of the President, Office of Science and Technology Policy and The Department of Homeland Security Science and Technology Directorate, *The National Plan for Research and Development In Support of Critical Infrastructure Protection*, 2004 (Washington, D.C.: Apr. 8, 2005).

Table 10: DHS Cybersecurity Awareness and Outreach Initiatives

Initiative	Description
National Cyber Alert System	DHS established the National Cyber Alert System (NCAS) to deliver targeted, timely, and actionable information to the public on how to secure computer systems. Information provided by the alert system is designed to be understandable by all computer users, both technical and nontechnical. More than 270,000 users have subscribed to the system and are receiving regular alerts and updates that enhance their ability to prepare for, mitigate, and respond to adverse cyber events. To date, NCAS has issued several alerts as well as “best practices” and “how-to” guidance messages. In addition, its “cyber tips” help to educate home users on basic security practices and increase overall awareness.
US-CERT public Web site	DHS manages the US-CERT public Web site, which provides information on cyber incidents and cybersecurity. According to NCSD officials, it receives about 3.5 million hits per month.
National Cyber Security Awareness Month	DHS partnered with the public and private sector to establish October as the National Cyber Security Awareness Month and participated in activities to raise awareness of cybersecurity nationwide.
Webcasts	In partnership with the Multi-State ISAC, NCSD has hosted a series of national Webcasts that examine critical and timely cybersecurity issues. The Chair of the Multi-State ISAC stated that the recent Webcasts have been viewed by over 3,000 individuals from nine countries.
National Cyber Security Alliance/ <i>StaySafeOnline</i> Program	DHS, along with other federal and private sector organizations, sponsors the National Cyber Security Alliance, a public/private partnership to promote cybersecurity and safe behavior online. It provides tools and resources through the <i>StaySafeOnline</i> program, a Web site for home users, small businesses, and educational institutions.
Cybersecurity awareness brochures	NCSD is developing informational materials to promote cybersecurity awareness, including brochures, fact sheets, and an electronic newsletter.

Source: GAO analysis of DHS information.

Although DHS has an active awareness and outreach program under way, more remains to be done to expand awareness of the department’s roles, responsibilities, and capabilities. Multiple CIP stakeholders have reported that they were unaware of DHS’s cybersecurity responsibilities. For example, officials from one federal agency indicated they have not independently interacted with NCSD about their sector’s cybersecurity efforts. In addition, at a recent regional security exercise, state and local government officials were not clear on DHS’s role in cybersecurity. NCSD acknowledges that it has more to do to expand awareness of its cybersecurity roles and capabilities and to increase its outreach efforts. In its strategic plan for cybersecurity, DHS has outlined goals, objectives, activities, and milestones for improving in these areas.

DHS Has Made Progress in Its Efforts to Encourage Cybersecurity Education but Lags in Developing Certification Standards

DHS has initiated multiple efforts to improve the education of future cybersecurity analysts, but much work remains to be done to develop certification standards. Key DHS cyber education initiatives are listed in table 11.

Table 11: Key Initiatives in Cybersecurity Education

Initiative	Description
National Centers of Academic Excellence in Information Assurance	DHS and the National Security Agency cosponsor the National Centers of Academic Excellence in Information Assurance Program to reduce vulnerabilities in our national information infrastructure by promoting higher education in information assurance and producing a growing number of professionals with information assurance expertise in various disciplines. Under this program, 4-year colleges and graduate-level universities are eligible to apply to be designated as a National Center of Academic Excellence in Information Assurance Education. Colleges and universities that achieve this designation receive formal recognition from the U.S. government and are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program.
Scholarship for Service program	DHS and the National Science Foundation cosponsor the Scholarship for Service program, which is also known as the Cyber Corps program. This program provides scholarship grant money to selected universities to fund the final 2 years of student bachelors, masters, or doctoral study in information assurance.
Job Fair	In January 2005, DHS, the National Science Foundation, the federal Chief Information Officers Council, and the Office of Personnel Management cosponsored the first annual winter job fair for Scholarship for Service students in Washington, D.C. Approximately 300 students attended the job fair, representing all 26 of the colleges and universities within the Scholarship for Service program. Twenty-nine federal agencies and national laboratories, including DHS's Information Analysis and Infrastructure Protection Directorate and the Office of the Chief Information Officer, the Central Intelligence Agency, the Department of Agriculture, the National Aeronautics and Space Administration, and the Idaho National Engineering and Environmental Laboratory, attended the job fair and interviewed students.

Source: GAO analysis of DHS information.

While DHS has made progress in expanding education and training in cybersecurity, it has more to do to develop baseline standards for cybersecurity certification. According to NCSA's progress report, each cyber-related industry certification currently is based on a different notion of what tasks information assurance employees perform. This leads to confusion on the part of employers when they attempt to assess what skill set they are getting when they hire a certified professional. DHS acknowledges this issue and has begun to take steps to address it. Specifically, DHS has partnered with the Department of Defense on an

initiative to create a national-level job task analysis and information assurance professional skill standards. The job task analysis and skill standards are expected to identify the knowledge, skills, and abilities associated with information assurance jobs across all sectors, and to provide a clear baseline for comparing and evaluating existing industry certifications and developing future certifications. The final goal is to produce a job task analysis and skill standard that reflects all sectors, is national in scope, and can be used to compare existing professional certifications and provide for future certifications.

In addition, in its strategic plan for cybersecurity, DHS identifies a number of actions and milestones for making progress in cybersecurity education, including promoting the creation of widely recognized, industry-led, vendor-neutral cybersecurity professional certifications based on a nationally recognized skill baseline.

DHS Interacts with Other Entities to Enhance Intergovernmental Cybersecurity, but Concerns Exist about the Scope and Effectiveness of These Efforts

DHS supports multiple interagency groups' efforts to improve government cybersecurity through communication and collaboration, but state and local government stakeholders have expressed concerns about the scope of these efforts.

DHS participates in numerous initiatives to enhance intergovernmental coordination. Key initiatives are listed in table 12.

Table 12: DHS’s Intergovernmental Cybersecurity Initiatives

Initiative	Description
Chief Information Security Officers Forum	<p>NCSO created the Chief Information Security Officers Forum to “bring together federal officials responsible for the information security of their respective agencies” and provide a “trusted venue for them to collaborate, leverage one another’s experiences, capabilities and programs, lessons learned, and address and discuss particularly problematic or challenging areas.” This forum has established working groups to study and draft best practices for specific areas of concern, such as patch management.</p>
National Cyber Response Coordination Group (NCRCG)	<p>The National Cyber Response Coordination Group was formalized in the Cyber Annex of the National Response Plan and is cochaired by NCSO, the Department of Justice’s Computer Crime and Intellectual Property Section, and the Department of Defense. It brings together agency management for response purposes during a significant national incident. The group coordinates intragovernmental and public/private preparedness and response to and recovery from national level cyber incidents and physical attacks that have significant cyber consequences. During such an incident, the NCRCG’s senior level membership is responsible for ensuring that the full-range of federal capabilities are deployed in a coordinated and effective fashion. NCRCG includes members from national security, law enforcement, defense, intelligence, and other government agencies.</p>
Government Forum of Incident Response and Security Teams (GFIRST)	<p>GFIRST is a group of technical and tactical practitioners of government agency security response teams responsible for securing government information technology systems.</p>
Federal Information Notice	<p>NCSO established Federal Information Notices to disseminate information to relevant federal authorities, such as federal chief information officers, federal chief information security officers, information system security managers and officers, system administrators, and other federal employees and contractors. The notices are to help keep federal agencies and departments aware of emerging threats and vulnerabilities, as well as to provide them with the information needed to mitigate, respond to, and recover from cyber attacks. DHS reports that the notices provide warnings of Internet security problems and offer explanations of potential problems that have not yet become serious enough to warrant public alert.</p>
Office of Management and Budget’s Security Line of Business Group	<p>NCSO is the cochair of the Office of Management and Budget’s recently formed security line of business effort. It is an effort to raise the level of cybersecurity posture of federal agencies and save funds by coming up with common security solutions across the government.</p>
Coordination with states	<p>DHS interacts with state governments through the Multi-State ISAC. Formed in 2003, this ISAC provides a central resource for gathering information on cyber threats to critical infrastructure from the states and providing two-way sharing of information between and among the states and ultimately with local government. The Multi-State ISAC also analyzes information and intelligence to support readiness and response efforts by federal, state, and local first responders and law enforcement. DHS, including NCSO, DHS’s Office of State and Local Government Coordination, and US-CERT, are included in this ISAC’s monthly conference calls. The ISAC also partners with NCSO on a national Webcast for increased awareness and education. Multi-State ISAC officials reported that DHS provides information that is useful and actionable for the state government sector.</p>
	<p>In addition, NCSO cosponsored a State of the State Conference with the National White Collar Crime Center that brought together state cyber enforcement officials to discuss (1) cyber activities in their respective states, (2) successful and unsuccessful mechanisms used to address cyber activities, and (3) ways that NCSO can assist states in their cybersecurity activities.</p>

(Continued From Previous Page)

Initiative	Description
Incident support	DHS supports individual government entities, providing resources and expertise during major incidents. For example, according to NCSD officials, the organization recently provided direct support to a state that had suffered a serious cybersecurity incident. NCSD's support included sending a team of experts to provide on-site resources, coordinating with federal law enforcement and intelligence communities, and providing advice for security practice improvements. In addition, NCSD officials stated that they had provided similar support to federal agencies.

Source: GAO analysis of DHS information.

While DHS has made concerted efforts to form and support intergovernmental partnerships, several governmental entities have expressed concerns about the scope of these efforts and their effectiveness. For example, officials representing a state government organization noted that DHS has not provided adequate attention to the states regarding cybersecurity and has not included local government IT officials in cybersecurity-related discussions. State officials also noted that DHS's focus on cybersecurity has been secondary to its physical security efforts; for example, there have been only limited grants to assist states with cybersecurity. As a result, these representatives have reported that there is a "fundamental lack of appreciation" for cybersecurity by state and local governments.

The Interim NIPP and DHS's strategic plan for cybersecurity acknowledge the importance of continually enhancing the security of federal, state, and local government systems through partnerships and information sharing. For example, the Interim NIPP includes a goal to build partnerships with federal, state, local, tribal, international, and private-sector stakeholders to implement CIP programs. In addition, DHS's strategic plan for cybersecurity establishes goals, objectives, and actions that involve securing governments' cyberspace through collaboration with key stakeholders in other federal, state, and local governments and in the private sector.

DHS Has Initiated Efforts in the International Community, but More Remains to Be Done

DHS is working in conjunction with other governments to promote a global culture of security but acknowledges that more remains to be done to accomplish its goals.

In recent years, NCSD has participated with its international counterparts in several initiatives to improve interaction and coordination. Table 13 lists

key international cybersecurity initiatives, including multilateral and bilateral efforts.

Table 13: International Cybersecurity Initiatives

	Description
Multilateral initiatives	
Cybersecurity Collaboration with Close Allies	NCSD established and chaired three international information sharing conference calls with government cybersecurity policymakers and emergency response operations representatives from United States, United Kingdom, Australia, Canada, and New Zealand. The purpose of these calls was to share information and to establish cooperation to help participants prepare for and manage cyber incidents globally, improve overall situational awareness, and foster collaborative efforts on common strategic initiatives. According to NCSD officials, these calls led to the five countries agreeing to undertake a collaborative effort on cybersecurity/critical information infrastructure protection.
Asia Pacific Economic Committee	NCSD actively participates in the Committee's Telecommunications Working Group, which has engaged in (1) an outreach program to educate member countries about computer emergency response teams and (2) a capacity-building program to provide training to member countries as they develop their own computer emergency response teams.
G-8 High Tech Crime Working Group	NCSD participates in the G-8 High Tech Crime Working Group. For example, it sent representatives as part of the U.S. delegation to the G-8 sponsored International Exercise in New Orleans in May 2005.
Organization of American States	NCSD participates in the Organization of American States' work program on cybersecurity, including a cybersecurity practitioners' workshop that was held in March 2005. The program is working toward building computer emergency response capabilities and an information sharing and watch and warning framework in the hemisphere.
International Watch and Warning Framework/Multilateral Conference	NCSD developed and organized a multilateral conference in Berlin, Germany, which was cohosted by DHS and the German Ministry of Interior in October 2004. The conference brought together cybersecurity policy, operations, and law enforcement representatives from 15 countries ^a to discuss vision, challenges, and watch and warning models and to consider establishing an international watch and warning framework. The conference included interactive discussions and a cyber tabletop exercise, and resulted in a set of intermediate agreements for information sharing and future work toward a more mature framework. As a follow up, a working group of the participating countries met in Paris in March 2005 to pursue the action plan from the conference and to take steps to build an International Watch and Warning Network.
Bilateral initiatives	
Canada and Mexico	NCSD has partnered with counterpart agencies in Canada and Mexico to launch new Cyber Security Working Groups to address critical information infrastructure issues of mutual concern, under the CIP Framework for Cooperation efforts with both Canada and Mexico, which are known as the Smart Border Action Plan and Border Partnership Action Plan, respectively.

(Continued From Previous Page)

	Description
US-India Cyber Security Forum	NCSD participates in the U.S.-India Cyber Security Forum, established in 2002. In addition, the forum created a new Watch, Warning, and Emergency Response Working Group to reflect collaboration between US-CERT and the newly established CERT-India. According to NCSD officials, the working group's action plan includes information-sharing objectives to improve situational awareness and incident response abilities between the United States and India, and to share experience and expertise on computer emergency response.
U.S.-United Kingdom Joint Contact Group	NCSD participates in the U.S.-United Kingdom Joint Contact Group, established between DHS and the United Kingdom's Home Office. According to NCSD officials, its action plan for cybersecurity includes information sharing and collaboration on watch and warning, threat analysis, incident response, exercise, and outreach efforts.

Source: GAO analysis of DHS information.

^aParticipating countries included Australia, Canada, Finland, France, Germany, Hungary, Italy, Japan, Netherlands, New Zealand, Norway, Sweden, Switzerland, United Kingdom, and the United States.

While NCSD has initiated numerous outreach and coordination efforts with the international community, important actions remain ahead. DHS's strategic plan for cybersecurity includes two objectives related to national security and international cyberspace security cooperation, to (1) create and pursue an international strategy to secure cyberspace and (2) promote collaboration, coordination, and information sharing with international communities. In addition, NCSD's January 2005 progress report described plans to work with its counterparts in Australia, Canada, New Zealand and the United Kingdom "to formulate a framework for on-going policy and operational cooperation and collaboration" that will "incorporate shared efforts on key strategic issues to address cybersecurity over the long term, including software assurance, research and development, attribution, control systems, and others." This framework is expected to enhance the allies' current information-sharing and incident-response efforts and to foster collaboration in other international activities.

In commenting on a draft of this report, DHS Science and Technology Directorate officials stated that the directorate had entered into international agreements with Canada and the United Kingdom for collaborative science and technology activities and had engaged in bilateral meetings with those countries on the topic of cybersecurity research and development.

NCSD Is Working to Integrate Cybersecurity with National Security, but Important Testing Remains to Be Done

DHS formed the National Cyber Response Coordination Group to coordinate the federal response to cyber incidents of national significance. It is a forum of national security, law enforcement, defense, intelligence, and other government agencies that coordinates intragovernmental and public/private preparedness and response to and recovery from national-level cyber incidents and physical attacks that have significant cyber consequences. During a significant national incident, the coordinating group's senior level membership is responsible for ensuring that the full range of federal capabilities are deployed in a coordinated and effective fashion. However, at the time of our review, there had not been a cyber incident of national significance to activate these procedures, and, according to NCSD officials, early tests of this coordination identified some lessons and showed the need to make improvements. For example, officials learned that they need to improve communication protocols and mechanisms.

DHS Continues to Face Challenges in Establishing Itself as a National Focal Point for Cyberspace Security

DHS faces a number of challenges that have impeded its ability to fulfill its cyber CIP responsibilities. Key challenges include achieving organizational stability; gaining organizational authority; overcoming hiring and contracting issues; increasing awareness about cybersecurity roles and capabilities; establishing effective partnerships with stakeholders (other federal, state, and local governments and the private sector); achieving two-way information sharing with these stakeholders; and providing and demonstrating the value DHS can provide.

Organizational stability: Over the last year, multiple senior DHS cybersecurity officials—including the NCSD Director, the Deputy Director responsible for Outreach and Awareness, and the Director of the US-CERT Control Systems Security Center, the Under Secretary for the Information Analysis and Infrastructure Protection Directorate and the Assistant Secretary responsible for the Information Protection Office—have left the department. Infrastructure sector officials stated that the lack of stable leadership has diminished NCSD's ability to maintain trusted relationships with its infrastructure partners and has hindered its ability to adequately plan and execute activities. According to one private-sector representative, the importance of organizational stability in fostering strong partnerships cannot be over emphasized.

Organizational authority: NCSD does not have the organizational authority it needs to effectively serve as a national focal point for

cybersecurity. Accordingly, NCSO officials lack the authority to represent and commit DHS to efforts with the private sector. Infrastructure and cybersecurity officials, including the chairman of the sector coordinators and representatives of the cybersecurity industry, have expressed concern that the NCSO's relatively low position within the DHS organization hinders its ability to accomplish cybersecurity-related goals. NCSO's lack of authority has led to some missteps, including DHS canceling an important cyber event without explanation and taking almost a year to issue formal responses to private sector recommendations resulting from selected National Cyber Security Summit task forces—even though responses were drafted within months.

A congressional subcommittee also expressed concern that DHS's cybersecurity office lacks the authority to effectively fulfill its role. In 2004, the subcommittee proposed legislation to elevate the head of the cybersecurity office to an assistant secretary position. Among other benefits, the subcommittee reported that such a change could

- provide more focus and authority for DHS's cybersecurity mission,
- allow higher level input into national policy decisions, and
- provide a single visible point of contact within the federal government to improve interactions with the private sector.

Hiring and contracting: Ineffective DHS management processes have impeded the department's ability to hire employees and maintain contracts. We recently reported that since its inception, DHS's leadership has provided a foundation for maintaining critical operations while undergoing transformation.²² However, in managing its transformation, we noted that DHS still needed to overcome a number of significant challenges, including addressing systemic problems in human capital and acquisition systems. Federal and nonfederal officials expressed concerns with DHS's hiring and contracting processes. For example, an NCSO official reported that the division has had difficulty in hiring personnel to fill vacant positions. These officials stated that once they found qualified candidates, some candidates decided not to apply and another withdrew his acceptance because they felt that the DHS hiring process took too long. In addition, an NCSO official stated that there had been times when DHS did not renew NCSO contracts

²²[GAO-05-207](#).

in a timely manner, requiring that key contractors work without pay until approvals could be completed and payments could be made. In other cases, NCSO was denied services from a vendor, because DHS had repeatedly failed to pay for its services. External stakeholders, including an ISAC representative, also noted that NCSO is hampered by how long it takes DHS to award a contract.

Awareness of DHS roles and capabilities: Many infrastructure stakeholders are not yet aware of DHS's cybersecurity roles and capabilities. Department of Energy critical infrastructure officials stated that the roles and responsibilities of DHS and the sector-specific agencies need to be better clarified in order to improve coordination. In addition, during a regional cyber exercise, private-sector and state and local government officials reported that the mission of NCSO and the capabilities that DHS could provide during a serious cyber-threat were not clear to them. NCSO's manager of cyber analysis and warning operations acknowledged that the organization has not done an adequate job in reaching out to the private sector regarding DHS's role and capabilities.

Effective partnerships: NCSO is responsible for leveraging the assets of key stakeholders, including other federal, state, and local governments and the private sector, in order to facilitate effective protection of cyber assets. The ability to develop partnerships greatly enhances the agency's ability to identify, assess, and reduce cyber threats and vulnerabilities, establish strategic analytical capabilities, provide incident response, enhance government cybersecurity, and improve international efforts. According to one infrastructure sector representative, effective partnerships require building relationships with mutually developed goals, shared benefits and responsibilities, and tangible, measurable results. However, this individual reported that DHS has not typically adopted these principles in pursuing partnerships with the private sector, which dramatically diminishes cybersecurity gains that government and industry could otherwise achieve. For example, DHS has often informed the infrastructure sectors about government initiatives or sought input after most key decisions have been made. Also, DHS has not demonstrated that it recognizes the value of leveraging existing private sector mechanisms, such as information-sharing entities and processes already in place and working. In addition, the instability of NCSO's leadership positions to date has led to problems in developing partnerships. Representatives from two ISACs reported that turnover at NCSO has hindered partnership efforts. Additionally, IT sector representatives stated that NCSO needs continuity of leadership, regular

communications, and trusted policies and procedures in order to build the partnerships that will allow the private sector to share information.

Information sharing: We recently identified information sharing in support of homeland security as a high-risk area, and we noted that establishing an effective two-way exchange of information to help detect, prevent, and mitigate potential terrorist attacks requires an extraordinary level of cooperation and perseverance among federal, state, and local governments and the private sector.²³ However, such effective communications are not yet in place in support of our nation's cybersecurity. Representatives from critical infrastructure sectors stated that entities within their respective sectors still do not openly share cybersecurity information with DHS. As we have reported in the past, much of the concern is that the potential release of sensitive information could increase the threat to an entity. In addition, sector representatives stated that when information is shared, it is not clear whether the information will be shared with other entities, such as other federal entities, state and local entities, law enforcement, or various regulators, or how it will be used or protected from disclosure. Representatives from the banking and finance sector stated that the protection provided by the Critical Infrastructure Information Act and the subsequently established Protected Critical Infrastructure Information Program is not clear and has not overcome the trust barrier. Alternatively, sector representatives have expressed concerns that DHS is not effectively communicating information with them. According to one infrastructure representative, DHS has not matched private sector efforts to share valuable information with a corresponding level of trusted information sharing. An official from the water sector noted that when representatives called DHS to inquire about a potential terrorist threat, they were told that DHS could not share any information and that they should "watch the news."

Providing value: According to sector representatives, even when organizations within their sectors have shared information with NCSID, the entities do not consistently receive useful information in return. They noted that without a clear benefit, they are unlikely to pursue further information sharing with DHS. Federal officials also noted problems in identifying the value that DHS provides. According to Department of Energy officials, DHS does not always provide analysis or reports based on the information that agencies provide. Federal and nonfederal officials also

²³[GAO-05-207](#).

stated that most of US-CERT's alerts have not been useful because the alerts lack essential details or have been based on already available information. Further, Treasury officials stated that US-CERT needed to provide relevant and timely feedback regarding the incidents reported to it.

Clearly, these challenges are not mutually exclusive. That is, addressing challenges in organizational stability and authority will help NCSD build the credibility it needs in order to establish effective partnerships and achieve two-way information sharing. Similarly, effective partnerships and ongoing information sharing with its stakeholders will allow DHS to better demonstrate the value it can add.

DHS has identified steps in its strategic plan for cybersecurity that can begin to address these challenges. Specifically, DHS has established goals and plans for improving human capital management, which should help stabilize the organization. Further, DHS has developed plans for communicating with stakeholders, which are intended to increase awareness of its roles and capabilities and to encourage information sharing. Also, DHS has established plans for developing effective partnerships and improving analytical and watch and warning capabilities, which could help build partnerships and begin to demonstrate added value. However, until it begins to address these underlying challenges, DHS cannot achieve significant results in coordinating cybersecurity activities and our nation will lack the effective focal point it needs to better ensure the security of cyberspace for public and private critical infrastructure systems.

Conclusions

As our nation has become increasingly dependent on timely, reliable information, it has also become increasingly vulnerable to attacks on the information infrastructure that supports the nation's critical infrastructures (including the energy, banking and finance, transportation, telecommunications, and drinking water infrastructures). Federal law and policy acknowledge this by establishing DHS as the focal point for coordinating cybersecurity plans and initiatives with other federal agencies, state and local governments, and private industry. DHS has made progress in planning and coordinating efforts to enhance cybersecurity, but much more work remains to be done to fulfill its basic responsibilities—including conducting important threat and vulnerability assessments and recovery plans.

As DHS strives to fulfill its mission, it faces key challenges in building its credibility as a stable, authoritative, and capable organization and in leveraging private/public assets and information in order to clearly demonstrate the value it can provide. Until it overcomes the many challenges it faces and completes critical activities, DHS cannot effectively function as the cybersecurity focal point intended by law and national policy. As such, there is increased risk that large portions of our national infrastructure are either unaware of key areas of cybersecurity risks or unprepared to effectively address cyber emergencies.

Recommendations for Executive Action

In order to improve DHS's ability to fulfill its mission as an effective focal point for cybersecurity, we recommend that the Secretary of Homeland Security implement the following three steps:

- engage appropriate stakeholders to prioritize key cybersecurity responsibilities so that the most important activities are addressed first, including responsibilities that are not detailed in the cybersecurity strategic plan: (1) perform a national cyber threat assessment; (2) facilitate sector cyber vulnerability assessments—to include identification of cross-sector interdependencies; and (3) establish contingency plans for cybersecurity, including recovery plans for key Internet functions;
- require NCSA to develop a prioritized list of key activities for addressing the underlying challenges that are impeding execution of its responsibilities; and
- identify performance measures and milestones for fulfilling its prioritized responsibilities and for performing activities to address its challenges, and track organizational progress against these measures and milestones.

We are not making new recommendations regarding cyber-related analysis and warning and cybersecurity information sharing at this time because our previous recommendations in these areas have not yet been fully implemented.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from DHS (see app. III). In DHS's response, the Director of the Departmental GAO/OIG Liaison Office stated that DHS agrees that strengthening cybersecurity is central to protecting the nation's critical infrastructures and that much remains to be done. In addition, DHS concurred with our recommendation to engage stakeholders in prioritizing its key cybersecurity responsibilities. The director stated that continued and expanded stakeholder involvement is critical and identified some of NCSA's significant activities—many of which are discussed in the body of this report. However, the director noted that DHS does not agree that the challenges it has experienced have prevented it from achieving significant results in improving the nation's cybersecurity posture. In addition, DHS did not concur with our recommendations to (1) develop a prioritized list of key activities for addressing the underlying challenges and (2) identify performance measures and milestones for fulfilling its prioritized responsibilities and for performing activities to address its challenges and track organizational progress. Specifically, the director reported that DHS already uses a prioritized list, performance measures, and milestones to guide and track its activities and sought additional clarification of these recommendations. The director also noted that our report makes a reference to previous recommendations involving cyber-related information sharing and strategic analysis and warning capabilities that have not been fully implemented, but he disagreed that there were any valid outstanding recommendations.

Because most of the nation's information infrastructure is owned by the private-sector, developing trusted partnerships and information-sharing relationships between the federal government and the private sector are critical. We agree that DHS has initiated many efforts as a focal point for the nation's efforts to secure cyberspace and have acknowledged these in our report, but the challenges it faces—including achieving organizational stability, achieving two-way information sharing with stakeholders, and demonstrating value—have hindered its progress to date. This view was reiterated by the federal and nonfederal stakeholders we interviewed.

Regarding our recommendations, while we agree with DHS that its strategic plan for cybersecurity identifies a number of activities (along with some performance metrics and milestones) that will begin to address the challenges, this plan does not include specific initiatives that would ensure that the challenges are addressed in a prioritized and comprehensive manner. For example, the strategic plan for cybersecurity does not include initiatives to help stabilize and build authority for the organization. Further,

the strategic plan does not identify the relative priority of its initiatives and does not consistently identify performance measure for completing its initiatives. As DHS moves forward in identifying initiatives to address the underlying challenges it faces, it will be important to establish performance metrics and milestones for fulfilling these initiatives. In fact, in its strategic plan for cybersecurity, DHS acknowledges that it needs to establish performance measures and milestones and to collect performance data for its key initiatives.

Regarding our previous recommendations related to information sharing, DHS identified plans for fulfilling our recommendations but did not provide any evidence that these efforts were completed. For example, in November 2004, DHS reported that by June 2005, it planned to develop an information-sharing plan including the elements we recommended; however, DHS has not yet completed this plan and has not provided any evidence that this plan will include the key elements we had recommended. In addition, in regard to our recommendation that DHS develop appropriate policies and procedures for information sharing and coordination within DHS and with other federal and nonfederal entities, DHS reported that it has many information sharing initiatives and high-level documents. However, DHS did not specify any DHS-level policies or procedures for information sharing. NCSA procedures, including the US-CERT Concept of Operations and Standard Operating Procedure, were still in draft at the time of our review. Thus, these recommendations remain open.

As for our previous recommendations to develop a strategic analysis and warning capability, we reported that DHS is still facing the same challenges in developing strategic analysis and warning capabilities that we reported on 4 years ago during a review of NCSA's predecessor. In 2001, we reported that a generally accepted methodology for analyzing strategic cyber-based threats did not exist. We also reported that the center did not have the industry-specific data on factors such as critical systems components, known vulnerabilities, and interdependencies. Therefore, we recommended that responsible executive-branch officials and agencies establish a capability for strategic analysis of computer-based threats, including developing a methodology and obtaining infrastructure data. In response to specific questions on these topics in April 2005, NCSA officials acknowledged that work remains to be done in developing cyber-related strategic analysis and warning capabilities. They stated that there is still no generally accepted methodology for analyzing strategic cyber-based threats and that NCSA is in the process of developing industry-specific data. In addition, these officials discussed a number of ongoing initiatives to

address various aspects of the methodology. Because these efforts are incomplete, our recommendations remain open.

DHS officials as well as others who were quoted in our report also provided technical corrections, which we have incorporated in this report as appropriate.

We are sending copies of this report to interested congressional committees, the Secretary of Homeland Security, and other interested parties. In addition, this report will be available at no charge on GAO's Web site at www.gao.gov.

If you have any questions on matters discussed in this report, please contact me at (202) 512-9286, or by e-mail at pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.



David A. Powner
Director, Information Technology
Management Issues

List of Congressional Requesters

The Honorable Joseph I. Lieberman
Ranking Member
Committee on Homeland Security
and Governmental Affairs
United States Senate

The Honorable Christopher Cox
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Daniel E. Lungren
Chairman
The Honorable Loretta Sanchez
Ranking Member
Subcommittee on Economic Security,
Infrastructure Protection, and Cybersecurity
Committee on Homeland Security
House of Representatives

The Honorable Tom Davis
Chairman
Committee on Government Reform
House of Representatives

The Honorable Mac Thornberry
House of Representatives

The Honorable Zoe Lofgren
House of Representatives

Objectives, Scope, and Methodology

Our objectives were to determine (1) the Department of Homeland Security's (DHS) roles and responsibilities for cyber critical infrastructure protection (CIP) and national information security, as established in law and policy, and determine the specific organizational structures DHS has created to fulfill them; (2) the status of DHS's efforts to protect the computer systems supporting the nation's critical infrastructures and to strengthen information security both inside and outside the federal government and the extent to which such efforts and DHS's organizational structures adequately address its responsibilities; and (3) the challenges DHS faces in fulfilling its cybersecurity roles and responsibilities.

To determine DHS's cyber roles and responsibilities supporting CIP, we analyzed relevant law and policy, including the Homeland Security Act of 2002, Homeland Security Presidential Directive (HSPD) 7, and the *National Strategy to Secure Cyberspace*. Because many of the roles and responsibilities in the law and policies are overlapping, we focused on identifying responsibilities related to cybersecurity that could be used to gauge DHS's progress and grouped them into 13 key responsibilities. We shared the 13 key responsibilities with DHS officials responsible for cybersecurity, and the officials concurred that these are important responsibilities. We also compared the key responsibilities with the activities that DHS identified in its cybersecurity plans and progress reports, to ensure that no key responsibilities were missed. To identify DHS's organizational structure for fulfilling its responsibilities, we analyzed DHS and National Cyber Security Division (NCSA) organizational charts and interviewed DHS officials.

To determine the status and adequacy of DHS's efforts, we analyzed key documents, including the Interim National Infrastructure Protection Plan, NCSA's cyber strategies and plans, and NCSA's policies and procedures, and we interviewed key DHS and NCSA officials. We compared DHS's efforts and plans with the 13 responsibilities to identify what has been accomplished and what more needs to be done. In addition, we gathered documents and performed structured interviews with officials from other federal agencies with established CIP roles. We included officials responsible for each agency's efforts to enhance CIP and the officials responsible for their respective agency's information security efforts. We spoke with officials from the Departments of Agriculture; Energy; Health and Human Services (including the Food and Drug Administration); Justice (including the Federal Bureau of Investigation); the Treasury; and the Environmental Protection Agency. We also interviewed representatives from the following infrastructure sectors: banking and finance, electricity,

water, and information technology. In addition, we interviewed representatives from the Information Sharing and Analysis Center (ISAC) council. We also interviewed officials from entities representing state governments, including the Multi-State ISAC and the National Association of State Chief Information Officers.

To identify the challenges facing DHS and NCSO as they attempt to fulfill their cybersecurity responsibilities, we analyzed our prior work on CIP as well as reports by the cybersecurity industry that offered recommendations for improving cybersecurity and CIP. We also interviewed DHS and NCSO officials, representatives from other federal agencies with CIP roles, infrastructure sector officials, and officials of an organization representing state governments. We also observed a regional infrastructure security tabletop exercise focusing on cybersecurity and identified challenges in achieving effective collaboration among public/private partners from discussions by the participants of this exercise. We performed our work from July 2004 to April 2005 in accordance with generally accepted government auditing standards.

DHS Organizations with Cyber-Related Roles

DHS established NCSA as the primary organization with responsibility for cybersecurity. However, multiple other organizations have roles and responsibilities that impact cybersecurity and require close coordination with NCSA. These include the following offices and suboffices:

- **Information Analysis Office**—which is to provide actionable intelligence essential for preventing acts of terrorism and, with timely and thorough analysis and dissemination of information about terrorists and their activities, improve the federal government’s ability to disrupt and prevent terrorist acts and to provide useful warning to state and local governments, the private sector, and our citizens.
- **Homeland Security Operations Center**—which provides real-time situational awareness and monitoring of the homeland, coordinates incidents and response activities and, in conjunction with the DHS Office of Information Analysis, issues advisories and bulletins concerning threats to homeland security, as well as specific protective measures.
- **Infrastructure Protection Office**—which is to coordinate national efforts to secure America’s critical infrastructure, including vulnerability assessments, strategic planning efforts, and exercises.
 - Infrastructure Protection Office’s **Infrastructure Coordination Division**—which plays a key role in coordinating with sector coordinating mechanisms (e.g., sector coordinating councils and government coordinating councils) concerning information sharing. In addition, it operates the National Infrastructure Coordination Center.
 - Infrastructure Coordination Division’s **Protected Critical Infrastructure Information Program Office**—which was established to encourage private industry and others with knowledge about the nation’s critical infrastructure to share sensitive and proprietary business information about this critical infrastructure with the government in accordance with the Critical Infrastructure Information Act of 2002 (CII Act). Protected CII is designed so that members of the private sector can voluntarily submit sensitive information regarding the nation’s critical infrastructure to DHS with the assurance that the information will be protected from public disclosure as long as it satisfies the requirements of the CII Act.

- Infrastructure Protection Office's **Protective Security Division**—which is to coordinate strategies for protecting the nation's critical physical infrastructure.
- Infrastructure Protection Office's **National Communications System**—which was established by executive order in 1982 as a federal interagency group responsible for national security and emergency preparedness telecommunications and was transferred to DHS by the Homeland Security Act of 2002. Its responsibilities include planning for, developing, and implementing enhancements to the national telecommunications infrastructure, which includes the Internet, to achieve effectiveness in managing and using national telecommunication resources to support the federal government during any emergency. In addition, through the National Coordinating Center for Telecommunications,¹ the National Communications System sponsors the Telecommunications Information Sharing and Analysis Center. The National Communications System is also jointly responsible with NCSA for developing the IT infrastructure sector plan.
- **DHS's Science and Technology Directorate**—which serves as the primary research and development arm of DHS. It uses our nation's scientific and technological resources to provide federal, state, and local officials with the technology and capabilities to protect the homeland. It focuses on catastrophic terrorism—threats to the security of our homeland that could result in large-scale loss of life and major economic impact.
- **Office of State and Local Coordination**—which was established to serve as a single point of contact for facilitation and coordination of departmental programs that impact state, local, territorial, and tribal governments.

¹The National Coordinating Center for Telecommunications is open to companies that provide telecommunications or network services, equipment, or software to the communications and information sector; select, competitive local exchange carriers; Internet service providers; vendors; software providers; telecommunications professional organizations and associations; or companies with participation or presence in the communications and information sector. Membership is also allowed for National Coordinating Center member federal departments and agencies, and for national security/emergency preparedness users.

-
- **Private Sector Office**—which works directly with individual businesses, trade associations, and other professional and nongovernmental organizations to share department information, programs, and partnership opportunities.

Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

May 3, 2005

Mr. David A. Powner
Director, Information Technology
Management Issues
Government Accountability Office
Washington, DC 20548

Dear Mr. Powner:

Re: Draft Report GAO-05-434, Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities.

Thank you for the opportunity to review the draft report. We agree that strengthening cybersecurity is central to protecting the nation's critical infrastructures and concur that much remains to be done. We do not, however, agree with the report's implication that the challenges experienced to date have prevented us from achieving significant results in improving the nation's cybersecurity posture. The recent (January 2005) National Cyber Security Division Progress Report detailed the significant progress that has been made across the broad spectrum of our cybersecurity responsibilities. Nevertheless, we welcome GAO's review and comments on our initial efforts. We note the report also makes a reference to "previous recommendations in these areas." We do not agree that there are any valid, outstanding recommendations in this area. The following represents the Departmental response to the recommendations contained in the draft report.

Recommendation:

Engage with appropriate stakeholders to prioritize key cybersecurity responsibilities so that the most important activities are addressed first, including responsibilities that are not detailed in the cybersecurity strategic plan: (1) perform a national cyber threat assessment, (2) facilitate sector cyber vulnerability assessments—to include identification of cross-sector interdependencies, and (3) establish contingency plans for cybersecurity, including recovery plans for key Internet functions.

Response: Concur. While stakeholder input has already been a contributing factor in the establishment of National Cyber Security Division's (NCSA) priorities, continued and expanded stakeholder involvement is critical in reviewing and revising these priorities in the future. Some of the significant NCSA activities in this area are noted below:

NCSA has made significant progress toward completing comprehensive threat assessments and sector specific vulnerability assessments, but we agree that more must be done. Establishing and formalizing the IT Sector, as the Sector Specific Agency/Responsibility (SSA/R) under the National Infrastructure Protection Plan (NIPP), has been challenging, given its breadth,

www.dhs.gov

Appendix III
Comments from the Department of Homeland
Security

complexity, and relative maturity. It is important to recognize the nature of these challenges, as it helps to understand the considerable progress made to date. The challenges include defining the boundaries of the Sector, developing effective partnerships, and identifying critical IT assets. This work is charting new territory in government and private sector collaboration. Because most of the IT Sector is privately owned, the government must ensure that the collaboration includes all the principal actors and that the collaboration is maintained and strengthened over time.

It is important that the work of the IT Sector be deliberate and comprehensive. Failing to identify and address all threats and vulnerabilities can have serious consequences. However, significant progress has been made, specifically in the development of appropriate IT Sector asset identification and vulnerability assessment methodologies, in establishing the IT Sector Government Coordinating Council (IT-GCC), and assisting the IT Sector in its efforts to establish the IT Sector Coordinating Council (IT-SCC).

For cross-sector interdependencies, NCSA has worked with the Sector Specific Agencies (SSA) to ensure the thoroughness of the cyber aspects of their Sector Specific Plans (SSP), and is improving the IT Sector asset identification and vulnerability assessment methodologies to address SSA cross-sector cyber efforts. NCSA is working with each SSA to ensure the quality and effectiveness of its cyber planning, and to ensure cross-sector consistency. In addition, NCSA has been fully engaged with OMB, as subject matter expert, to ensure the quality, consistency, and effectiveness of the federal agency Critical Infrastructure Protection plans. Lastly, NCSA has established a Control Systems Security program to identify control systems in critical infrastructure across all sectors, to understand their vulnerabilities and interdependencies, and develop and recommend effective near-term protective measures for legacy systems.

With respect to recovery, the Office of Infrastructure Protection (IP) has formed a strategic partnership in the form of the Internet Disruption Working Group (IDWG) that will leverage past efforts of the federal government and the private sector while combining resources and avoiding duplication and conflict. Currently, IDWG is building on past efforts of IP, reaching out to key Internet companies in the private sector, and drawing on US Computer Emergency Readiness Team (US-CERT) resources to determine: (1) the degree of critical infrastructure sectors' business and operational dependency on the Internet; (2) which private sector companies the government needs to work with to prevent a major disruption; and (3) what surge capabilities would be needed to assist the National Cyber Response Coordination Group (NCRCG) in managing a crisis and reconstituting service in the event of a significant disruption. These efforts contribute to and will measure progress through the Interagency Security Planning Effort for FY 2005, within the Risk Management/Protective Measures Working Group of the National Infrastructure Protection Plan Senior Leadership Council.

Recommendation:

Develop a prioritized list of key activities for addressing the underlying challenges that are impeding NCSA's execution of its responsibilities.

Response: Non-concur. NCSA's strategic plan already provides a prioritized list of key activities that are reviewed, updated, and revised on a quarterly basis. Through regular communication with the Assistant Secretary for Infrastructure Protection, obstacles are already being identified and prioritized. This recommendation, as written, does not explain why these

Appendix III
Comments from the Department of Homeland
Security

efforts are insufficient or what specific additional actions GAO would like to see accomplished. Pending further definition of GAO's intent, we non-concur with this recommendation.

Recommendation:

Identify performance measures and milestones for fulfilling its prioritized responsibilities and for performing activities to address its challenges, and track organizational progress against these measures and milestones.

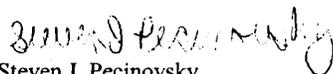
Response: Non-concur. Performance measures and milestones are already identified in NCSD's strategic plan. Unlike organizations that have been in place for a significant period of time, the milestones facing NCSD are primarily the development of new programs and establishment of a system for monitoring the success of these programs. In its initial strategic plan, NCSD has defined milestones that are measurable, although often not in quantitative terms. That is, the initial milestones direct the implementation of programs within a specified period of time, or the implementation of stages in program development in a specified time. The initial measure of success is whether or not the programs got off the ground in a timely manner and are moving ahead on schedule. As the programs become more established, performance measures will increasingly shift towards quantitative measures to evaluate the relative success of the program.

In addition to already having identified its performance measures and milestones in its strategic plan, NCSD has already implemented procedures to systematically track organizational progress. Early in each quarter NCSD program managers are reminded of impending deadlines at the end of the quarter. Action is taken at the start of each quarter to ensure that a milestone is met or that obstacles to success are addressed and overcome.

This recommendation, as written, does not explain why these efforts are insufficient or what specific additional actions GAO would like to see accomplished. Pending further definition of GAO's intent, we non-concur with this recommendation.

We thank you again for the opportunity to review the report and provide comments.

Sincerely,


Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to those named above, Joanne Fiorino, Michael Gilmore, Barbarol James, Colleen M. Phillips, and Nik Rapelje 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