United States Government Accountability Office

GAO

Report to Congressional Requesters

June 2006

INTERNET INFRASTRUCTURE

DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan

GA0-06-672

June 2006

INTERNET INFRASTRUCTURE

DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-672, a report to congressional requesters

Why GAO Did This Study

Since the early 1990s, growth in the use of the Internet has revolutionized the way that our nation communicates and conducts business. While the Internet was originally developed by the Department of Defense, the vast majority of its infrastructure is currently owned and operated by the private sector. Federal policy recognizes the need to prepare for debilitating Internet disruptions and tasks the Department of Homeland Security (DHS) with developing an integrated public/private plan for Internet recovery. GAO was asked to (1) identify examples of major disruptions to the Internet, (2) identify the primary laws and regulations governing recovery of the Internet in the event of a major disruption, (3) evaluate DHS plans for facilitating recovery from Internet disruptions, and (4) assess challenges to such efforts.

What GAO Recommends

GAO is suggesting that Congress consider clarifying the legal framework guiding Internet recovery. GAO is also making recommendations to the Secretary of the Department of Homeland Security to strengthen the department's ability to serve as a focal point for helping to recover from Internet disruptions by completing key plans and activities and addressing challenges. In written comments, DHS agreed with GAO's recommendations and provided information on activities it was taking to implement them.

www.gao.gov/cgi-bin/getrpt?GAO-06-672.

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

A major disruption to the Internet could be caused by a cyber incident (such as a software malfunction or a malicious virus), a physical incident (such as a natural disaster or an attack that affects key facilities), or a combination of both cyber and physical incidents. Recent cyber and physical incidents have caused localized or regional disruptions but have not caused a catastrophic Internet failure.

Federal laws and regulations addressing critical infrastructure protection, disaster recovery, and the telecommunications infrastructure provide broad guidance that applies to the Internet, but it is not clear how useful these authorities would be in helping to recover from a major Internet disruption. Specifically, key legislation on critical infrastructure protection does not address roles and responsibilities in the event of an Internet disruption. Other laws and regulations governing disaster response and emergency communications have never been used for Internet recovery.

DHS has begun a variety of initiatives to fulfill its responsibility for developing an integrated public/private plan for Internet recovery, but these efforts are not complete or comprehensive. Specifically, DHS has developed high-level plans for infrastructure protection and incident response, but the components of these plans that address the Internet infrastructure are not complete. In addition, the department has started a variety of initiatives to improve the nation's ability to recover from Internet disruptions, including working groups to facilitate coordination and exercises in which government and private industry practice responding to cyber events. However, progress to date on these initiatives has been limited, and other initiatives lack time frames for completion. Also, the relationships among these initiatives are not evident. As a result, the government is not yet adequately prepared to effectively coordinate public/private plans for recovering from a major Internet disruption.

Key challenges to establishing a plan for recovering from Internet disruptions include (1) innate characteristics of the Internet (such as the diffuse control of the many networks making up the Internet and private sector ownership of core components) that make planning for and responding to disruptions difficult, (2) a lack of consensus on DHS's role and when the department should get involved in responding to a disruption, (3) legal issues affecting DHS's ability to provide assistance to restore Internet service, (4) reluctance of many in the private sector to share information on Internet disruptions with DHS, and (5) leadership and organizational uncertainties within DHS. Until these challenges are addressed, DHS will have difficulty achieving results in its role as a focal point for helping to recover the Internet from a major disruption.

Contents

Tables

Figures

Abbreviations

DHS	Department of Homeland Security
IP	Internet Protocol
NCS	National Communications System
NCSD	National Cyber Security Division
US-CERT	United States Computer Emergency Readiness Team

Contents

GAO
Accountability * Integrity * Reliability

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

June 16, 2006

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. Our country has come to rely on the Internet as a critical infrastructure supporting commerce, education, and communication. While the benefits of this technology have been enormous, this widespread interconnectivity poses significant risks to the government's and our nation's computer systems and, more importantly, to the critical operations and infrastructures they support.

Federal regulation 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 systems.[1] To accomplish this mission, DHS is to work with federal agencies, state and local governments, and the private sector. Federal policy also recognizes the need to be prepared for the possibility of debilitating disruptions in cyberspace and, because the vast majority of the Internet infrastructure is owned and operated by the private sector, tasks DHS with developing an integrated public/private plan for Internet recovery.[2] Last year, we reported on DHS efforts to fulfill its cybersecurity responsibilities and noted that the department had not developed key cybersecurity recovery plans—including a plan for recovering key Internet functions.[3]

Because of your interest in DHS's efforts to develop a joint plan for recovering the Internet in case of a major disruption, you asked that we (1) identify examples of major disruptions to the Internet, (2) identify the primary laws and regulations governing recovery of the Internet in the event of a major disruption, (3) evaluate DHS's plans for facilitating

[1]Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (Dec. 17, 2003).

[2]The White House, *National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

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

recovery from Internet disruptions, and (4) assess challenges to such efforts.

To accomplish these objectives, we assessed documentation of disruptions to the Internet and compiled case studies of incidents that have affected the Internet. We also reviewed relevant laws and regulations related to critical infrastructure protection, disaster response, and the telecommunications infrastructure. We assessed DHS progress and plans for handling Internet disruptions. In order to identify challenges to effective Internet recovery planning, we also interviewed officials from DHS, other federal agencies, and representatives of the private sector who have a role in operating the Internet infrastructure. Appendix I provides additional details on our objectives, scope, and methodology. We performed our work from August 2005 to May 2006 in accordance with generally accepted government auditing standards.

Results in Brief

A major disruption to the Internet could be caused by a cyber incident (such as a software malfunction or a malicious virus), a physical incident (such as a natural disaster or an attack that affects facilities and other assets), or a combination of both cyber and physical incidents. Recent cyber and physical incidents have caused localized or regional disruptions, highlighting the importance of recovery planning. For example, a 2002 root server attack highlighted the need to plan for increased server capacity at Internet exchange points in order to manage the high volumes of data traffic during an attack. However, recent incidents also have shown the Internet as a whole to be flexible and resilient. Even in past severe circumstances, the Internet did not suffer a catastrophic failure.

Several federal laws and regulations provide broad guidance that applies to the Internet, but it is not clear how useful these authorities would be in helping to recover from a major Internet disruption. Specifically, the Homeland Security Act of 2002 and Homeland Security Presidential Directive 7 provide guidance on protecting our nation's critical infrastructures. However, they do not specifically address roles and responsibilities in the event of an Internet disruption. In addition, the Defense Production Act and the Stafford Act provide authority to federal agencies to plan for and respond to incidents of national significance, such as disasters and terrorist attacks. However, the Defense Production Act has never been used for Internet recovery and the Stafford Act does not authorize the provision of resources to for-profit companies—such as those that own and operate core Internet components. The Communications Act

of 1934 and the National Communications System authorities govern the telecommunications infrastructure and help ensure communications during national emergencies, but they have never been used for Internet recovery. Thus, it is not clear how effective they would be in assisting Internet recovery.

DHS has begun a variety of initiatives to fulfill its responsibility for developing an integrated public/private plan for Internet recovery, but these efforts are not yet complete or comprehensive. Specifically, DHS has developed high-level plans for infrastructure protection and incident response, but the components of these plans that address the Internet infrastructure are not complete. In addition, DHS has started a variety of initiatives to improve the nation's ability to recover from Internet disruptions, including working groups to facilitate coordination and exercises in which government and private industry practice responding to cyber events. However, progress to date on these initiatives has been limited and other initiatives lack time frames for completion. Also, the relationships among these initiatives are not evident. As a result, risk remains that the government is not yet adequately prepared to effectively coordinate public/private plans for recovering from a major Internet disruption.

Key challenges to establishing a plan for recovering from an Internet disruption include (1) innate characteristics of the Internet (such as the diffuse control of the many networks that make up the Internet and the private-sector ownership of core components) that make planning for and responding to disruptions difficult, (2) lack of consensus on DHS's role and when the department should get involved in responding to a disruption, (3) legal issues affecting DHS's ability to provide assistance to entities working to restore Internet service, (4) reluctance of many in the private sector to share information on Internet disruptions with DHS, and (5) leadership and organizational uncertainties within DHS. Until these challenges are addressed, DHS will have difficulty achieving results in its role as a focal point for helping to recover the Internet from a major disruption.

Given the importance of the Internet infrastructure to our nation's communications and commerce, we are suggesting that Congress consider clarifying the legal framework guiding Internet recovery. We are also making recommendations to the Secretary of the Department of Homeland Security to strengthen the department's ability to effectively serve as a focal point for helping to recover from Internet disruptions by establishing

clear milestones for completing key plans, coordinating various Internet recovery-related activities, and addressing key challenges to Internet recovery planning.

DHS provided written comments on a draft of this report in which it agreed with our recommendations and provided information on initial activities it is taking to implement them (see app. V). 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.

Background

The Internet: An Overview

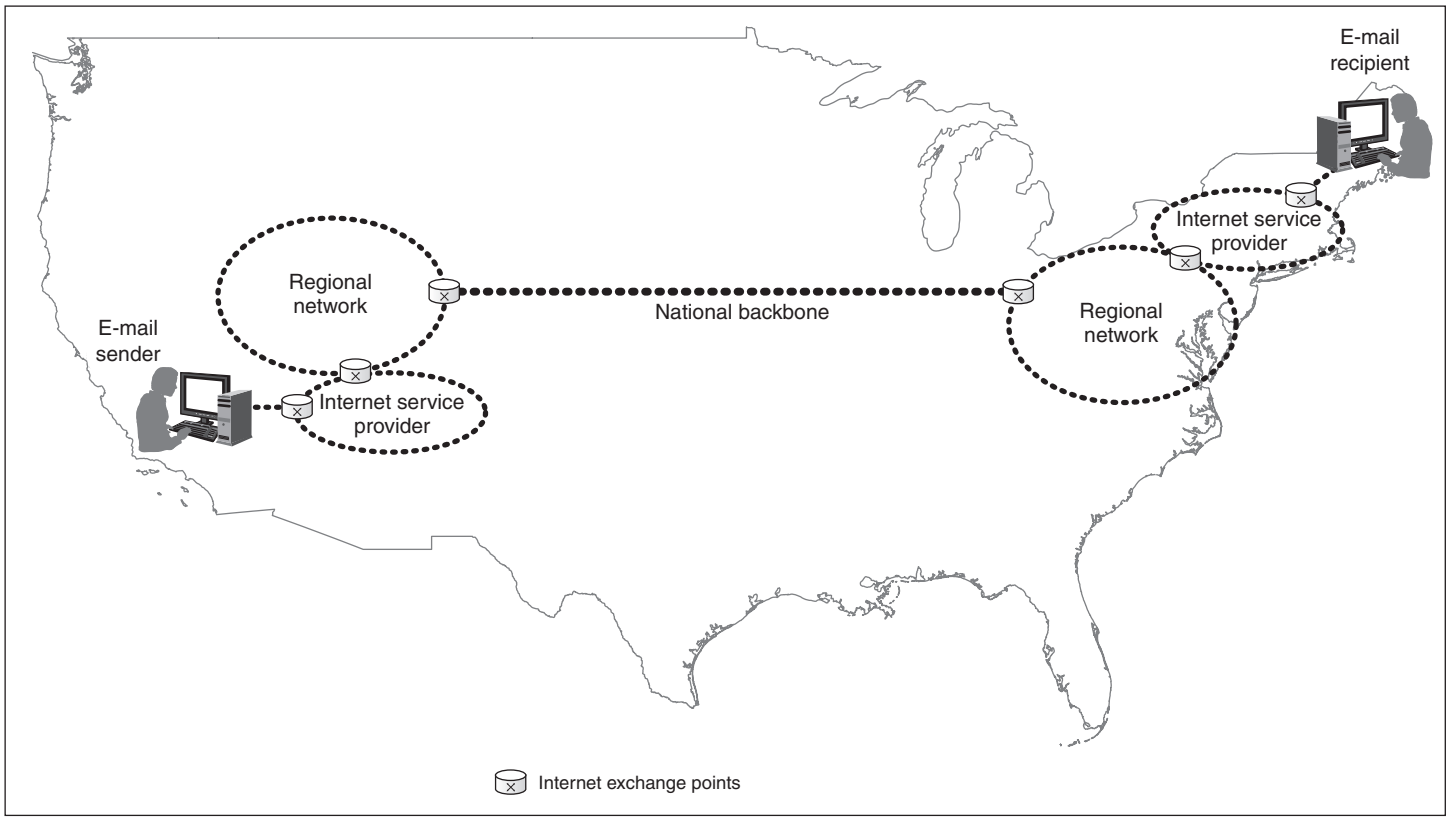
The Internet is a vast network of interconnected networks. It is used by governments, businesses, research institutions, and individuals around the world to communicate, engage in commerce, do research, educate, and entertain. While most Americans are familiar with Internet service providers—such as America Online and EarthLink—that provide consumers with a pathway, or "on-ramp," to the Internet, many are less familiar with how the Internet was developed, the underlying structure of the Internet, and how it works.

In the late 1960s and the 1970s, the Department of Defense's Advanced Research Projects Agency developed a network to allow multiple universities to communicate and share computing resources. In the ensuing decades, this project grew to become a large network of networks and was joined with an array of scientific and academic computers funded by the National Science Foundation. This expanded network provided the backbone infrastructure of today's Internet. In 1995, the federal government began to turn the backbone of the Internet over to a consortium of commercial backbone providers. From that point on, the Internet infrastructure was owned and operated by private companies—including telecommunications companies, cable companies, and Internet service providers.

Today's Internet connects millions of small, medium, and large networks. When an Internet user wants to access a Web site or to send an e-mail to someone who is connected to the Internet through a different Internet service provider, the data must be transferred between networks. Transit across the Internet is provided by either national backbone providers,

regional network operators, or a combination of both. National backbone providers are companies that own and operate high-capacity, long-haul backbone networks. These providers transmit data traffic over long distances using high-speed, fiber-optic lines. Because national backbone operators do not service all locations worldwide, regional network providers supplement the long-haul traffic by providing regional service. Data cross between networks at Internet exchange points—which can be either hub points where multiple networks exchange data or private interconnection points arranged by transit providers. At these exchange points, computer systems called routers determine the optimal path for the data to reach their destination. The data then continue their path through the national and regional networks and exchange points, as necessary, to reach the recipient's Internet service provider and the recipient (see fig. 1).

Figure 1: Example of an E-mail Transiting the Internet



Source: GAO.

The networks that make up the Internet communicate via standardized rules called *protocols*. These rules can be considered voluntary because there is no formal institutional or governmental mechanism for enforcing them. However, if any computer deviates from accepted standards, it risks losing the ability to communicate with other computers that follow the standards. Thus, the rules are essentially self enforcing. One critical set of rules is the *Transmission Control Protocol/Internet Protocol* suite. These protocols define a detailed process that a sender and receiver agree upon for exchanging data. They describe the flow of data between the physical connection to the network and on to the end-user application. Specifically, these protocols control the addressing of a message by the sender, its division into packets, its transmission across networks, and its reassembly and verification by the receiver. This protocol suite has become the de facto communication standard of the Internet because many standard services (including mail transfer, news, and Web pages) are available on systems that support these protocols.[4]

Another critical set of protocols, collectively known as the *Domain Name System*, ensures the uniqueness of each e-mail and Web site address. This system links names like www.senate.gov with the underlying numerical addresses that computers use to communicate with each other. It translates names into addresses and back again in a process invisible to the end user. This process relies on a system of servers, called *domain name servers*, which store data linking names with numbers. Each domain name server stores a limited set of names and numbers. They are linked by a series of 13 *root servers*, which coordinate the data and allow users to find the server that identifies the sites they want to reach. Domain name servers are organized into a hierarchy that parallels the organization of the domain names. For example, when someone wants to reach the Web site at www.senate.gov, his or her computer will ask one of the root servers for help.[5] The root server will direct the query to a second server that knows the location of names ending in the .gov top-level domain.[6] If the address

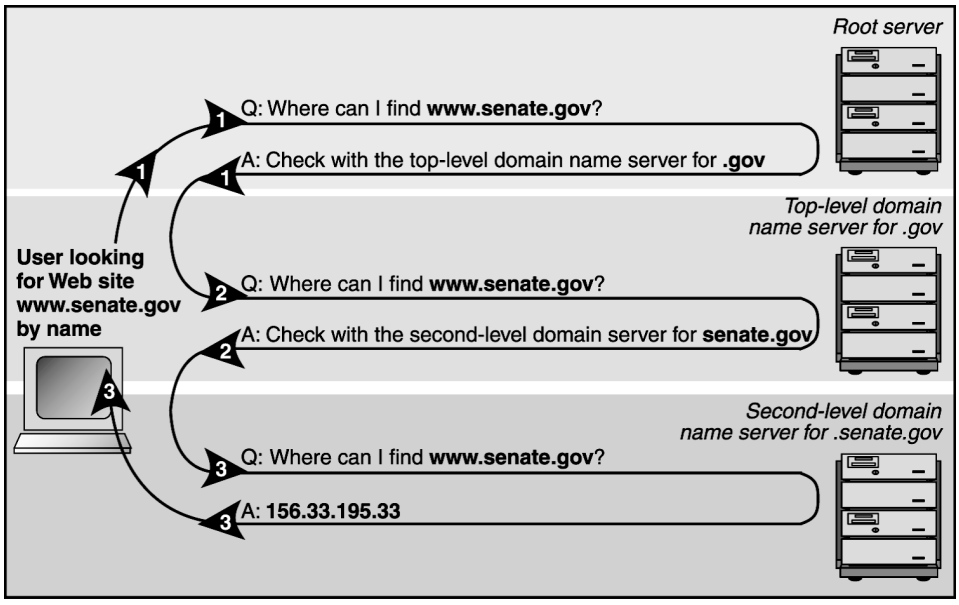
[4]We reported on issues associated with these protocols in *Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks*, GAO-05-471 (Washington, D.C.: May 20, 2005).

[5]This example assumes that the required domain name information is not available on the user's local network.

[6]Although the Department of Commerce has authority to modify the root file containing this top-level domain information, it has delegated this authority to the Internet Corporation for Assigned Names and Numbers, a nonprofit organization, and VeriSign, a private corporation.

includes a subdomain, the second server refers the query to a third server—in this case, one that knows the addresses for all names ending in senate.gov. The third server will then respond to the request with a numerical address, which the original requester uses to establish a direct connection with the www.senate.gov site. Figure 2 illustrates this example.

Figure 2: How the Domain Name System Translates a Web Site Name into a Numerical Address



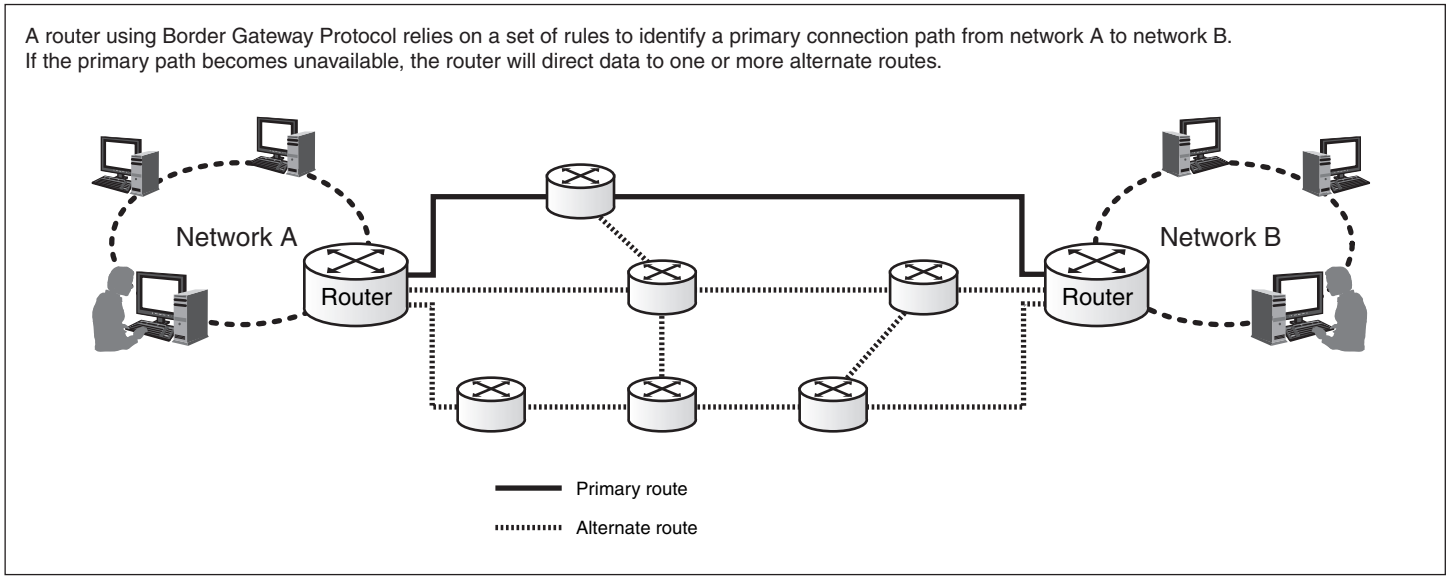
Source: GAO.

Another critical set of rules is called the *Border Gateway Protocol*—a protocol for routing packets between autonomous systems.[7] This protocol is used by routers located at network nodes to direct traffic across the Internet. Typically, routers that use this protocol maintain a routing table that lists all feasible paths to a particular network. They also determine metrics associated with each path (such as cost, stability, and speed), so that the best available path can be chosen. This protocol is important

[7]An autonomous system is a set of routers that are administered using an interior gateway protocol to route packets among that set of routers and an exterior gateway protocol, such as Border Gateway Protocol, to route packets to other autonomous systems.

because if a certain path becomes unavailable, the system will send data over the next best path (see fig. 3).

Figure 3: Example of Dynamic Routing Using Border Gateway Protocol



Source: GAO.

The Internet Is a Critical Information Infrastructure

From its origins in the 1960s as a research project sponsored by the U.S. government, the Internet has grown increasingly important to both American and foreign businesses and consumers, serving as the medium for hundreds of billions of dollars of commerce each year. According to the U.S. Census Bureau, retail e-commerce sales in the United States were an estimated $86 billion in 2005. The Internet has also become an extended information and communications infrastructure, supporting vital services such as power distribution, health care, law enforcement, and national defense.

Federal regulation recognizes the need to protect critical infrastructures. In December 2003, the President updated a national directive for federal departments and agencies to identify and prioritize critical infrastructure sectors and key resources and to protect them from terrorist attack. (See

table 1 for a list of critical infrastructure sectors.)[8] This directive recognized that since a large portion of these critical infrastructures is owned and operated by the private sector, a public/private partnership is crucial for the successful protection of these critical infrastructures.

Table 1: Critical Infrastructure Sectors

Sector	Description
Agriculture	Provides for the fundamental need for food. The infrastructure includes supply chains for feed and crop production.
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.
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.
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.
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.
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.
Drinking water and water treatment systems	Sanitizes the water supply through about 170,000 public water systems. These systems depend on reservoirs, dams, wells, treatment facilities, pumping stations, and transmission lines.
Emergency services	Saves lives and property from accidents and disasters. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.
Energy	Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. This sector is divided into electricity and oil and natural gas.
Food	Carries out the postharvesting of the food supply, including processing and retail sales.
Government	Ensures national security and freedom and administers key public functions.
Government facilities	Includes the buildings owned and leased by the federal government for use by federal entities.
Information technology	**Produces hardware, software, and services that enable other sectors to function.**
National monuments and icons	Includes key assets that are symbolically equated with traditional American values and institutions or U.S. political and economic power.
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.
Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The United States Postal Service and other carriers provide the services of this sector.

[8]Homeland Security Presidential Directive 7 (Dec. 17, 2003).

(Continued From Previous Page)

Sector	Description
Public health and healthcare	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. This sector consists of health departments, clinics, and hospitals.
Telecommunications	**Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.**
Transportation	Enables movement of people and assets that are vital to our economy, mobility, and security, using aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.

Sources: Homeland Security Presidential Directive 7 and the National Strategy for Homeland Security.

In its plan for protecting these critical infrastructures, DHS recognizes that the Internet is a key resource composed of assets within both the information technology and the telecommunications sectors.[9] It notes that the Internet is used by all sectors to varying degrees, and that it provides information and communications to meet the needs of businesses, government, and the other critical infrastructure sectors. Similarly, the national cyberspace strategy states that cyberspace is the nervous system supporting our nation's critical infrastructures and recognizes the Internet as the core of our information infrastructure.[10]

It is also important to note that there are critical interdependencies between sectors. For example, the telecommunications and information technology sectors, like many other sectors, depend heavily on the energy sector.

Attacks on the Information Infrastructure Are Increasing

In recent years, cyber attacks involving malicious software or hacking have been increasing in frequency and complexity. These attacks can come from a variety of actors. Table 2 lists sources of cyber threats that have been identified by the U.S. intelligence community.

[9]DHS, *National Infrastructure Protection Plan*.

[10]The White House, *National Strategy to Secure Cyberspace*.

Table 2: Sources of Cyber Threats Identified by the U.S. Intelligence Community

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 to enable them to coordinate attacks and to distribute phishing[a] schemes or malware[b] attacks.
Criminal groups	Criminal groups 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 would 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 within the hacker community. Although 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 also have become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite tradecraft to threaten difficult targets, such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of causing an isolated or brief disruption that results in 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.
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 malicious software to gather sensitive information.

Source: GAO analysis of data from the Federal Bureau of Investigation, the Central Intelligence Agency, and the Software Engineering Institute's CERT® Coordination Center.

[a]Phishing involves the creation and use of e-mail and Web sites that are designed to look like the e-mail and Web sites 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.

[b]Spyware/Malware is software designed with a malicious intent, such as a virus.

An intelligence report on global trends[11] forecast that terrorists may develop capabilities to conduct both cyber and physical attacks against nodes of the world's information infrastructure—including the Internet and other systems that control critical industrial processes—such as electricity grids, refineries, and flood control mechanisms. The report stated that terrorists already have specified the U.S. information infrastructure as a target and currently are capable of physical attacks that would cause at least brief, isolated disruptions.

According to a Congressional Research Service report, the annual worldwide cost of major cyber attacks was, on average, $13.5 billion from 2000 to 2003. A more recently published report estimated that the worldwide financial impact of virus attacks was $17.5 billion in 2004 and $14.2 billion in 2005.

Multiple Organizations Could Help in Recovering the Internet from a Major Disruption

In the event of a major Internet disruption, multiple organizations could help recover Internet service. These organizations include private industry, collaborative groups, and government organizations. Private industry is central to Internet recovery because private companies own the vast majority of the Internet's infrastructure and often have response plans. Collaborative groups—including working groups and industry councils—provide information-sharing mechanisms to allow private organizations to restore services. Additionally, government initiatives could facilitate responding to major Internet disruptions.

Private Industry

Private industry organizations are critical to recovering Internet services in the event of a major disruption because they own and operate the vast majority of the Internet's infrastructure. This group of Internet infrastructure owners and operators includes telecommunications companies (such as AT&T and Verizon Communications), cable companies (such as Cox Communications and Time Warner Cable), Internet service providers (such as AOL and EarthLink), and root server operators (such as VeriSign and the University of Maryland). These entities own or operate cable lines; telephone lines; fiber-optic cables; or critical core systems, such as network routers and domain name servers.

[11]The National Intelligence Council, *Mapping the Global Future* (December 2004).

These private companies currently deal with cyber attacks and physical disruptions on the Internet on a regular basis. According to representatives of Internet infrastructure owners and operators, these firms typically have disaster recovery plans in place. For example, a representative from a major telecommunications company stated that the company has emergency response plans for its primary and secondary emergency operations centers. Similarly, representatives of a cable trade association reported that most cable companies have standard disaster recovery plans and a network operations center from which they can monitor recovery operations.

Infrastructure representatives also noted that in the event of a network disruption, companies that are competitors work together to resolve the disruption. They said that although the companies are competitors, they have a business interest in cooperating because it is common to rely on each other's networks. For example, a representative of a major telecommunications company noted that the company has "mutual-aid" agreements with its competitors to exchange technicians and hardware in the event of an emergency.

Collaborative Groups

Collaborative groups—working groups and industry councils that the private and public sectors have established to allow technical information sharing—help handle and recover from Internet disruptions. These collaborative groups are usually composed of individuals and experts from separate organizations. In the event of a major Internet disruption, these groups allow individuals from different companies to exchange information in order to assess the scope of the disruption and to restore services. Table 3 provides descriptions of selected collaborative groups.

Table 3: Examples of Collaborative Groups

Group	Description
North American Network Operators Group	This group of network operators coordinates and disseminates technical information related to backbone/enterprise networking technologies and operational practices. It was originally established to discuss operational issues regarding the National Science Foundation's high-speed research and education network, which became the Internet. In the mid-1990s, the group revised its charter to include a broader base of network service providers. Although the National Science Foundation originally funded the group, it is now funded by conference registration fees and donations from vendors. Through the group's mailing list, members collaborate and assist each other in resolving network operating issues. In the event of a major Internet disruption, these information-sharing mechanisms are used to resolve issues related to the disruption. For example, group members used their mailing list to collaborate with each other when the Slammer worm hit in January 2003, causing significant Internet congestion. Through the mailing list, members were able to corroborate events and share mitigation strategies.
Network Service Providers Security Consortium	This group was originally established in 2001 to allow individuals in the network service provider community to coordinate on network security issues and problems. Its primary information-sharing mechanism is through its e-mail list. Members of the list who observe disruptions or malicious activity can post their observations or concerns to the list, and other members can take action or provide assistance. Membership in the list is only available to those who have been identified by other group members as having a relevant need for the information on the list. As of March 2006, approximately 500 people subscribe to the list. If the list were not available or an issue needed to be addressed immediately, the group's organizer would be able to coordinate collaboration between the necessary parties. According to the group's organizer, the closed nature of the list is crucial to its value. The limited membership allows the building of trusted relationships and gives each member confidence that information posted to the list will not be misused. The organizer stated that the list has been very effective at resolving disruption issues. For example, the consortium's mailing list played a major role in resolving the root Domain Name System server attacks that occurred in October 2002.
Packet Clearing House	The Packet Clearing House is a nonprofit research institute that supports operations and analyses in the areas of Internet traffic exchange, routing economics, and global network development. It hosts a hotline telephone system, called the Inter-Network Operations Center Dial-By-Autonomous System Number (a unique identifier for autonomous systems on the Internet). This system is a global voice telephony network that connects the network operations centers and security incident response teams of critical Internet infrastructure owners and operators, such as backbone providers, Internet service providers, and Internet exchange point operators. The hotline also connects critical individuals within the policy, regulatory, Internet governance, security, and vendor communities. The hotline is a closed system, ensuring secure and authenticated communications. It uses a combination of mechanisms to create a resilient, high-survivability network. Additionally, the hotline telephone system carries both routine operational traffic and emergency-response traffic. Representatives of several Internet service providers noted that they use this system to contact other network operators in order to resolve problems quickly.
Information Technology Information Sharing and Analysis Center	This center is made up of representatives of companies from across the information technology industry. It helps facilitate operational information sharing, communication with other infrastructure sectors, and crisis response. The center works to improve security, reliability, and disaster recovery in information technology. The center identifies threats and vulnerabilities to information technology infrastructure (including the Internet) and shares best practices for how to quickly and properly address them. The representatives also stated that the Information Technology Information Sharing and Analysis Center facilitates information sharing and participates in exercises to test its ability to respond to incidents such as a major Internet disruption. For example, the center assisted with DHS's recent Cyber Storm exercise in February 2006. The center took a leadership role in Cyber Storm and prepared a concept of operations that addressed incident response to cyber or physical attacks.

(Continued From Previous Page)

Group	Description
Telecommunications Information Sharing and Analysis Center	In 1984, following the divestiture of AT&T, the National Coordinating Center for Telecommunications was established to allow information sharing between representatives of the telecommunications companies. In January 2000, the center was designated the information sharing and analysis center for the telecommunications industry. The center is unique among information sharing and analysis centers in that it is actually a joint government/industry operation. According to a center representative, the main role of the Telecommunications Information Sharing and Analysis Center during an Internet disruption is to provide a protected forum in which industry members can collaborate and freely share information. In turn, this coordination effort will help expedite the overall Internet recovery. The industry chair of the center noted that this forum enables members to form trusted relationships with each other where they otherwise may not exist between competitors. An example of this cooperation occurred during the Code Red and NIMDA cyber attacks. Center members coordinated to understand and mitigate the attacks.
National Security Telecommunications Advisory Committee	This committee provides industry-based analyses and recommendations to the President and the executive branch regarding telecommunications policy and proposals for enhancing national security and emergency preparedness. The committee is made up of 30 Presidentially appointed industry leaders, usually chief executive officers of companies in the telecommunications industry. Since the committee is composed of telecommunications executives, their role in Internet recovery is strategic as opposed to operational. Members of the committee have long established relationships with DHS's National Communications System and National Coordinating Center for Telecommunications. Committee representatives reported that the committee works closely with these entities during response and recovery activities following a terrorist attack or natural disaster. The committee and these entities also share information related to a variety of other issues, including modifications to federal policy associated with telecommunications in support of national security and emergency preparedness and changes in the commercial telecommunications marketplace. Additionally, the committee publishes reports that cover topics related to Internet recovery. In an October 2005 report, the committee provides an industry perspective on lessons learned in responding to the September 11, 2001, terrorist attacks. In the October report, the committee deemed Internet services to be increasingly important in disaster response and central to the mission-critical operations of business and government agencies, and it identified steps the government could take to help the coordination center better address potential network security issues, such as distributed denial-of-service attacks and software viruses.

Source: GAO.

Government Organizations—DHS

Federal policies and plans[12] assign DHS lead responsibility for facilitating a public/private response to and recovery from major Internet disruptions. Within DHS, responsibilities reside in two divisions within the Preparedness Directorate: the National Cyber Security Division (NCSD) and the National Communications System (NCS). NCSD operates the U.S. Computer Emergency Readiness Team (US-CERT), which coordinates defense against and response to cyber attacks. The other division, NCS,

[12]These federal policies and plans include the *National Strategy to Secure Cyberspace*, the interim *National Infrastructure Protection Plan*, the Cyber Incident Annex to the *National Response Plan* (December 2004), and Homeland Security Presidential Directive 7.

provides programs and services that ensure the resilience of the telecommunications infrastructure in times of crisis.

National Cyber Security Division

In June 2003, DHS created NCSD to serve as a national focal point for addressing cybersecurity issues and to coordinate the implementation of the *National Strategy to Secure Cyberspace*. Its mission is to secure cyberspace and America's cyber assets in cooperation with public, private, and international entities.

NCSD is the government lead on a public/private partnership supporting the *US-CERT*, an operational organization responsible for analyzing and addressing cyber threats and vulnerabilities and disseminating cyber-threat warning information. In the event of an Internet disruption, US-CERT facilitates coordination of recovery activities with the network and security operations centers of owners and operators of the Internet and with government incident response teams.

NCSD also serves as the lead for the federal government's cyber incident response through the *National Cyber Response Coordination Group*. This group is the principal federal interagency mechanism for coordinating the preparation for, and response to, significant cyber incidents—such as a major Internet disruption. In the event of a major disruption, the group convenes to facilitate intragovernmental and public/private preparedness and operations. The group brings together officials from national security, law enforcement, defense, intelligence, and other government agencies that maintain significant cybersecurity responsibilities and capabilities. Members use their established relationships with the private sector and with state and local governments to help coordinate and share situational awareness, manage a cyber crisis, develop courses of action, and devise response and recovery strategies.

NCSD also recently formed the *Internet Disruption Working Group*, which is a partnership between NCSD, NCS, the Department of the Treasury, the Department of Defense, and private-sector companies, to plan for ways to improve DHS's ability to respond to and recover from major Internet disruptions. The goals of the working group are to identify and prioritize the short-term protective measures necessary to prevent major disruptions to the Internet or reduce their consequences and to identify reconstitution measures in the event of a major disruption.

National Communications System

NCS is responsible for ensuring a communications infrastructure for the federal government under all conditions—ranging from normal situations to national emergencies and international crises. NCS is composed of members from 23 federal departments and agencies.[13] Although originally focused on traditional telephone service, due to the convergence of the Internet and telecommunications NCS has taken a larger role in Internet-related issues and has partnered with NCSD and private companies to address issues related to major Internet disruptions. For example, NCS now helps manage issues related to disruptions of the Internet backbone (e.g., high-capacity data routes).

The *National Coordinating Center for Telecommunications* (National Coordinating Center), which serves as the operational component of NCS, also has a role in Internet recovery. The center has eight resident industry members (representing companies that were originally telephone providers) as well as additional nonresident members, including representatives of newer, more Internet-oriented companies. During a major disruption to telecommunications services, the center communicates with both resident and nonresident members, with the goal of restoring service as soon as possible. In the event of a major Internet disruption, the National Coordinating Center plays a role in the recovery effort through its partnerships and collaboration with telecommunications and Internet-related companies.

Government Organizations—Federal Communications Commission

The Federal Communications Commission can support Internet recovery by coordinating resources for restoring the basic communications infrastructures over which Internet services run. For example, after Hurricane Katrina, the commission granted temporary authority for private companies to set up wireless Internet communications supporting various

[13]These entities include the Department of State, the Central Intelligence Agency, the Department of the Treasury, the Federal Emergency Management Agency, the Department of Defense, the Joint Staff, the Department of Justice, the General Services Administration, the Department of the Interior, the National Aeronautics and Space Administration, the Department of Agriculture, the Nuclear Regulatory Commission, the Department of Commerce, the National Security Agency, the Department of Health and Human Services, the National Telecommunications and Information Administration, the Department of Transportation, the United States Postal Service, the Department of Energy, the Federal Reserve Board, the Department of Veterans Affairs, the Federal Communications Commission, and the Department of Homeland Security.

relief groups; federal, state, and local government agencies; businesses; and victims in the disaster areas.

The commission also sponsors the Network Reliability and Interoperability Council. A primary goal of the council is to prevent Internet disruptions from occurring in the first place. The council has developed a list of best practices for Internet disaster recovery that provides guidance on strategic issues (such as exercising disaster recovery plans) as well as operational issues (such as how to restore a corrupt domain name server).[14]

Prior Evaluations of DHS's Cybersecurity Responsibilities Have Highlighted Issues and Challenges Facing the Department

In May 2005, we issued a report on DHS's efforts to fulfill its cybersecurity responsibilities.[15] We noted that while DHS had initiated multiple efforts to fulfill its responsibilities, it had not fully addressed any of the 13 key cybersecurity responsibilities (see table 4) noted in federal law and policy. For example, we noted that the department established US-CERT 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 with law enforcement entities. However, DHS had not yet developed national cyber threat and vulnerability assessment or government/industry cybersecurity recovery plans—including a plan for recovering key Internet functions.

We also noted in our May 2005 report that DHS faced a number of challenges that have impeded its ability to fulfill its cyber responsibilities. These challenges included achieving organizational stability, gaining organizational authority, overcoming hiring and contracting issues, increasing awareness of cybersecurity roles and capabilities, establishing effective partnerships with stakeholders, achieving two-way information sharing with stakeholders, and demonstrating the value that DHS can provide. We made recommendations to the department to strengthen its ability to implement key responsibilities by completing critical activities and resolving underlying challenges. DHS agreed that strengthening cybersecurity is central to protecting the nation's critical infrastructures

[14]The Network Reliability and Interoperability Council, NRIC Best Practices, *NRIC Best Practices Selector Tool*, http://www.bell-labs.com/cgi-user/krauscher/bestp.pl (viewed Apr. 19, 2006).

[15]GAO-05-434.

and that much remained to be done, but it has not yet addressed our recommendations. We continue to evaluate DHS's progress in implementing our recommendations.

Table 4: DHS's Key Cybersecurity Responsibilities

• Develop a national plan for critical infrastructure protection, including cybersecurity.	• Identify and assess cyber threats and vulnerabilities.
• Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector.	• Support efforts to reduce cyber threats and vulnerabilities.
• Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities.	• Promote and support research and development efforts to strengthen cyberspace security.
• Develop and enhance national cyber analysis and warning capabilities.	• Promote awareness and outreach.
• Provide and coordinate incident response and recovery planning efforts.	• 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.

Although Both Cyber and Physical Incidents Have Caused Disruptions, the Internet Has Not Yet Suffered a Catastrophic Failure

The Internet's infrastructure is vulnerable to disruptions in service due to terrorist and other malicious attacks, natural disasters, accidents, technological problems, or a combination of the above. Disruptions to Internet service can be caused by cyber and physical incidents—both intentional and unintentional. Private network operators routinely deal with Internet disruptions of both types. Recent cyber and physical incidents have caused localized or regional disruptions, highlighting the importance of recovery planning. However, these incidents have also shown the Internet as a whole to be flexible and resilient. Even in severe circumstances, the Internet has not yet suffered a catastrophic failure.

Internet Disruptions Have Been Caused by Both Cyber and Physical Incidents

The Internet can be disrupted by either cyber or physical incidents, or by a combination of the two. These incidents can be intentional (such as a cyber attack or a terrorist attack on our nation's physical infrastructure) or unintentional (such as a software malfunction or a natural disaster). Table 5 provides examples of intentional and unintentional cyber and physical incidents.

Table 5: Examples of Potential Internet Disruptions

	Cyber incident	Physical incident
Intentional act	• malicious code (virus, worm, or other attack)	• terrorist bomb
	• hacking	• foreign nation attack
	• distributed denial-of-service attack	• intentional cutting of fiber-optic cables
	• insider manipulating systems (changing router configurations)	
Unintentional act	• software glitch	• severe natural event (hurricane, earthquake, or flood)
	• hardware malfunction	• accidental cutting of fiber-optic cables
	• improper configuration of software or hardware	• other industrial accidents (chemical spill or fire)

Source: GAO.

A cyber incident could cause a disruption if it affects a network protocol or an application that is integral to the working of the Internet. A cyber incident could be unintended (such as a software problem) or intended (such as an attack using malicious software or hacking that causes a disruption of service). Unintended incidents have caused significant disruptions in the past. For example, in 1998, a major Internet backbone provider had a massive outage due to a software flaw in the infrastructure that caused systems to crash; in 2002, a different provider had an outage due to a router with a faulty configuration.

Intentional incidents, or malicious attacks, have been increasing in frequency and complexity and recently have been linked to organized crime. Examples of malicious attacks include viruses and worms. Viruses and worms are often used to launch denial-of-service attacks, which flood targeted networks and systems with so much data that regular traffic is either slowed or stopped. Such attacks have been used ever since the groundbreaking Morris worm in November 1988, which brought 10 percent

of the systems connected to the Internet to a halt. More recently, 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.[16]

Cyber attacks can also cause Internet disruptions by targeting specific protocols, such as the Border Gateway Protocol or the Domain Name System. If a vulnerability in the Border Gateway Protocol was exploited, the ability of Internet traffic to reach its destination could be limited or halted. Some experts believe that it could take weeks to recover from a major attack on the Border Gateway Protocol. The Domain Name System is also susceptible to various attacks, including the corruption of stored domain name information and the misdirection of addresses. Recently, hackers have used domain name servers to launch denial-of-service attacks—thereby amplifying the strength of the attacks. A network security expert stated that there have been numerous attacks of this type recently, and that some attacks have targeted top-level domains[17] and Internet service providers. Attacks against top-level domain servers could disrupt users' capability to connect to various Internet addresses. It could take several days to recover from a massive disruption of the domain name server system.

As the number of individuals with computer skills has increased, more intrusion, or hacking, tools have become 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. Experts also agree that there has been a steady advance in the sophistication and effectiveness of attack technology.

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

[17]Top-level domains are the right-most label following the last period in a domain name; for example, for www.senate.gov, .gov is the top-level domain. There are generic top-level domains, which include .com, .edu, .gov, .int, .mil, .net, and .org, among others. There are also country code top-level domains, such as .us, .uk, and .jp.

In the case of insider incidents, these tools may not even be necessary, because insiders often have unfettered access to their employers' computer systems. In one incident, an insider installed unauthorized backdoor access to his employer's systems. After his termination, the insider used these back doors to gain access to the systems and to delete accounts, change passwords, and delete security logs. While this is a case of an insider disrupting a single network, an insider could also use this knowledge to disrupt the operation of an Internet service provider. For example, an insider at a company that develops critical routing hardware might be able to use specific technical knowledge of the products to create an attack that could disrupt networks that use that particular equipment.

To date, cyber attacks have caused various degrees of damage. The following case studies provide examples of cyber attacks; the effects of these attacks; and the government's role, if any, in recovery (see figs. 4 and 5).

Figure 4: Case Study—The Slammer Worm

On Saturday, January 25, 2003, the Slammer worm infected more than 90 percent of vulnerable computers worldwide within 10 minutes of its release on the Internet by exploiting a known vulnerability for which a patch had been available since July 2002. Slammer caused network outages, canceled airline flights, and automated teller machine failures. In addition, the Nuclear Regulatory Commission confirmed that the Slammer worm had infected a private computer network at a nuclear power plant, disabling a safety monitoring system for nearly 5 hours and causing the plant's process computer to fail. The worm reportedly also affected communications on the control networks of at least five utilities by propagating so quickly that control system traffic was blocked. In addition, on Monday, January 27, the worm infected more networks when U.S. and European business hours started. Cost estimates on the impact of the worm range from $1.05 billion to $1.25 billion.

Slammer resulted in temporary loss of Internet access to some users and increased network traffic worldwide. Postincident studies noted that if the worm had been malicious or had exploited more widespread vulnerabilities, it would have caused a significant disruption to Internet traffic.

Responses to Slammer were quick. Within 1 hour, Web site operators were able to filter the worm. The disruption was partly resolved by network operators blocking the main communication channel that the worm was using, which helped control the spread of the worm. Security experts advised network operators to use firewalls to block the channel and to apply the patch before reconnecting services. In addition, private-sector network operators used the North American Network Operators Group mailing list to collaborate with each other in restoring infected networks. The federal government coordinated with security companies and Internet service providers and released an advisory recommending that federal departments and agencies patch and block access to the affected channel. However, most of these activities occurred after the worm had stopped spreading because it had propagated so quickly.

Source: GAO analysis of GAO and other published reports.

Figure 5: Case Study—A Root Server Attack

On Monday, October 21, 2002, a coordinated denial-of-service attack was launched against all of the root servers in the Domain Name System. All 13 root servers, located around the world, were targeted. The root servers experienced an unusually high volume of traffic. Two root server operators reported that traffic was 3 times the normal level, while another reported that traffic was 10 times the normal level. The attacks lasted for approximately 1 hour and 15 minutes. While reports of the attack differ, they all agreed that at least 9 of the servers experienced degradation in service. Specifically, 7 failed to respond to legitimate network traffic and 2 others failed intermittently during the attack.

Some root servers were unreachable from many parts of the global Internet because of traffic congestion from the attack. While all of the servers continued to answer any queries they received (because of their substantial backup capacity), many did not receive all of the queries that had been routed to them due to the high volume of traffic. However, average end users hardly noticed the attack. The attack became visible only as a result of various Internet health-monitoring projects. According to experts, the root name servers would have to be down for several hours before the effects would be noticeable to end users.

The response to these attacks was handled by the server operators and their service providers. The Domain Name System servers worked as they were designed to, and demonstrated robustness against a concerted, synchronized attack. However, the attack pointed to a need to increase the capacity of servers at Internet exchange points in order to manage the high volumes of data traffic that occur during an attack. The attacks led to systems receiving faster-than-normal upgrades. According to experts familiar with the attack, the government did not have a role in recovering from this attack.

Source: GAO analysis of interviews and published reports from sources, including root name server operators and current and former government officials.

A physical incident could be caused by an intentional attack, a natural disaster, or an accident. For example, terrorist attacks, storms, earthquakes, and unintentional cutting of cables can all cause physical disruptions. Physical incidents causing Internet and telecommunications disruptions occur regularly—often as a result of the accidental cutting of cable lines. Physical incidents could affect various aspects of the Internet infrastructure, including underground or undersea cables and facilities that house telecommunications equipment, Internet exchange points, or Internet service providers. Such incidents could also disrupt the power infrastructure—leading to an extended power outage and thereby disrupting telecommunications and Internet service. The following case studies provide examples of physical incidents that caused Internet disruptions and the effect of these incidents (see figs. 6 to 8).

Figure 6: Case Study—The Baltimore Train Tunnel Fire

On July 18, 2001, a 60-car freight train derailed in a Baltimore tunnel, causing a fire that interrupted Internet and data services between Washington and New York. The tunnel housed fiber-optic cables that served seven of the biggest U.S. Internet service providers. The fire burned and severed fiber-optic cables, causing backbone slowdowns for at least three major Internet service providers. There were sporadic reports from across the Northeast corridor about service disruptions and delays. For example, users in Baltimore did not suffer disrupted service, while users in Washington D.C. did suffer disruptions. In addition, there were selected impacts far outside the disaster zone. For example, the U.S. embassy in Lusaka, Zambia, experienced problems with e-mail. Two of the service providers had service restored within 2 days. Despite the outages caused by the fire, the Internet continued to operate.

Efforts to recover Internet service were handled by the affected Internet service providers. City officials also worked with telecommunications and networking companies to reroute cables. Other federal and local government efforts to resolve the disruption consisted of responding to the immediate physical issues of extinguishing the fire, maintaining safety in the surrounding area, and rerouting traffic.

Source: GAO analysis of a Department of Transportation report.

Figure 7: Case Study—The September 11, 2001, Terrorist Attack on the World Trade Center

On September 11, 2001, terrorists crashed two commercial airplanes into the World Trade Center, which led to the deaths of nearly 3,000 people and the destruction of 12 buildings containing millions of square feet of office space. The attack physically damaged one of the Internet's most important hubs—New York City—disrupting the local communications infrastructure (including facilities, critical computer systems, and fiber-optic cables that ran under the ruined buildings). In addition, the attack disrupted electrical power in Lower Manhattan. Local telecommunications facilities used back-up power systems until these ran out of fuel or batteries, and then they shut down their operations. In addition, some undamaged local data centers were inaccessible because of areawide closures. Repairs of key infrastructure centers were delayed because of structural concerns for buildings, and government-ordered evacuations.

These events had a devastating effect on the regional communications infrastructure, but they had little effect on Internet service as a whole. The attack disrupted financial and communications systems, which led to the closing of financial markets for up to 1 week, and interrupted Internet connectivity to several universities, medical colleges, and hospitals and to the city government's official Web site. There were also some far-reaching and unexpected effects: Internet service providers in parts of Europe lost connectivity and there were Domain Name System disruptions in South Africa due to interconnections in New York City. For the Internet as a whole, however, functions were largely back to normal within 15 minutes, and there were no widespread connectivity issues. This demonstrated the flexibility and adaptability of the network. For example, when Internet users were unable to reach popular Web sites because of the high volume of traffic, Internet service providers reduced the complexity of Web sites and reallocated computer resources to handle more traffic. In addition, Internet operators rerouted traffic to bypass the physical damage in lower Manhattan.

In the aftermath of the attack, many Internet service providers increased staffing at network operations centers, coordinated with other service providers, and improvised links to ensure that their networks would continue to run smoothly. However, many problems in restoring telecommunications services were logistical ones, such as obtaining food, fuel, and access to restricted areas.

The federal government's involvement in restoration efforts included facilitating communications and providing logistical support. The government was also responsible for securing the area and providing access to those with need. It also provided military transport to the New York area for key telecommunications personnel when commercial air traffic was shut down.

Source: GAO analysis of report entitled *The Internet Under Crisis Conditions: Learning from September 11*, the National Research Council, National Academy Press: Washington, D.C., 2003, and other published reports.

Figure 8: Case Study—Hurricane Katrina

On August 29, 2005, Hurricane Katrina made landfall in Louisiana and significantly damaged or destroyed the communications infrastructure in Louisiana, Mississippi, and Alabama. According to the Federal Communications Commission, the storm caused outages for over 3 million telephone customers, 38 emergency 9-1-1 call centers, hundreds of thousands of cable customers, and over 1,000 cellular sites. Importantly, the Coast Guard's computer hub in New Orleans dropped off-line, resulting in no computer or Internet connectivity to all coastal ports within the area. Coast Guard units resorted to using telephones and fax machines to communicate.

Source: BellSouth Corporation.

A substantial number of the networks that experienced service disruptions recovered relatively quickly. Many networks were restored during the night and the following morning, and hundreds were restored by August 30. In some cases, local providers restored their own service, while in other cases network service was moved to other providers. According to the Federal Communications Commission, commercial carriers restored service to over 80 percent of the 3 million affected telephone customers within 10 days of Hurricane Katrina. Despite the overall devastation caused by Katrina, the hurricane had minimal affect on the overall functioning of the Internet. According to an Internet-monitoring service provider, while there was a loss of routing around the affected area, there was no significant impact on global Internet routing.

Federal and private-sector officials disagree on how effective the government was in facilitating telecommunications restoration after the storm. According to an NCS official, the organization heightened the alert status of the National Coordinating Center for Telecommunication's 24-hour watch, conducted analyses of critical communications assets in the projected impact area, and activated a National Response Coordination Center. Additionally, the National Coordinating Center and NCS coordinated with the communications companies for various preparations, such as moving personnel to safety, coordinating with fuel and equipment providers, and rerouting communications traffic away from affected areas. NCS officials acknowledged that the scope of the disaster and difficulties coordinating with state officials made these efforts challenging.

Private-sector representatives stated that with the exception of the Federal Communications Commission (which coordinated provision of some governmental resources and information), coordination with the government was limited and virtually no assistance was received. Representatives reported that requests for assistance, such as food, water, fuel, and secure access to facilities, were denied because the Stafford Act (which authorizes such provisioning) does not extend to for-profit companies. These representatives also stated that the government made time-consuming and duplicative requests for information about their networks without identifying how this reporting would be beneficial. Some reported that certain government actions impeded recovery efforts. For example, private security contractors hired by telecommunications companies were not permitted to carry firearms in Louisiana because of licensing rules. In certain cases, the government commandeered fuel destined for telecommunications companies and displaced telecommunications staff from hotels to house federal officials.

Sources: GAO analysis of published reports and testimonies by DHS, FCC, NSTAC, and Renesys as well as interviews with private-sector officials.

The Internet Has Not Yet Experienced a Catastrophic Disruption

Since its inception, the Internet has experienced disruptions of varying scale—from fast-spreading worms, to denial-of-service attacks, to physical destruction of key infrastructure components. However, the Internet has yet to experience a catastrophic disruption. Experts agree—and case studies show—that the Internet is resilient and flexible enough to handle and recover from many types of disruptions. While specific regions may experience Internet disruptions, backup servers and the ability to reroute traffic limit the effect of many targeted attacks. These efforts highlight the importance of recovery planning.

However, it is possible that a complex attack or set of attacks could cause the Internet to fail. It is also possible that a series of attacks against the Internet could undermine users' trust—and thereby reduce the Internet's utility.

Existing Laws and Regulations Apply to the Internet, but Numerous Uncertainties Exist in Using Them for Internet Recovery

Several federal laws and regulations provide broad guidance that applies to the Internet infrastructure, but it is not clear how useful these authorities would be in helping to recover from a major Internet disruption, because some do not specifically address Internet recovery and others have seldom been used. Pertinent laws and regulations address critical infrastructure protection, federal disaster response, and the telecommunications infrastructure (see app. II for additional details).

Specifically, the Homeland Security Act of 2002[18] and Homeland Security Presidential Directive 7[19] establish critical infrastructure protection as a national goal and describe a strategy for cooperative efforts by the government and the private-sector to protect the cyber- and physical-based systems that are essential to the operations of both the economy and the government. These authorities apply to the Internet because it is a core communications infrastructure supporting the information technology and telecommunications sectors. However, this law and regulation do not specifically address roles and responsibilities in the event of an Internet disruption.

[18]The Homeland Security Act of 2002, Pub. L. No. 107-296 (Nov. 25, 2002).

[19]Homeland Security Presidential Directive 7 (Dec. 17, 2003).

Regarding federal disaster response, the Defense Production Act[20] and the Stafford Act[21] provide authority to federal agencies to plan for and respond to incidents of national significance—like disasters and terrorist attacks. Specifically, the Defense Production Act authorizes the President to ensure the timely availability of products, materials, and services needed to meet the requirements of a national emergency. The act is applicable to critical infrastructure protection and restoration, but it has never been used for Internet recovery. The Stafford Act authorizes federal assistance to states, local governments, nonprofit entities, and individuals in the event of a major disaster or emergency. However, the act does not authorize assistance to for-profit companies—such as those that own and operate core Internet components. Several representatives of private companies reported that they were unable to obtain needed resources to restore the communications infrastructure in the aftermath of Hurricane Katrina because the act does not extend to for-profit companies.

Other legislation and regulations, including the Communications Act of 1934[22] and the National Communications System (NCS) authorities,[23] govern the telecommunications infrastructure and help ensure communications during national emergencies. The act governs the regulation of the telecommunications infrastructure upon which the Internet depends. However, coverage of the Internet is subsumed in provisions that govern interstate wire and radio communications, and there is no specific provision governing Internet recovery. NCS authorities establish guidance for operationally coordinating with industry to protect and restore key national security and emergency preparedness communications services. These authorities grant the President certain emergency powers regarding telecommunications, including the authority to require any carrier subject to the Communications Act of 1934 to grant preference or priority to essential communications.[24] The President may also, in the event of war or national emergency, suspend regulations

[20]Act of September 8, 1950, c. 932, 64 Stat. 798, as amended; codified at 50 U.S.C. App. Section 2061 et seq.

[21]Pub. L. No. 93-288, 88 Stat. 143 (1974).

[22]Communications Act of 1934 (June 19, 1934), ch. 652, 48 Stat. 1064.

[23]Executive Order 12472 (Apr. 3, 1984), as amended by Executive Order 13286 (Feb. 28, 2003).

[24]Communications Act of 1934, Section 706, 47 U.S.C § 606.

governing wire and radio transmissions and authorize the use or control of any such facility or station and its apparatus and equipment by any department of the government. Although these authorities remain in force and are implemented in the *Code of Federal Regulations*, they have been seldom used—and never for Internet recovery. Thus, it is not clear how effective they would be if used for this purpose.

In commenting on the statutory authority for Internet reconstitution following a disruption, DHS agreed that this authority is lacking and noted that the government's roles and authorities related to assisting Internet reconstitution following a disruption are not fully defined. In a written response, DHS attorneys identified several statutes and other authorities that provide authority for the NCS telecommunications response functions in a situation involving national security and emergency preparedness. DHS stated the following:

"The Internet infrastructure is owned and operated by the private sector. Although certain policies direct DHS to work with the private sector to ensure infrastructure protection, DHS does not have the authority to direct Internet owners and operators in their recovery efforts."

DHS Initiatives Supporting Internet Recovery Planning Are under Way, but Much Remains to Be Done and the Relationships among Initiatives Are Not Evident

DHS has begun a variety of initiatives to fulfill its responsibility for developing an integrated public/private plan for Internet recovery, but these efforts are not complete or comprehensive. Specifically, DHS has developed high-level plans for infrastructure protection and national disaster response, but the components of these plans that address the Internet infrastructure are not complete. In addition, DHS has started a variety of initiatives to improve the nation's ability to recover from Internet disruptions, including working groups to facilitate coordination and exercises in which government and private industry practice responding to cyber events. While these activities are promising, some initiatives are not complete, others lack time lines and priorities, and still others lack effective mechanisms for incorporating lessons learned. In addition, the relationships among these initiatives are not evident. As a result, the nation is not prepared to effectively coordinate public/private plans for recovering from a major Internet disruption.

DHS Has Developed High-level Protection and Response Plans, but Key Components Are Not Complete

Federal policy establishes DHS as the central coordinator for cyberspace security efforts and tasks the department with developing an integrated public/private plan for Internet recovery.[25] DHS has two key documents that guide its infrastructure protection and recovery efforts, but components of these plans dealing with Internet recovery are not complete.

The *National Response Plan* is DHS's overarching framework for responding to domestic incidents. The plan, which was released in December 2004, contains the following two components that address issues related to telecommunications and the Internet:

- The Emergency Support Function 2 of the plan identifies federal actions to provide temporary emergency telecommunications during a significant incident and to restore telecommunications after the incident. It assigns roles and responsibilities to different federal agencies; provides guidelines for incident response; and identifies actions to take before, during, and after the incident. Because the Internet is supported by the telecommunications infrastructure, this section of the plan could help with Internet recovery efforts.

- The Cyber Incident Annex identifies policies and organizational responsibilities for preparing for, responding to, and recovering from cyber-related incidents impacting critical national processes and the national economy. The annex recognizes the National Cyber Response Coordination Group as the principal federal interagency mechanism to coordinate the government's preparation for, response to, and recovery from a major Internet disruption or significant cyber incident.

These components, however, are not complete in that the Emergency Support Function 2 does not directly address Internet recovery, and the Cyber Incident Annex does not reflect the National Cyber Response Coordination Group's current operating procedures. DHS officials acknowledged that both Emergency Support Function 2 and the Cyber Incident Annex need to be revised to reflect the maturing capabilities of the National Cyber Response Coordination Group, the planned organizational changes affecting NCS and NCSD, and the convergence of voice and Internet networks. However, DHS has not reached consensus on the best

[25]The White House, *National Strategy to Secure Cyberspace*.

approach for revising these components, and it has not established a schedule for revising the overall plan.

The *Draft National Infrastructure Protection Plan* consists of both a base plan and sector-specific plans, but these have not been finalized. A January 2006 draft of the base plan identifies roles, responsibilities, and a high-level strategy for infrastructure protection across all sectors. It emphasizes the need to protect and recover the cyber infrastructure, including the Internet. Additionally, the sector plans are expected to apply the strategies identified in the base plan to the infrastructure sectors. For example, the information technology sector plan identifies relationships within the information technology sector and with other infrastructure sectors. It also identifies preliminary steps for infrastructure protection, such as identifying key assets and the consequences of the failure of those assets.

DHS is planning to finalize its base plan in 2006, but it has not yet set a date for doing so. Once this plan is released, it will lead to the development of the more detailed sector-specific plans. The next versions of the information technology and telecommunications sector plans are due to DHS within 180 days of the release of the final base plan.

While DHS's intentions to revise these plans are necessary steps in the right direction, the plans do not fulfill the department's responsibility to develop an integrated public/private plan for Internet recovery. Several representatives of private-sector firms supporting the Internet infrastructure expressed concerns about both plans, noting that the plans would be difficult to execute in times of crisis. Other representatives were uneasy about the government developing recovery plans, because they were not confident in the government's ability to successfully execute the plans. DHS officials acknowledged that it will be important to obtain input from private-sector organizations as they refine these plans and initiate more detailed public/private planning.

Until both the *National Response Plan* and the *National Infrastructure Protection Plan* are updated and more detailed public/private planning begins, DHS lacks the integrated approach to Internet recovery called for in the cyberspace strategy and risks not being prepared to effectively coordinate such a recovery.

Other DHS Initiatives Related to Internet Recovery Planning Are under Way, but They Are Incomplete and the Relationships among the Initiatives Are Not Evident

While the *National Response Plan* outlines an overall framework for incident response, it is designed to be supplemented by more specific plans and activities. DHS has numerous initiatives under way to better define its ability to assist in responding to major Internet disruptions. These initiatives include task forces, working groups, and exercises. While these activities are promising, some initiatives are incomplete, others still lack time lines and priorities, and others lack an effective mechanism for incorporating lessons learned. In addition, the relationships and interdependencies among different initiatives are not evident.

As a result, tangible progress toward improving the government's ability to help recover from a major Internet disruption has been limited.

DHS Plans to Revise the Role and Mission of the National Communications System, but This Effort Is Not Yet Complete

DHS plans to revise the role and mission of the National Communications System (NCS) to reflect the convergence of voice and data communications, but this effort is not yet complete. NCS is responsible for ensuring the availability of a viable national security and emergency preparedness communications infrastructure. Originally focused on traditional telephone service, NCS has recently taken on a larger role in Internet-related issues due to the convergence of the infrastructures that serve traditional telephone traffic and those that serve data (such as Internet traffic). A presidential advisory committee on telecommunications[26] has established two task forces to recommend changes to NCS's role, mission, and functions to reflect this convergence. One task force focused on changes due to next-generation network technologies, while the other focused on revising the role and mission of NCS's National Communications Center. Appendix III provides additional details on the two task forces.

Both task forces have made recommendations to improve NCS's operations, but DHS has not yet developed plans to address these recommendations. Until NCS completes efforts to revise its role and mission, the group is at risk of not being prepared to address the unique issues that could be caused by future Internet disruptions.

[26]The National Security Telecommunications Advisory Committee advises the President on issues and problems related to implementing national security and emergency preparedness telecommunications policy.

National Cyber Response Coordination Group Is Defining Its Roles and Responsibilities, but Much Remains to Be Done

As a primary entity responsible for coordinating governmentwide responses to cyber incidents—such as major Internet disruptions—DHS's National Cyber Response Coordination Group is working to define its roles and responsibilities, but much remains to be done. The group reported that it has begun efforts to define its roles, responsibilities, capabilities, and activities. For example, the group has developed a concept of operations—which includes a high-level recovery function—but is waiting for the results of additional analyses before revising and enhancing the concept of operations. The group also drafted operating procedures that it used during a national cyber exercise in February 2006, and it plans to incorporate lessons learned from the exercise into the operating procedures and to issue revised procedures by June 2006. The group also reported that it has made progress on initiatives to (1) map the current capabilities of government agencies to detect, respond to, and recover from cyber incidents; (2) identify secure communications capabilities within the government that can be used to respond to cyber incidents; (3) perform a gap analysis of different agencies' capabilities for responding to cyber incidents; and (4) establish formal resource-sharing agreements with other federal agencies as well as state and local governments. However, much remains to be done to complete these initiatives.

One challenge facing the National Cyber Response Coordination Group is the "trigger" for government involvement. Currently, the group can be activated by

- a cyber incident that may relate to or constitute a terrorist attack, a terrorist threat, a threat to national security, a disaster, or any other cyber emergency requiring federal government response;
- a confirmed, significant cyber incident directed at one or more national critical infrastructures;
- a cyber incident that impacts or potentially impacts national security, national economic security, public health or safety, or public confidence and morale;
- discovery of an exploitable vulnerability in a widely used protocol;
- other complex or unusual circumstances related to a cyber incident that requires interagency coordination; or
- any cyber incident briefed to the President.

DHS officials acknowledged that the trigger to activate this group is imprecise and will need to be clarified. Because key activities to define roles, responsibilities, capabilities, and the appropriate trigger for government involvement are still under way, the group is at risk of not being able to act quickly and definitively during a major Internet disruption.

The Internet Disruption Working Group Was Established to Work with the Private Sector to Establish Plans to Respond to Major Internet Disruptions, but It Lacks Time Lines and Priorities for Its Initiatives

Since most of the Internet is owned and operated by the private sector, NCSD and NCS established the Internet Disruption Working Group to work with the private sector to establish priorities and develop action plans to prevent major disruptions of the Internet and to identify recovery measures in the event of a major disruption. The group includes representatives of both domestic and international government agencies and private Internet-related companies. According to DHS officials who organized the group, the group held its first forum in November 2005 to begin to identify real versus perceived threats to the Internet, refine the definition of an Internet disruption, determine the scope of a planned analysis of disruptions, and identify near-term protective measures.

DHS officials stated that they had identified a number of potential future plans, including meeting with industry representatives to

- better understand what constitutes normal network activity and what suggests malicious activity;
- further refine the definition of an Internet disruption;
- determine which public/private organizations would be contacted in an emergency and what contingency plans the government could establish;
- encourage implementation of best practices for protecting key Internet infrastructure, including the Domain Name System; and
- consider requiring improved security technologies for the Domain Name System and the Border Gateway Protocol in government contracts.

Efforts such as those previously mentioned appear to be worthwhile; however, agency officials have not yet finalized plans, resources, or milestones for these efforts. Until they do, the benefits of these efforts will not be fully realized.

The North American Incident Response Group Is an Additional Mechanism for Outreach to the Private Sector, but Its Efforts Are Early

In addition to the Internet Disruption Working Group, US-CERT officials formed the North American Incident Response Group. The group, modeled on similar groups in Asia and Europe, includes both public and private-sector network operators who would be the first to recognize and respond to cyber disruptions. In September 2005, US-CERT officials conducted regional workshops with group members to share information on structure and programs and incident response, and to seek ways for the government and industry to work together operationally. The attendees included 32 organizations, such as computer security incident response teams; information sharing and analysis centers; members of private firms that provide security services; information technology vendors; and other organizations that participate in cyber watch, warning, and response functions. US-CERT officials stated that these events were highly successful, and that they hope to continue to hold such events quarterly beginning in 2006.

As a result of the first meetings, US-CERT officials developed a list of action items and assigned milestones to some of these items. For example, US-CERT has established a secure instant messaging capability to communicate with group members. In addition, it plans to conduct a survey of the group members to determine what they need from US-CERT and what types of information they can provide.

While the outreach efforts of the North American Incident Response Group are promising, DHS has only just begun developing plans and activities to address the concerns of private-sector stakeholders.

DHS Has Conducted Initial Exercises That Address Cyber Disruption, but Efforts to Incorporate Lessons Learned into DHS Operations Are Lacking

Over the last few years, DHS has conducted several broad intergovernmental exercises to test regional responses to significant incidents that could affect the critical infrastructure. These regional exercises included incidents that could cause localized Internet disruptions, and they resulted in numerous findings and recommendations regarding the government's ability to respond to and recover from a major Internet disruption. For example, selected exercises found that both the government and private-sector organizations were poorly prepared to effectively respond to cyber events. They cited the lack of clarity on roles and responsibilities, the lack of coordination and communication, and a limited understanding of cybersecurity concerns as serious obstacles to effective response and recovery from cyber attacks and disruptions. Furthermore, regional participants reported being unclear regarding who was in charge of incident management at the local, state, and national levels.

More recently, in February 2006, DHS conducted an exercise called Cyber Storm, which was focused primarily on testing responses to a cyber-related incident of national significance. The exercise involved a simulated large-scale attack affecting the energy and transportation infrastructures, using the telecommunications infrastructure as a medium for the attack. The results of this exercise have not yet been published. (Details on these exercises are provided in app. IV.)

Exercises that include Internet disruptions can help to identify issues and interdependencies that need to be addressed. However, DHS has not yet identified planned activities and milestones or identified which group should be responsible for incorporating into its plans and initiatives lessons learned from the regional and Cyber Storm exercises. Without a coordination process, plans, and milestones, there is less chance that the lessons learned from the exercises will be successfully transferred to operational improvements.

The Relationships and Interdependencies among Various DHS Initiatives Are Not Evident

While DHS has various initiatives under way—including efforts to update the *National Response Plan*, task forces assessing changes to NCS, working groups on responding to cyber incidents, and exercises to practice recovery efforts—the relationships and interdependencies among these various efforts are not evident. For example, plans to update the *National Response Plan* to better reflect the Internet infrastructure are related to task force efforts to suggest changes to NCS to deal with the convergence of voice and data technologies. However, it is not clear how these initiatives are being coordinated. Furthermore, the National Cyber Response Coordination Group, the Internet Disruption Working Group, and the North American Incident Response Group are all meeting to discuss ways to address Internet recovery, but the interdependencies among the groups have not been clearly established. Additionally, it is not evident that lessons learned from the various cyber-related exercises are being incorporated in the planned revision of the *National Response Plan* or the ongoing efforts of the various working groups. Without a thorough understanding of the interrelationships among its various initiatives, DHS risks pursuing redundant efforts and missing opportunities to build on related efforts.

DHS officials acknowledged that they have not yet fully coordinated the various initiatives aimed at enhancing the department's ability to help respond to and recover from a major Internet disruption, but they noted

that the complexity of this undertaking and the number of entities involved in Internet recovery make this effort challenging.

Multiple Challenges Exist to Planning for Recovery from Internet Disruptions

Although DHS has various initiatives under way to improve Internet recovery planning, it faces key challenges in developing a public/private plan for Internet recovery, including (1) innate characteristics of the Internet that make planning for and responding to a disruption difficult, (2) a lack of consensus on DHS's role and on when the department should get involved in responding to a disruption, (3) legal issues affecting DHS's ability to provide assistance to restore Internet service, (4) reluctance of the private-sector to share information on Internet disruptions with DHS, and (5) leadership and organizational uncertainties within DHS. Until it addresses these challenges, DHS will have difficulty achieving results in its role as the focal point for recovering the Internet from a major disruption.

Key Internet Characteristics Make Recovery More Difficult

The Internet's diffuse structure, vulnerabilities in its basic protocols, and lack of agreed-upon performance measures make planning for and responding to a disruption more difficult.

Control of the Internet Is Diffuse

The diffuse control of the Internet makes planning for recovering from a disruption more challenging. The components of the Internet are not all governed by the same organization. Some components of the Internet are controlled by government organizations, while others are controlled by academic or research institutions. However, the vast majority of the Internet is owned and operated by the private sector. Each organization makes decisions to implement or not implement various standards based on issues such as security, cost, and ease of use. Therefore, any plan for responding to a disruption requires the agreement and cooperation of these private-sector organizations.

In addition, the Internet is international. According to private-sector estimates, only about 20 percent of Internet users are in the United States. Cyber actors in one country have the potential to impact systems connected to the Internet in another country. This geographical diversity makes planning for Internet recovery more difficult.

Vulnerabilities in Internet-Related Protocols Make Responding to Disruptions Difficult

The Internet's protocols have vulnerabilities that can be exploited. Examples of these vulnerabilities include the following:

- The version of Internet Protocol (IPv4) that is widely used today has certain security limitations that have been addressed but are not fully integrated into the protocol. The newest version of the protocol (IPv6) addresses some of these limitations, but it has not yet been fully adopted.[27]

- The Domain Name System, which directs users to the correct Web site based on the name they typed in, was not originally built with the intent of being resistant to attacks. Domain name servers or caches storing Domain Name System information can be corrupted. Although some protective measures have been implemented, a method to encrypt and protect Domain Name System information has not yet been widely deployed.

- Border Gateway Protocol, the protocol that transmits routing information among separate networks, has vulnerabilities that, if not mitigated, could subject those networks to attack. For example, a malicious actor could advertise incorrect routing information. Because this protocol provides the basis for all Internet connectivity, a successful attack could have wide-ranging effects.

Lack of Standards for Measuring Internet Performance Hinders the Ability to Recognize Disruptions and Recover Accordingly

There are no well-accepted standards for measuring and monitoring the Internet infrastructure's availability and performance. Instead, individuals and organizations rate the Internet's performance according to their own priorities.

The commonly used version of Internet Protocol (IPv4) does not guarantee a priority or speed for delivery, but rather provides "best effort" service. The next version (IPv6) has features that may help the delivery of future Internet traffic, but it is not yet widely used.[28] The topic of guaranteeing a particular level of service, called "quality of service," is currently the subject of much research. For example, NCS requested information from private companies on the potential for prioritizing certain types of Internet service over others if network capacity was limited; NCS found that there is

[27]GAO-05-471.

[28]GAO-05-471.

currently no offering of a priority service, nor is there any consensus by industry on a standard approach to prioritization. Obstacles to offering the service include both technical and financial challenges. Since there are no clear standards for quality of service, prioritizing service if capacity is limited or setting thresholds that indicate a disrupted network can be difficult.

Private-sector representatives identified additional challenges to network measurement and performance standards, including a reluctance to share proprietary performance data that other companies could use for competitive advantage, flaws in measurement techniques, and the ability to "spoof" performance data.

The lack of agreement on standards for measurement and performance limits the ability of the government and private sector to readily identify poor performance and identify when recovery efforts should begin.

There Is No Consensus on DHS's Role in Responding to Internet Disruption or the Appropriate Trigger for Its Involvement

There is a lack of consensus about the role DHS should play in responding to a major Internet disruption and about the appropriate trigger for its involvement. As we previously noted in this report, the lack of clear legislative authority for Internet recovery efforts complicates the definition of this role.

DHS's Role Lacks Consensus

DHS is currently providing information to private industry through existing US-CERT and National Coordinating Center relationships and conducting exercises such as Cyber Storm. US-CERT and National Coordinating Center officials are also working to improve their relationships with the private sector. However, DHS officials acknowledged that their role in recovering from an Internet disruption needs additional clarification, because private industry owns and operates the vast majority of the Internet.

Private-sector officials representing telecommunication backbone providers and Internet service providers were also unclear about the types of assistance DHS could provide in responding to an incident and about the value of such assistance. While many officials stated that the government did not have a direct recovery role, others identified a variety of roles ranging from providing information on specific threats (which DHS currently does through US-CERT), providing security and disaster relief support during a crisis, funding backup communication infrastructures,

and driving improved Internet security through requirements for its own procurement. Clearly, there was no consensus among the officials on this issue. Table 6 summarizes potential roles suggested by private-sector representatives and DHS officials' assessments of each area.

Table 6: Potential DHS Roles

Potential role	DHS assessment of activities
Serve as a focal point with state and local governments to establish standard credentials to allow Internet and telecommunications companies access to areas that have been restricted or closed in a crisis.	NCS officials stated that credentials are primarily controlled by state and local government officials. However, NCS stated that it is working with a telecommunications company and Georgia on a pilot credentialing process for telecommunications and electric power teams in a disaster area to restore critical infrastructure. Once the pilot process is generally agreed to with Georgia officials, NCS stated it will share this information with other state and local officials to provide them with the option of adopting it the next hurricane season. The agency may consider a formal credentialing system for the next hurricane season.
Provide logistical assistance, such as fuel, power, and security, to Internet infrastructure operators.	NCS currently does not provide such services directly, and the Stafford Act does not authorize DHS to provide direct assistance to private companies. However, the National Coordinating Center has assisted companies in obtaining these services from other companies in previous physical disruptions. An NCS official acknowledged that providing these services in the case of Hurricane Katrina was challenging because of the scale of the disaster and difficulties in coordination with other government organizations.
Conduct a more formal analysis of physical diversity in service routes so that a customer with multiple telecommunications vendors would be able to determine the extent to which the vendors' circuits physically overlap.	NCS stated it has developed a formal analysis process to assist federal agencies in conducting analyses of physical diversity in service routes for any given site. The formal NCS analysis process requires full collaboration between NCS and the requesting agency. An abbreviated analysis process is also available for those agencies wishing to conduct their analyses independently. However, DHS stated that an overall analysis of physical diversity in service routes for all federal agency locations would be a massive undertaking. It would also be extremely expensive and is currently beyond even industry's capability to maintain.
Focus on smaller scale exercises targeted at specific Internet disruption issues. An example would be an exercise focused on root server/top-level domain attacks.	DHS officials stated that they agree with this premise and are planning a tabletop exercise specifically focused on the Internet. A group of government and private-sector experts first met to plan the exercise in March 2006. The exercise is currently planned for June 2006.
Limit the initial focus for Internet recovery planning to key national security and emergency preparedness functions, such as public health and safety, similar to NCS's approach to telephone service. This would make the scope of planning efforts more manageable.	DHS officials agree that this may be a more appropriate place to start. They stated that a focus on these areas would likely be more positively received by the private sector than larger scale planning efforts. However, they stated that this prioritization will require discussions among stakeholders. These officials noted that the Next Generation Network Task Force addressed prioritization. However, there are no immediate plans that target this particular issue.

(Continued From Previous Page)

Potential role	DHS assessment of activities
Fund backup communications systems.	NCS initiated a program, called the Shared Resources High-Frequency Radio Program, to provide backup radio communications during an emergency. The purpose of the program is to provide a single, interagency emergency message-handling system by bringing together existing radio resources of federal, state, and industry organizations when normal communications are destroyed or unavailable for the transmission of national security and emergency preparedness information. In addition, DHS operates the Critical Infrastructure Warning Information Network, a private communications network designed to serve as a reliable and survivable network capability with no logical dependency on the Internet or the public-switched network. In the event of a significant cyber attack that disrupts telecommunications networks and/or the Internet, this network is expected to provide a secure capability for interagency incident managers to communicate. DHS plans to extend the network to private-sector communications backbone providers.
Establish a system for prioritizing recovery of Internet service similar to the existing Telecommunications Service Priority Program.	DHS officials and industry representatives noted that the existing Telecommunications Service Priority Program applies to physical restoration of both voice circuits and data circuits, including Internet traffic. However, prioritization of particular traffic on the Internet faces numerous technical challenges and is not supported by current legislation. DHS stated that this issue will become more significant as existing telecommunications circuit-switched networks migrate to packet-switched networks.
Use federal contracting mechanisms to require use of more secure Internet technologies, such as secure Domain Name System and secure Border Gateway Protocols.	DHS officials noted that they can coordinate with the Office of Management and Budget in addressing this issue, but that the office has authority for providing federal agencies with overarching policy. They also stated that DHS's Science and Technology Directorate and the National Institute of Standards and Technology have developed guidance documents to encourage the use of a secure Domain Name System in federal information technology systems. The Science and Technology Directorate is also coordinating with the General Services Administration to begin to implement a secure Domain Name System in the .gov and global root Domain Name System servers. These officials noted that standards for securing Border Gateway Protocol are still not fully agreed to—beyond some common best practices for simple security—and that DHS and the National Institute of Standards and Technology are working to develop standards and technology to support securing Border Gateway Protocol. These officials cautioned that expenses and the timing of implementation are key issues. Federal agencies can specify what they want, but ultimately the costs of enhanced services will have to be paid.

Sources: GAO interviews with private-sector infrastructure owners and operators to identify potential roles and a written assessment by DHS on these potential roles.

The Trigger for Government Involvement Is Unclear

The difference between a minor and a major Internet disruption can be a combination of factors. The severity of a disruption can be influenced by

- the length of time that the disruption lasts;
- the impact of the disruption on the operation of the Internet, both in quality of operation (e.g., if the speed of the Internet is affected), and the number of users that cannot access the Internet;
- the impact that the disruption has on society, such as the impact on national security or economic security; and
- the simultaneity of events (e.g., a disruption coinciding with a national disaster or terrorist attack could be more severe than a disruption occurring on an uneventful day).

However, it is not clear when the government should get involved in a disruption. For example, the lessons learned from the DHS-sponsored regional exercises show that

- organizations do not know how and to whom they should report a cyber attack and what information to convey;
- local and state emergency operations centers often lack procedures to determine when they should activate for a cyber event;
- private-sector participants often do not inform government authorities about what they see as routine events because of company policy, legal constraints, or liability concerns; and
- it is unclear when a cybersecurity incident becomes a source of concern and what types of incidents should be communicated to local and federal law enforcement.

The trigger for the *National Response Plan*, which is DHS's overall framework for incident response, is poorly defined and has been found by both GAO and the White House to need revision.[29] DHS officials acknowledged that the definition for activation of its National Cyber Response Coordination Group is very broad and needs clarification. In

[29]GAO, *Hurricane Katrina: GAO's Preliminary Observations Regarding Preparedness, Response, and Recovery*, GAO-06-442T (Washington, D.C.: Mar. 8, 2006); and the White House, *The Federal Response to Hurricane Katrina: Lessons Learned* (Washington, D.C.: February 2006).

addition, other DHS officials stated that, in their meetings with private-sector firms and other government agencies, they have determined that they need to further refine the definition of when government should be involved during an Internet disruption.

DHS officials have stated that a successful public/private partnership is critical to the success of efforts to plan for responding to Internet disruptions. Since private-sector participation in DHS planning activities for Internet disruption is voluntary, agreement on the appropriate trigger for government involvement and on the role of government in resolving an Internet disruption are essential to any plan's success. Without a consensus on the appropriate role of government in responding to the disruption, or on the trigger for government involvement, planning for response to the disruption is difficult.

Legal Issues Affect DHS's Ability to Provide Assistance during Recovery Efforts

There are key legal issues affecting DHS's ability to provide assistance to help restore Internet service. As previously noted, key legislation and regulations guiding critical infrastructure protection, disaster recovery, and the telecommunications infrastructure do not provide specific authorities for Internet recovery. As a result, there is no clear legislative guidance on what government entity would be responsible in the case of a major Internet disruption.

In addition, while the Stafford Act authorizes the government to provide federal assistance to states, local governments, nonprofit entities, and individuals in the event of a major disaster or emergency, it does not authorize assistance to for-profit corporations. Several representatives of telecommunications companies reported that they had requested federal assistance from DHS during Hurricane Katrina. Specifically, they requested food, water, and security for the teams they were sending in to restore the communications infrastructure, and fuel to power their generators. DHS responded that it could not fulfill these requests, noting that the Stafford Act did not extend to for-profit companies.

Many in the Private Sector Are Reluctant to Share Internet Information with the Government

Because a large percentage of the nation's critical infrastructure—including the Internet—is owned and operated by the private sector, public/private partnerships are crucial for successful critical infrastructure protection. Although certain policies direct DHS to work with the private sector to ensure infrastructure protection, DHS does not have the authority to direct Internet owners and operators in their recovery

efforts. Instead, it must rely on the private sector to share information on incidents, disruptions, and recovery efforts.

We have previously reported that many in the private sector are reluctant to share information with the federal government.[30] Many private-sector representatives questioned the value of providing information to DHS regarding planning for and recovery from Internet disruption. Concerns included the potential for disclosure of the information and the perceived lack of benefit in providing the information. In addition, DHS identified provisions of the Federal Advisory Committee Act[31] as having a "chilling effect" on cooperation with the private sector. The act governs the structure of certain federal advisory groups and requires that membership in and information about the groups' activities be public record. However, both the act itself and other federal legislation provide the ability to limit disclosure of sensitive information provided to the government. While DHS officials stated that the agency was working on a solution to problems posed by the act, they did not provide us with information on potential solutions or milestones for completing these activities. The uncertainties regarding the value and risks of cooperation with the government limit incentives for the private sector to cooperate in Internet recovery planning efforts.

DHS's Leadership and Organizational Issues Impact Its Ability to Address Internet Disruption

In 2003 and again in 2005, we identified the transformation of DHS from 22 agencies into one department as a high-risk area.[32] As part of this body of work, we noted that organizational and management practices are critical to successfully transforming an organization. Additionally, we reported on the importance of top leadership driving any transformation and the need for a stable and authoritative organizational structure. However, DHS has lacked permanent leadership while developing its plans for Internet recovery and reconstitution. In addition, the organizations with roles in Internet recovery have overlapping responsibilities and may be reorganized

[30]GAO, *Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information*, GAO-06-383 (Washington, D.C.: Apr. 17, 2006); *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: Mar. 17, 2006); and GAO-05-434.

[31]Pub. L. No. 92-463, 86 Stat. 770 (1972) codified at 5 U.S.C. app. 2.

[32]GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005); and *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003).

once DHS selects permanent leadership. As a result, it is difficult for DHS to develop a clear set of organizational priorities and to coordinate among the various activities responsible for Internet recovery planning.

DHS Has Lacked Permanent Leadership in Key Roles

In recent years, DHS has experienced a high level of turnover in its cybersecurity division and has lacked permanent leadership in key roles. In May 2005, we reported that multiple senior DHS cybersecurity officials had recently left the department.[33] These officials included the NCSD Director, the Deputy Director responsible for Outreach and Awareness, 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.

Subsequently, in July 2005, the DHS Secretary announced a major reorganization of the department. Under this reorganization, the Information Analysis and Infrastructure Protection Directorate, which contained NCS and NCSD, was renamed the Directorate for Preparedness, which would be managed by an appointed under secretary. The responsibilities of NCS and NCSD were placed under a new Assistant Secretary for Cyber Security and Telecommunications. DHS stated that the creation of a position for Assistant Secretary for Cyber Security and Telecommunications within the department would elevate the position of cybersecurity in the department and by doing so raise visibility for the issue. However, as of May 2006, no candidate for the assistant secretary position had yet been publicly announced. In addition, the current head of NCSD is in an acting position and has been since October 2004.

While DHS stated that the lack of a permanent assistant secretary has not hampered its efforts in protecting critical infrastructure, several private-sector representatives stated that DHS's lack of leadership in this area has limited progress. Specifically, these representatives stated that filling key leadership positions would enhance DHS's visibility to the Internet industry and potentially improve its reputation.

DHS Organizations Have Overlapping Responsibilities

DHS officials acknowledged that the current organizational structure has overlapping responsibilities in planning for and recovering from a major Internet disruption. NCSD is responsible for planning and response activities governing information technology, while NCS has the lead for

[33] GAO-05-434.

telecommunications. However, because of the convergence of voice and data networks, NCS has become more involved in Internet issues.

There is currently no written division of responsibilities between NCS and NCSD related to Internet recovery. NCS officials stated that a revision of the Emergency Support Function 2 would help address the apparent overlap, but DHS has not established a date for finalizing this document. Furthermore, DHS officials stated that the new assistant secretary would have discretion to reorganize NCS and NCSD. For example, NCS and NCSD could be combined, or one or more program areas could be modified. As a result, it is difficult for DHS to develop a clear set of organizational priorities and to coordinate among the various activities responsible for Internet recovery planning.

Conclusions

As a critical information infrastructure supporting our nation's commerce and communications, the Internet is subject to disruption—from both intentional and unintentional incidents. While major incidents to date have had regional or local impacts, the Internet has not yet suffered a catastrophic failure. Should such a failure occur, however, existing legislation and regulations supporting critical infrastructure protection, disaster response, and the telecommunications infrastructure do not specifically address roles and responsibilities for Internet recovery.

A national policy, the *National Strategy to Secure Cyberspace*, establishes DHS as the focal point for ensuring the security of cyberspace—a role that includes developing joint public/private plans for facilitating a recovery from a major Internet disruption. While DHS has initiated efforts to refine high-level disaster recovery plans, the components of these plans that pertain to the Internet are not complete. Additionally, while DHS has undertaken several initiatives to improve Internet recovery planning, much remains to be done. Specifically, some initiatives lack clear time lines, lessons learned are not consistently being incorporated in recovery plans, and the relationships between the various initiatives are not clear.

DHS faces numerous challenges to developing integrated public/private recovery plans—not the least of which is the fact that the government does not own or operate much of the Internet. In addition, there is no consensus among public and private stakeholders about the appropriate role of DHS and when it should get involved; legal issues limit the actions the government can take; the private sector is reluctant to share information on Internet performance with the government; and DHS is undergoing

important organizational and leadership changes. As a result, the exact role of the government in helping to recover the Internet infrastructure following a major disruption remains unclear.

Matters for Congressional Consideration

Given the importance of the Internet as a critical infrastructure supporting our nation's communications and commerce, Congress should consider clarifying the legal framework that guides roles and responsibilities for Internet recovery in the event of a major disruption. This effort could include providing specific authorities for Internet recovery as well as examining potential roles for the federal government, such as providing access to disaster areas, prioritizing selected entities for service recovery, and using federal contracting mechanisms to encourage more secure technologies. This effort also could include examining the Stafford Act to determine if there would be benefits in establishing specific authority for the government to provide for-profit companies—such as those that own or operate critical communications infrastructures—with limited assistance during a crisis.

Recommendations for Executive Action

To improve DHS's ability to facilitate public/private efforts to recover the Internet in case of a major disruption, we recommend that the Secretary of the Department of Homeland Security implement the following nine actions:

- Establish dates for revising the *National Response Plan* and finalizing the *National Infrastructure Protection Plan*—including efforts to update key components relevant to the Internet.

- Use the planned revisions to the *National Response Plan* and the *National Infrastructure Protection Plan* as a basis, draft public/private plans for Internet recovery, and obtain input from key Internet infrastructure companies.

- Review the NCS and NCSD organizational structures and roles in light of the convergence of voice and data communications.

- Identify the relationships and interdependencies among the various Internet recovery-related activities currently under way in NCS and NCSD, including initiatives by US-CERT, the National Cyber Response Coordination Group, the Internet Disruption Working Group, the North

American Incident Response Group, and the groups responsible for developing and implementing cyber recovery exercises.

- Establish time lines and priorities for key efforts identified by the Internet Disruption Working Group.
- Identify ways to incorporate lessons learned from actual incidents and during cyber exercises into recovery plans and procedures.
- Work with private-sector stakeholders representing the Internet infrastructure to address challenges to effective Internet recovery by
  - further defining needed government functions in responding to a major Internet disruption (this effort should include a careful consideration of the potential government functions identified by the private sector in table 6 of this report),
  - defining a trigger for government involvement in responding to such a disruption, and
  - documenting assumptions and developing approaches to deal with key challenges that are not within the government's control.

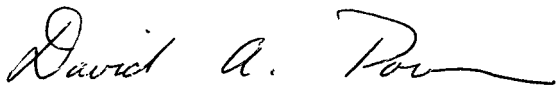
Agency Comments

We received written comments from DHS on a draft of this report (see app. V). In DHS's response, the Director of the Departmental GAO/Office of Inspector General Liaison Office concurred with our recommendations. DHS stated that it recognizes that the Internet is an important component of the information infrastructure in which both the information technology and telecommunications sectors share an interest. It also stated that because of the increasing reliance of various critical infrastructure sectors on interconnected information systems, the Internet represents a significant source of interdependencies for many sectors. DHS agreed that strengthened collaboration between the public and private sectors is critical to protecting the Internet. DHS also provided information on initial actions it is taking to implement our recommendations.

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.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the report date. At that time, we will send copies of this report to interested congressional committees, the Secretary of the Department 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 us at (202) 512-9286 and at (202) 512-6412, or by e-mail at pownerd@gao.gov and rhodesk@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 VI.



David A. Powner
Director, Information Technology Management Issues

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

List of Congressional Requesters:

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

The Honorable Tom Coburn, MD
Chairman
The Honorable Tom Carper
Ranking Member
Subcommittee on Federal Financial Management,
Government Information, and International Security
Committee on Homeland Security
and Governmental Affairs
United States Senate

The Honorable Joe Barton
Chairman
Committee on Energy and Commerce
House of Representatives

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

Objectives, Scope, and Methodology

Our objectives were to (1) identify examples of major disruptions to the Internet, (2) identify the primary laws and regulations governing recovery of the Internet in the event of a major disruption, (3) evaluate the Department of Homeland Security's (DHS) plans for facilitating recovery from Internet disruptions, and (4) assess challenges to such efforts.

To determine the types of major disruptions to the Internet, we analyzed our prior work on cybersecurity issues as well as reports by private organizations, research experts, and government agencies. We identified incidents that were representative of types of disruptions that have actually occurred. We compiled case studies by reviewing and summarizing research reports and interviewing private-industry experts and government officials. We also conducted interviews with individuals in the private/public sectors, including representatives of private companies that operate portions of Internet infrastructure.

To determine the primary laws and regulations for recovering the Internet in the event of a major disruption, we analyzed relevant laws and regulations related to infrastructure protection, disaster response, and the telecommunications infrastructure. These laws and regulations included the Homeland Security Act of 2002, Homeland Security Presidential Directive 7, the Defense Production Act, the Stafford Act, the Communications Act of 1934, and the National Communications System (NCS) authorities. We also obtained the perspectives of DHS and the Federal Communications Commission on the laws and regulations that govern Internet recovery. Additionally, we conducted interviews with DHS and other government officials as well as representatives of the telecommunications and information technology sectors.

To assess plans for recovery of Internet service in the event of a major disruption, we analyzed key documents, such as the interim *National Infrastructure Protection Plan*, the *National Response Plan*, a report from the National Coordinating Center Task Force, and reports from regional tabletop security exercises. We observed a portion of DHS's Cyber Storm exercise, which focused on facilitating government and private industry organizations to address an array of cybersecurity issues. We also spoke with the Deputy Manager of NCS and the Deputy Director of the NCSD to identify DHS's initiatives in the area of Internet protection and recovery. Additionally, we interviewed representatives from private companies that operate portions of Internet infrastructure. These included representatives of major telecommunications and cable companies, Internet service providers, and root server operators. We also interviewed representatives

from three information sharing and analysis centers[1] to obtain their perspectives on DHS's capabilities in the area of Internet recovery.

To identify the challenges that may affect current recovery plans, we analyzed DHS plans, congressional testimony, and other evaluations of challenges to Internet recovery. We also interviewed officials at DHS, including NCSD's Deputy Director of Strategic Initiatives and Deputy Director of Operations and NCS's Chief of the Critical Infrastructure Protection Division. In addition, we interviewed other agencies that are involved with the government's efforts in the area of Internet recovery and experts in the private sector and academia. We performed our work from August 2005 to May 2006 in accordance with generally accepted government auditing standards.

[1]These were the Telecommunications, Information Technology, and Multi-State Information Sharing and Analysis Centers.

Legislation and Regulations Govern Critical Infrastructure Protection, Disaster Response, and the Telecommunications Infrastructure

Multiple Laws and Regulations Govern Protection of Critical Infrastructure

Federal laws and policies establish critical infrastructure protection as a national goal and describe a strategy for cooperative efforts by government and the private sector to protect the cyber- and physical-based systems that are essential to the minimum operations of the economy and the government. The primary authorities governing protection of critical infrastructure include the Homeland Security Act of 2002 and Homeland Security Presidential Directive 7.

The Homeland Security Act of 2002

The Homeland Security Act of 2002[1] 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 the recovery from attacks that do occur.

The act also assigns DHS a number of responsibilities for critical infrastructure protection, 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, or preemption of or response to terrorist attacks.

Additionally, the act specifically charged DHS with providing state and local government entities and, upon request, private entities that own or operate critical infrastructure, with

- analyses and warnings concerning vulnerabilities and threats to critical infrastructure systems,
- crisis management support in response to threats or attacks on critical information systems, and
- technical assistance with respect to recovery plans to respond to major failures of critical information systems.

[1]Pub. L. No. 107-296 (Nov. 25, 2002).

Homeland Security Presidential Directive 7

Homeland Security Presidential Directive 7, dated December 17, 2003, 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. The directive defines responsibilities for (1) DHS, (2) sector-specific federal agencies that are responsible for addressing specific critical infrastructure sectors, and (3) other departments and agencies.

The directive also makes DHS responsible for coordinating the national effort to enhance the protection of the critical infrastructure and key resources of the United States. Under the directive, the Secretary of DHS is to serve as the principal federal official to lead, integrate, and coordinate implementation of efforts among federal departments and agencies, state and local governments, and the private sector to protect critical infrastructure and key resources. The Secretary also is to work closely with other federal departments and agencies, state and local governments, and the private sector in accomplishing the objectives of the directive. The Secretary is given responsibility to coordinate protection activities for several key infrastructure sectors, including the information technology and telecommunications sectors.

Homeland Security Presidential Directive 7 provides that DHS is to collaborate with the appropriate private-sector entities and to encourage the development of information-sharing and analysis mechanisms. Additionally, the department and sector-specific agencies are to collaborate with the private sector and continue to support sector-coordinating mechanisms to

- identify, prioritize, and coordinate the protection of critical infrastructure and key resources and
- facilitate sharing of information about cyber and physical threats, vulnerabilities, incidents, potential protective measures, and best practices.

Multiple Laws Govern Federal Response to Disasters and Incidents of National Significance

Federal planning for disaster recovery is governed by legislation including the Defense Production Act and the Stafford Act.

Defense Production Act

The Defense Production Act was enacted at the outset of the Korean War to ensure the availability of industrial resources to meet the needs of the Department of Defense.[2] The act is intended to facilitate the supply and timely delivery of products, materials, and services to military and civilian agencies, in times of peace as well as in times of war. Presently, only titles I, III, and VII of the Defense Production Act remain in effect.[3] DHS identified the act as a primary authority that supports telecommunications emergency planning and response functions.

Title I of the act authorizes the President to ensure the timely availability of products, materials, and services needed to meet current defense preparedness and military readiness requirements as well as the requirements of a national emergency. Under section 101 of the act, the President may require preferential performance on contracts and orders to meet approved national defense requirements and may allocate materials, services, and facilities as necessary to promote the national defense in a national emergency. Homeland Security Presidential Directive 7, previously discussed, specifically acknowledges the authority of the Department of Commerce to use the act to ensure the timely availability of industrial products, materials, and services to meet homeland security requirements.

Title III of the act authorizes the use of financial incentives to expand productive capacity and supply. It authorizes loan guarantees, loans, purchases, purchase guarantees, and installation of equipment in contractor facilities for those goods necessary for national defense. It is used only in cases where domestic sources are required and domestic firms

[2]Act of September 8, 1950, c. 932, 64 Stat. 798, as amended; codified at 50 U.S.C. App. Section 2061 et seq.

[3]Congressional Research Service, David E. Lockwood, *Defense Production Act: Purpose and Scope*, RS20587 (Oct. 16, 2002).

cannot, or will not, act on their own to meet a national defense production need.

Title VII of the Defense Production Act defines national defense to include domestic emergency preparedness and critical infrastructure protection and restoration activities. The act's authorities, therefore, are available to meet requirements in a civil disaster, such as a major Internet disruption.

The act also authorizes the President to provide antitrust defenses to private firms participating in voluntary agreements aimed at solving production and distribution problems.

The Year 2000 computer transition and the September 11, 2001, attacks prompted new interest in the act and its application to information technology and cybersecurity. Some commentators indicated that the act would be a useful tool in managing a critical infrastructure emergency.[4] In January 2001, President Clinton directed the Secretary of Energy to exercise authority under the act, among other statutes, to ensure the availability of natural gas for high-priority uses in California. President Clinton found that ensuring natural gas supplies to California was necessary and appropriate to maximize domestic supplies and to promote the national defense. President Bush subsequently extended this executive order.[5]

In recent years, Congress has expanded the Defense Production Act's coverage to include crises resulting from natural disasters or "man-caused events" not amounting to an armed attack on the United States.[6] The definition of national defense in the act was expanded in 1994 to include

[4]*For example*, Joseph J. Petrillo, "Time to dust off emergency procurement rules?," *Government Computer News* (Nov. 5, 2001); Lee M. Zeichner, "Use of the Defense Production Act for 1950 for Critical Infrastructure Protection," reprinted in *Security in the Information Age; New Challenges, New Strategies*, Joint Economic Committee, United States Congress (May 2002); and Major Federal Legislation, A "Legal Foundations" Study, Report 6 of 12, Report to the President's Commission on Critical Infrastructure Protection (1997).

[5]The California Energy Crisis and Use of the Defense Production Act, Hearing Before the Committee on Banking, Housing, and Urban Affairs, United States Senate, 107th Cong. 1st Sess. (Feb. 9, 2001).

[6]S. Rep. No. 108-156, 108th Cong. 1st Sess. September 30, 2003, at 1-2.

emergency preparedness activities authorized by the Stafford Act.[7] In 2003, the act was reauthorized through September 30, 2008.[8] It was also amended to add explicit authority to use the act for critical infrastructure protection and restoration. In addition, the 2003 Act (section 5) added a definition of critical infrastructure to the act.[9]

The Stafford Act

The Robert T. Stafford Disaster Relief and Emergency Assistance Act (the Stafford Act)[10] authorizes federal assistance to states, local governments, nonprofit entities, and individuals in the event of a major disaster or emergency. For example, the President, at the request of a governor, may declare a "major disaster," which is defined as follows:

"Major disaster means any natural catastrophe (including any hurricane, tornado, storm, high water, winddriven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought), or, regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this Act to supplement the efforts and available resources of States, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby."

A presidential declaration that a major disaster has occurred activates the federal response plan for the delivery of federal disaster assistance. The Federal Emergency Management Agency is responsible for coordinating the federal and private response effort. A presidential declaration of a major disaster[11] triggers several Stafford Act authorities, including, for example, federal activities to

[7]Pub. L. No. 103-337, section 3411(b) (Oct. 5, 1994).

[8]Pub. L. No. 108-195 (Dec. 19, 2003).

[9]That definition reads as follows: "The term 'critical infrastructure' means any systems and assets, whether physical or cyber-based, so vital to the United States that the degradation or destruction of such systems and assets would have a debilitating impact on national security and national public health or safety."

[10]Pub. L. No. 93-288, 88 Stat. 143 (1974).

[11]The Stafford Act also authorizes declaration of an emergency, which has less stringent requirements and triggers less comprehensive forms of assistance. Congressional Research Service, Keith Bea, *Federal Stafford Act Disaster Assistance: Presidential Declarations, Eligible Activities, and Funding*, RL33053 (Jan. 24, 2006).

- support state and local governments to facilitate the distribution of consumable supplies;
- help distribute aid to victims through state and local governments and voluntary organizations, perform life- and property-saving assistance, clear debris, and use the resources of the Department of Defense;
- repair and reconstruct federal facilities;
- repair, restore, and replace damaged facilities owned by state and local governments, as well as private nonprofit facilities that provide essential services or contributions for other facilities or hazard mitigation measures in lieu of repairing or restoring damaged facilities; and
- establish—during or in anticipation of an emergency—temporary communications systems, and make such communications available to state and local government officials.

Specific Laws and Regulations Govern the Telecommunications Infrastructure That Supports the Internet

The Internet is enabled by the telecommunications infrastructure that supports transmission of data. Key laws and regulations include the Communications Act of 1934, as amended, and the National Communications System (NCS) authorities.

Communications Act of 1934, as Amended

The primary federal telecommunications law is the Communications Act of 1934. Its original purpose was to regulate interstate and foreign commerce in communications by wire and radio by licensing radio stations and regulating the telecommunications monopolies of the time.[12] The 1934 Act also created the Federal Communications Commission to implement the act.[13] The 1934 act, as amended, has remained for more than 60 years as the

[12]Congressional Research Service, Charles B. Goldfarb, *Telecommunications Act: Competition, Innovation, and Reform*, RL33034 (Aug. 12, 2005) and 47 U.S.C. 151 et seq.

[13]Communications Act of 1934, June 19, 1934, ch. 652, 48 Stat. 1064.

basis of federal regulation of telecommunications services.[14] The Telecommunications Act of 1996[15] amended the 1934 Act to enhance competition in the telecommunications market. These laws govern regulation of forms of transmission upon which the Internet depends. There is, however, no general regulatory provision for the Internet in the act and no specific provision providing authorities and responsibilities for Internet recovery.

NCS Authorities

NCS was established by a memorandum signed by President Kennedy in 1963, following the Cuban Missile Crisis.[16] The memorandum called for establishing a national communications system by linking together and improving the communication facilities and components of various federal agencies. This original memorandum has since been amended and superseded over time.

The executive order currently in force is Executive Order 12472, April 3, 1984, which was amended slightly by Executive Order 13286 on February 28, 2003. Executive Order 12472, as amended by Executive Order 13286, established NCS and provided that its mission was to assist the President, the National Security Council, the Homeland Security Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Management and Budget in, among other responsibilities, "the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery and reconstitution."

The administrative structure includes a National Communications System Committee of Principals, an executive agent, and a manager. The Homeland Security Act of 2002 transferred NCS to DHS. To reflect this change, Executive Order 13286 made the Secretary of DHS the Executive Agent.

[14]Section 706 of the act, discussed below, grants wartime powers to the President, enabling the federal government to provide telecommunications services deemed critical to national security interest during times of war or national emergency.

[15]Pub. L. No. 104-104, 110 Stat. 56 (1996).

[16]Congressional Research Service, John Moteff, *Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives*, RL32357 (Apr. 16, 2004).

NCS's mission with regard to critical infrastructure protection is to ensure the reliability and availability of telecommunications for national security and emergency preparedness. Its mission includes, but it is not necessarily limited to, responsibility for (1) ensuring the government's ability to receive priority services for national security and emergency preparedness purposes in current and future telecommunications networks by conducting research and development and participating in national and international standards bodies and (2) operationally coordinating with industry for protecting and restoring national security and emergency preparedness services in an all-hazards environment.[17]

Section 706 of the Communications Act of 1934 grants the President certain emergency powers regarding telecommunications, including the authority to grant essential communications "preference or priority with any carrier" subject to this act.[18] The President may also, in the event of war or national emergency, suspend regulations governing wire and radio transmissions and "authorize the use or control of any such facility or station and its apparatus and equipment by any department of the Government." Section 706 is implemented in Executive Order 12472, which provides that the Director of the Office of Science and Technology Policy shall direct the exercise of the war power functions of the President under section 706(a), (c)-(e) of the Communications Act of 1934, as amended (47 U.S.C. 606). Section 706 is implemented in the *Code of Federal Regulations* at title 47, chapter II.

[17]GAO, *Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed*, GAO-02-918T (Washington, D.C.: July 9, 2002).

[18]47 U.S.C. § 606.

Two Task Forces Have Assessed NCS Roles and Mission

The National Security Telecommunications Advisory Committee advises the President on issues and problems related to implementing national security and emergency preparedness telecommunications policy. The committee recently formed two task forces to provide recommendations on changes to DHS's NCS division and operations.

Next Generation Network Task Force

In May 2004, the Next Generation Network Task Force was formed to develop recommendations on changes that needed to be made to NCS as a result of issues such as the convergence of voice and data communications. The task force was to (1) define the expected structure for next-generation networks, such as those using Internet-based protocols; (2) identify national security and emergency preparedness user requirements for next-generation networks and outline how these requirements will be met; and (3) examine relevant user scenarios and expected cyber threats and recommend optimal actions to address these threats.

The task force agreed to present its findings and recommendations in two separate reports to the President—a near-term recommendations report and a final comprehensive report.

In March 2005, the task force issued near-term recommendations for the federal government. While the recommendations did not address NCS's role in recovering from an Internet disruption, they included

- exploring the use of government networks as alternatives for critical emergency communications during times of national crisis;
- using and testing existing and leading-edge technologies and commercial capabilities to support critical emergency user requirements for security and availability;
- studying and supporting industry efforts in areas that present the greatest emergency communications risks during the period of convergence, including gateways, control systems, and first responder communications systems; and
- reviewing the value of satellite systems as a broad alternative transmission channel for critical emergency communications.

The final report, issued in March 2006, contained recommendations that the federal government

- require federal agencies to plan for and invest in resilient and alternate communications mechanisms to be used in a crisis,
- develop identity management tools to support priority emergency communication on next-generation networks,
- develop supporting policies for emergency communications on next-generation networks, and
- improve DHS incident management capabilities.

DHS has not yet developed specific plans to address the recommendations from either report.

National Coordinating Center Task Force

In October 2004, a task force was established to examine the future mission and role of the National Coordinating Center, which is part of NCS. This task force was to study the direction of the center over the next year, 3 years, and 5 years, including how industry members of the center should continue to partner with the government and how the center should be structured.

The task force researched the center's functions and mapped the center's authorities to its missions. It studied the center's organizational structure, information sharing and analysis, incident management and leadership, and international mutual-aid abilities.

In its report issued in May 2006, the task force found that since the September 11 attacks the number of companies participating in the National Coordinating Center has more than doubled, but the influx of new members has hindered information sharing because of the time it takes to develop trusted relationships between members. The report also found that members wanted government to increase its sharing of threat information with the communications industry through the National Coordinating Center. The report recommended that

- the National Coordinating Center broaden center membership by including additional firms, such as cable operators, satellite operators, and Internet service providers;

- NCS examine the possible combination of the National Coordinating Center and the Information Technology Information Sharing and Analysis Center;
- DHS clarify responsibilities and authorities in emergency situations to facilitate response to telecommunications disruptions;
- DHS revise the Cyber Incident Annex to the *National Response Plan* to clarify the trigger for the annex and the appropriate role of the government in responding to such an incident;
- the National Coordinating Center develop a concept of operations for responding to cyber events; and
- DHS resolve confusion over legal or jurisdictional issues in responding to cyber or communications crises.

DHS has not yet developed a plan to address these findings and recommendations.

DHS Has Conducted Disaster Response Exercises That Include Cyber Incidents

DHS Has Conducted Regional Exercises Involving Cyber Attacks

Over the last few years, DHS has conducted several exercises to test the federal and regional response to incidents affecting critical infrastructures. Among other events, these exercises included incidents that could cause localized Internet disruptions. Specifically, DHS sponsored two cyber tabletop exercises with Connecticut and New Jersey, as well as a series of exercises in the Pacific Northwest and Gulf Coast regions of the United States.

The series of exercises in the Pacific Northwest was named Blue Cascades. Blue Cascades II, conducted in September 2004, addressed a scenario involving cyber attacks and attacks that disrupted infrastructure, including telecommunications and electric power. The scenario explored regional capabilities to deal with threats, interdependences, cascading impacts, and incident response. Blue Cascades III, conducted in March 2006, focused on the impact of a major earthquake in the area and the resulting efforts to recover and restore services. Both exercises were sponsored by NCSD and organized by the Pacific Northwest Economic Region.

Purple Crescent II, held in New Orleans, Louisiana, in October 2004, was also designed to raise awareness of infrastructure interdependencies and to identify how to improve regional preparedness. The scenario involved a cell of terrorists that used an approaching major hurricane to test their ability to disrupt regional infrastructures, government and private organizations, and particularly disaster preparedness operations using cyber attacks. The exercise was sponsored by the Gulf Coast Regional Partnership for Infrastructure Security and funded by NCSD.

The objectives of these exercises included

- raising awareness of infrastructure-related cybersecurity issues and vulnerabilities;
- identifying response and recovery challenges;
- bringing together physical security, emergency management, and other disciplines involved in homeland security and disaster response;
- identifying roles and responsibilities in addressing cyber attacks and disruptions;

- determining ways to foster public/private cooperation and information sharing;
- identifying preparedness gaps associated with cybersecurity and related interdependencies; and
- producing an action plan of activities.

The exercises resulted in many findings regarding the overall preparedness for cyber incidents (see table 7). Overall, the exercises found that both the government and private-sector organizations were poorly prepared to effectively respond to cyber events. The lack of clarity on roles and responsibilities coupled with both the lack of coordination and communication and limited understanding of cybersecurity concerns pose serious obstacles to effective response and recovery from cyber attacks and disruptions. Furthermore, it was unclear who was in charge of incident management at the local, state, or national levels.

Table 7: Selected Lessons Learned from DHS Regional Exercises with Cyber Components

Area	Selected lessons learned
Skills, knowledge, and preparedness	• Many exercise participants demonstrated a basic understanding of high-level cybersecurity issues, but they were not knowledgeable about more complex cyber vulnerabilities and interdependencies that could cause cascading impacts. • Organizations overestimated their technical capabilities to protect against threats and attacks and to respond and recover expeditiously in the exercise scenario. • It appeared that few organizations had any formal alternative communications plans. • The dependence of emergency preparedness activities on information systems and electronic communications needs to be tested and assessed. Furthermore, vulnerabilities need to be identified and cost-effective mitigation measures need to be adopted. • It was unclear what redundant and alternative communications were available to organizations in a major cyber disruption, or if available, whether these capabilities were regularly tested.

(Continued From Previous Page)

Area	Selected lessons learned
Coordination	• While a cooperative spirit was demonstrated by participating organizations during the exercise, this cooperation appeared to be based on ad hoc personal relationships, and it is focused on physical incidents. • Participants for the most part focused on their own organizational interests, with minimal public/private coordination or formalized relationships. • With the exception of sector-specific Information Sharing and Analysis Centers and cybersecurity professional associations, organizations rarely coordinate on cyber threat and incident response activities, chiefly for legal and liability reasons. • Government agencies at the state level interact with other state entities, and federal agencies with federal offices, with little coordination at federal and state levels. There appears to be little coordination among the many federal, other government and private organizations with cybersecurity missions. • Private-sector participants emphasized that their organizations do not inform government authorities about what is seen as routine events because of company policy, legal constraints or liability concerns.
Triggers and thresholds for reporting	• Regional organizations lack information on what organization they should contact to report a cyber event or to seek guidance in dealing with an incident. • State and local emergency operations centers lack threshold criteria to determine when they should activate for a cyber attack. • It is unclear when a cybersecurity incident becomes a source of concern and what types of incidents should be communicated to local and federal law enforcement.
Government actions	• No one organization is mandated as the focal point for cybersecurity threats and incident response. The federal government has a number of organizations that have missions to respond to cyber incidents and there are also state and private-sector response organizations and vendors. As a result, it was not clear to the participants what role DHS elements and other federal agencies would play in a cyber incident. • Some participants believed DHS and US-CERT should undertake the lead role in dealing with major cyber attacks while other participants—chiefly private-sector representatives—did not see a federal government lead role as appropriate or desirable. • Participants described cyber incident management as “confused” or “loose.”

Source: GAO analysis of the Purple Crescent II exercise held in October 2004 and the Blue Cascades II exercise held in September 2004.

The after-action reports from the exercises recommended areas for additional study and planning, including

- additional study of the vulnerabilities of critical infrastructures to cyber attack;
- improved information on training, assessments, and resources to be used against cyber attacks;
- improved federal, state, local, and private-sector planning and coordination; and
- defined thresholds for what constitutes a major cyber attack.

Cyber Storm Was DHS's First National Exercise Focused on Cyber Attacks

Cyber Storm, held in February 2006 in Washington, D.C., was the first DHS-sponsored national exercise to test response to a cyber-related incident of national significance. The exercise involved a simulated, large-scale attack affecting the energy, information technology, telecommunications, and transportation infrastructures. DHS officials stated that they plan to hold a similar exercise every other year.

According to information provided by agency officials, the exercise involved eight federal departments and three agencies, three states, and four foreign countries. The exercise also involved representatives from the private sector, including nine information technology companies, six electric companies, and two airlines. The exercise objectives included testing interagency, intergovernmental, and public/private coordination of incident response.

Representatives of private-sector companies provided mixed responses on the value of exercises such as Cyber Storm. Selected representatives expressed concerns about the overly broad scope and the difficulty in justifying dedicating resources for the exercises due to the lack of clear goals and outcomes. Another representative stated that government exercises help the government but exercises involving private-sector coordination with multiple agencies would also be helpful. Another representative stated that exercises were only of value if there was a process for integrating lessons learned from the exercises into policies and procedures. Two representatives, from a private-sector company that participated in Cyber Storm, stated that, while useful, the exercise was not designed for network operators, who would benefit from more comprehensive training in incident response.

Comments from the Department of Homeland Security

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

Homeland Security

June 2, 2006

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

Dear Mr. Powner:

RE: Draft Report GAO-06-672, Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan (GAO Job Code 310499)

The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the draft report. We recognize that the Internet is an important component of the information infrastructure in which both the information technology (IT) and telecommunications sectors share an interest. Moreover, because of the increasing reliance of various Critical Infrastructure and Key Resources (CI/KR) sectors on interconnected networked information systems, the Internet represents a significant source of interdependencies for many sectors. In this regard, we agree with the Government Accountability Office (GAO) that recent incidents have shown the Internet as a whole is resilient. We also agree that strengthening collaboration between the public and private sector with constant attention to risk mitigation, response and recovery planning is critical to protect the Internet.[1] Finally, as noted in each response, DHS has already focused on issues raised in the recommendations and has either addressed a recommendation or is in the process of implementing a recommendation. Nevertheless, we welcome GAO's review and appreciate the opportunity to comment on each of the nine recommended actions that are intended to improve DHS' ability to facilitate public and private efforts to recover the Internet in case of a major disruption.

Recommendation 1: Establish dates for revising the National Response Plan and finalizing the National Infrastructure Protection Plan — including efforts to update key components relevant to the Internet.

[1] The Internet is generally understood as a vast network of interconnected global information systems that are logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons. This network supports communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols.

www.dhs.gov

Response: We agree with the recommendation. Implementation of the National Infrastructure Protection Plan (NIPP) is one of the three priorities called for as part of the National Preparedness Goal. The final draft of the NIPP Base Plan was provided to the Homeland Security Council Critical Infrastructure Protection Policy Coordinating Committee, which recently gave its concurrence. We anticipate the final interagency approval and signatures from the HSPD-7 departments and agencies will be forthcoming.

The pending release of the final NIPP Base Plan is an important milestone, but it is the *implementation* of that plan and the accompanying seventeen Sector-Specific Plans (SSPs) that will help build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR. Combined with the updated cyber component of the NIPP Base Plan, the development of these SSPs represents progress in efforts to update the key NIPP components relevant to the Internet. Specifically, the SSPs for the IT and telecommunications sectors will address plans for protecting the Internet, and will include consideration of the interdependencies between the two sectors. These plans are already undergoing development in collaboration with public and private sector security partners. Significant progress has been made on both, and completion of all SSPs is scheduled for 180 days after the release of the NIPP Base Plan.

With regard to the National Response Plan (NRP) revision, the Homeland Security Council (HSC) directed DHS to complete an interagency review of the NRP to incorporate critical revisions prior to the onset of the 2006 Hurricane Season. On May 25, 2006, DHS incorporated the revisions into the NRP in a Notice of Change. The revisions are based on organizational changes within DHS, as well as the lessons learned from the experience of responding to Hurricanes Katrina, Wilma, and Rita in 2005. As one part of the NRP Notice of Change, DHS created a NRP Quick Reference Guide as an appendix to the NRP, which provides senior officials with a concise summary of key concepts, relationships and roles and responsibilities outlined in the NRP. In addition, DHS intends to initiate a comprehensive stakeholder review of the NRP in the fall of 2006.

Recommendation 2: Using the planned revisions to the National Response Plan and National Infrastructure Protection Plan as a basis, draft public/private plans for Internet recovery and obtain input from key Internet infrastructure companies.

Response: We agree with the recommendation. DHS' National Cyber Security Division (NCSD) and the National Communications System (NCS), both located within the Directorate of Preparedness, are actively engaged with the private sector in furthering a mutual understanding of government's and industry's respective roles and responsibilities in connection with a disruption of the Internet or its supporting infrastructure. In August 2005, the President's National Security Telecommunications Advisory Committee (NSTAC) hosted an event entitled, "Incident Management in Next Generation Network," between key industry and government leaders regarding next steps for collaboratively responding to incidents affecting the shared public Internet infrastructure. These types of events build relationships and are key because the Internet infrastructure is, for the most part, owned and operated by the private sector.

NCSD has several initiatives underway specifically focused on building relationships with private industry to determine risks and needs in the event of an Internet disruption. For example, the United States Computer Emergency Readiness Team (US-CERT), through its leadership of the North American Incident Response Group (NAIRG), continues to develop operational relationships and processes to enhance US-CERT's ability to respond to an Internet disruption of national significance. Additionally, the National Cyber Response Coordinating Group (NCRCG) has developed thresholds for activating the Group and a concept of operations for responding to cyber incidents, which would include Internet disruptions. Although the NCRCG role is not operational, it plays a key role in facilitating effective Federal response to incidents.

Finally, ongoing collaboration with subject matter experts from the private sector and academia through the Internet Disruption Working Group (IDWG) further supports and validates government/industry efforts to identify key Internet infrastructure contacts, thresholds, and processes to facilitate situational awareness, incident management, and recovery actions. This collaboration, along with simulations such as the recent Cyber Storm exercise and the upcoming IDWG tabletop exercise, provide data points to clarify industry and government roles and responsibilities during an Internet disruption, and will lead to the enhancement of mitigation measures to be included in the public/private plans.

Recommendation 3: Review the NCS and NCSD organizational structure and roles in light of the convergence of voice and data communications.

Response: We agree with the recommendation and believe it can be closed. DHS has addressed the organizational structure by placing NCS and NCSD in a newly created Office of Cyber Security and Telecommunications within the Directorate of Preparedness. This reorganization clearly acknowledges the increasing convergence between the telecommunications and IT sectors. NCSD and NCS work closely together to coordinate efforts to protect the Nation's critical cyber systems and telecommunications transport layer. In addition, NCSD's operational division, US-CERT and the NCS's National Coordinating Center for Telecommunications work together to analyze potential threats, mitigate risks and collaborate as appropriate with respect to response and recovery initiatives. NCS and NCSD together chair the IDWG and play a lead role in the NCRCG as discussed below.

Recommendation 4: Identify the relationships and interdependencies between the various Internet-recovery related activities currently under way in NCS and NCSD, including initiatives by US-CERT, the National Cyber Response Coordination Group, the Internet Disruption Working Group, the North American Incident Response Group, and the groups responsible for developing and implementing cyber recovery exercises.

Response: We agree with the recommendation. NCS and NCSD have identified and capitalized on relationships and interdependencies between Internet-recovery related activities within DHS. There has been significant and strategic collaboration between IDWG, NCRCG, and US-CERT through major initiatives such as the IDWG Forum, Exercise Cyber Storm, NCRCG meetings and working groups, as well as the upcoming

IDWG Tabletop exercise. Further, in the event of an Internet disruption of national significance, the Secretary of DHS may activate the Interagency Advisory Committee (IAC),[2] which would work in coordination with the NCRCG.

US-CERT is the operational entity having real-time responsibility for responding to a Federal cyber incident and, when applicable, an incident that has an actual or perceived potential to require the activation of the NCRCG. DHS//NCSD co-chairs the NCRCG with the Department of Justice and the Department of Defense. The NCRCG and US-CERT collaborate with respect to information sharing, and work in coordination with the IAC. During an incident of national significance that involves cyber, the NCRCG would provide a cyber incident management role to the IAC.

The IDWG is not an operational entity and has no incident response or recovery responsibilities. The IDWG engages with the private sector, academia, and international security experts to examine risks and develop recommendations to improve preparedness. Findings and recommendations developed by the IDWG are provided to the US-CERT, NCRCG, and other like entities having direct response and recovery roles within their respective organizations.

With respect to the North American Incident Response Group (NAIRG), it is the intent of US-CERT to foster operational relationships with incident response organizations such as NAIRG within the private sector. In this regard, the NAIRG is not a government organization and is without any extant actions/taskings.

In regard to groups responsible for cyber exercises, the NCSD Exercise Program is the focal point for cyber exercise management and execution within DHS. It supports those activities (US-CERT, NCRCG, IDWG, etc.) that have identified requirements for further discovery to better understand roles, responsibilities and processes, and identification of gaps. In addition, the NCSD Exercise Program is the exercise sponsor for the National Cyber Exercise: Cyber Storm, a biennial cyber exercise focused on strategic and operational issues such as interagency preparedness, response and recovery under the Cyber Annex to the NRP; cross-sector interdependencies on the underlying information systems including control systems; and, public-private collaboration and coordination. It should be noted that the US-CERT, NCRCG and other industry experts were significant players during the February, 2006 Cyber Storm Exercise.

Recommendation 5: Establish timelines and priorities for key efforts identified by the Internet Disruption Working Group.

---

[2] Pursuant to recommendations made in numerous after action reports examining the Federal government's response to Hurricanes Katrina, Rita, and Wilma, the Department has recently put forward a proposal for a number of changes to the National Response Plan. One of these changes would replace the existing Interagency Incident Management Group (IIMG) with an Interagency Advisory Committee, "a task organized advisory body comprised of senior representatives from DHS components and headquarters staff offices, other Federal departments and agencies, and NGOs . . . [which] provide[s] the Secretary with strategic recommendations that facilitate immediate and effective action(s) to prevent, prepare for, respond to, and/or recover from an incident."

Response: We agree with the recommendation. The IDWG has identified milestones and priorities for key efforts along with their respective timelines as part of the NCSD strategic plan. The initial activity of the IDWG was a one day forum of facilitated discussion among Internet and policy experts addressing perceived and real vulnerabilities and threats to key Internet resources. A draft report outlining key efforts is in the process of being finalized. In collaboration with US-CERT, NCRCG, and the private sector, the IDWG continues to refine a project plan that addresses timelines and priorities.

Recommendation 6: Identify ways to incorporate lessons learned from actual incidents and during cyber exercises into recovery plans and procedures.

Response: We agree with the recommended action. As the cyber exercise focal point for DHS, NCSD has the responsibility to provide the venue and environment for participants to take part in exercises and garner lessons learned both during the planning process and actual exercise execution. In this role as facilitator of Cyber Storm, the NCSD Exercise Program has conducted 5 after action conferences to date (Federal, NCRCG, Private Sector, States and International) as part of the process to draft an exercise After Action Report (AAR) for all stakeholders/participants. The Cyber Storm AAR will cover macro lessons learned based on the exercise objectives. In addition to this process, many participants will conduct their own internal AAR efforts in order to develop specific organizational lessons learned and internal action recommendations. NCSD has also begun its own process to develop an action plan based on the AAR and is collaborating with other Departments and Agencies as well as the private sector on implementing changes to policy and procedures. Further, US-CERT has already developed specific internal action recommendations and has begun to implement them based on the lessons learned from Cyber Storm.

Recommendation 7: Working with the private-sector stakeholders representing the Internet infrastructure, address challenges to effective Internet recovery by further defining needed government functions during a major Internet disruption (this effort should include a careful consideration of the potential government functions identified by the private sector in table 6 of this report).

Response: We agree with the recommendation. DHS recognizes NCS and NCSD face challenges in planning comprehensive strategies for responding to and reconstituting after a cyber incident of national significance. It is axiomatic, that only a truly functioning private/public partnership will result in the plans and strategies necessary as the majority of the Internet infrastructure is owned and operated by the private sector. DHS will continue to make progress by exercising and testing response actions and capabilities, building relationships, and bringing attention to the severity of the threat against the infrastructure.

DHS has formed a strategic partnership through the IDWG to combine resources, avoid duplication of effort, and leverage Federal government, academia, and private sector work on the issue of Internet disruptions. The IDWG works with major stakeholders to

identify and prioritize short-term protective measures necessary to prevent major disruptions of the Internet, especially as it relates to identifying necessary government functions during such an incident, and to identify responsive/reconstitution measures in the event of a major disruption. This group has reviewed previous Internet disruption reports to identify and leverage high priority actions to improve the resiliency of the Internet quickly and effectively.

In addition, US-CERT has been attending the North American Network Operator's Group (NANOG) meetings for the last three years to continue to establish closer ties to tier one through tier three Internet providers to work issues of national significance. US-CERT also participates in a number of technical venues to further coordination efforts and works with subject matter experts on topics ranging from Domain Name Systems (DNS) issues to core Internet Protocol topics. The US-CERT also works within the Forum of Incident Response Teams community (www.first.org) and a number of other international incident response teams for situational awareness and collaboration.

Recommendation 8: Define a trigger for government involvement in responding to such a disruption.

Response: We generally agree with the recommendation. However, the dynamics of the Internet, and business processes and policies of its owners and operators pose a significant challenge to defining a standard set of thresholds. As noted above, DHS continues to address this challenge and is collaborating with the private sector to better understand existing operational and corporate governance policies. The IDWG has begun an information sharing study to review the information sharing environment. This study should provide insights regarding a consensus on the effectiveness of establishing standard thresholds and/or processes for sharing information between private sector Internet owners/operators and DHS.

Recommendation 9: Document assumptions and develop approaches to deal with key challenges that are not within the government's control.

Response: We concur with the recommendation. Many of the challenges confronting enhancement of existing processes are, for the most part, identified in the report. These challenges include: lack of authority, dynamics of the Internet infrastructure, technology enhancement (to include technology convergence), defining thresholds, understanding of government's role, and private sector business processes/governance policies. DHS is addressing challenges with the Internet owners and operators through forums, tabletop exercises, and smaller action teams consisting of subject matter experts who will address those actions identified within the IDWG forum.

Related Issues:

An ongoing DHS focus is cyber threat analysis. This effort encompasses many different organizations and elements, including threat information collection requirements, scenario development, and cyber threat products for all sectors. Dialogue between public

and private IT sector partners, DHS' Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and the intelligence community will help to promote and invigorate cyber threat analysis by leveraging the capabilities, insights, and experience that each organization represents.

Thank you again for the opportunity to review this report and provide additional comments.

Sincerely,

Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

MMcP

GAO Contacts and Staff Acknowledgments

GAO Contacts

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

Staff Acknowledgments

In addition to those named above, Don R. Adams, Naba Barkakati, Scott Borre, Neil Doherty, Vijay D'Souza, Joshua A. Hammerstein, Bert Japikse, Joanne Landesman, Frank Maguire, Teresa M. Neven, and Colleen M. Phillips 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