United States Government Accountability Office

GAO

Testimony before the Subcommittee on Federal Financial Management, Government Information, and International Security, Senate Committee on Homeland Security and Governmental Affairs

For Release on Delivery
Expected at 9:30 a.m. EDT
Friday, July 28, 2006

INTERNET INFRASTRUCTURE

Challenges in Developing a Public/Private Recovery Plan

Statement of David A. Powner
Director, Information Technology Management Issues

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

July 2006

INTERNET INFRASTRUCTURE

Challenges in Developing a Public/Private Recovery Plan

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-863T, a testimony before the Subcommittee on Federal Financial Management, Government Information, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate

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 originated as a U.S. government-sponsored research project, 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 summarize its report being released today—*Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, GAO-06-672 (Washington, D.C.: June 16, 2006). This report (1) identifies examples of major disruptions to the Internet, (2) identifies the primary laws and regulations governing recovery of the Internet in the event of a major disruption, (3) evaluates DHS plans for facilitating recovery from Internet disruptions, and (4) assesses challenges to such efforts.

What GAO Recommends

In its report, GAO suggests that Congress consider clarifying the legal framework guiding Internet recovery and makes recommendations to DHS to strengthen its ability to help recover from Internet disruptions. In written comments, DHS agreed with GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-06-863T.

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 physical incident (such as a natural disaster or an attack that affects key facilities), a cyber incident (such as a software malfunction or a malicious virus), or a combination of both physical and cyber incidents. Recent physical and cyber incidents, such as Hurricane Katrina, have caused localized or regional disruptions but have not caused a catastrophic Internet failure.

Federal laws and regulations that address 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 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 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 the Internet to recover from a major disruption.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to join today's hearing on reconstitution of critical networks such as the Internet. 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 recovery efforts for public and private critical infrastructure systems.[1] Additionally, federal policy recognizes the need to be prepared for the possibility of debilitating Internet disruptions and tasks DHS with developing an integrated public/private plan for Internet recovery.[2] Last July, we testified before you on DHS's responsibilities for cybersecurity-related critical infrastructure protection.[3] In that testimony, we discussed the status of DHS's efforts and challenges faced by DHS in fulfilling its responsibilities. We reported that DHS had much work ahead of it. In a related report, we recommended that DHS prioritize cybersecurity-related responsibilities—including establishing recovery plans for key Internet functions.[4]

As requested, our testimony summarizes a report we released that (1) identifies examples of major disruptions to the Internet, (2) identifies the primary laws and regulations governing recovery of the Internet in the

[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: Challenges in Addressing Cybersecurity*, GAO-05-827T (Washington, D.C.: July 19, 2005).

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

event of a major disruption, (3) evaluates DHS's plans for facilitating recovery from Internet disruptions, and (4) assesses challenges to such efforts.[5] The report includes matters for congressional consideration and recommendations to DHS for improving Internet recovery efforts. In preparing for this testimony, we relied on our work supporting the accompanying report. That report contains a detailed overview of our scope and methodology. All the work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Results in Brief

A major disruption to the Internet could be caused by a physical incident (such as a natural disaster or an attack that affects facilities and other assets), by a cyber incident (such as a software malfunction or a malicious virus), or by a combination of both physical and cyber incidents. Recent physical and cyber 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 have also shown the Internet as a whole to be flexible and resilient. Even in severe circumstances, the Internet did not suffer a catastrophic failure. Nevertheless, 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.

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. The Defense Production Act and the Stafford Act provide authority to federal agencies to plan for and respond to incidents of national significance like disasters and terrorist attacks. However, the Defense Production Act has never been used for Internet recovery. In addition, the Stafford Act does not authorize

[5]GAO, *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, GAO-06-672 (Washington, D.C.: June 16, 2006).

the provision of resources to for-profit companies such as those that own and operate core Internet components. The Communications Act of 1934 and National Communication System authorities govern the telecommunications infrastructure and help ensure communications during national emergencies, but they have never been used for Internet recovery either. Thus, it is not clear how effective these laws and regulations would be in assisting Internet recovery.

DHS has begun a variety of initiatives to fulfill its responsibility to develop an integrated public/private plan for Internet recovery, but these efforts are not yet comprehensive or complete. 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 timeframes for completion. Also, the relationships between these initiatives are not evident. As a result, the 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 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 suggested in our accompanying report, that Congress consider clarifying the legal framework guiding

Internet recovery.[6] We also made recommendations to the Secretary of Homeland Security to strengthen the department's ability to serve effectively 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. In written comments, DHS agreed with our recommendations and provided information on initial activities it was taking to implement them.

Background

The Internet is a vast network of interconnected networks that is used by governments, businesses, research institutions, and individuals around the world to communicate, engage in commerce, do research, educate, and entertain. 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. 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. Today, private industry—including telecommunications companies, cable companies, and Internet service providers—owns and operates the vast majority of the Internet's infrastructure. 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, including criminal groups, hackers, and terrorists.

Federal regulation recognizes the need to protect critical infrastructures such as the Internet. It directs federal departments and agencies to identify and prioritize critical infrastructure sectors and key resources and to protect them from terrorist attack. Furthermore, it recognizes 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. 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. In its plan for protecting critical infrastructures, DHS recognizes that the Internet is a

[6]GAO-06-672.

key resource composed of assets within both the information technology and the telecommunications sectors.[7] It notes that the Internet is used by all critical infrastructure sectors to varying degrees and provides information and communications to meet the needs of businesses and government.

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. In addition, government initiatives could facilitate response to major Internet disruptions.

Federal policies and plans[8] 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, provides programs and services that assure the resilience of the telecommunications infrastructure in times of crisis. Additionally, 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 relief groups; federal, state, and local government agencies; businesses; and victims in the disaster areas.

Prior evaluations of DHS's cybersecurity responsibilities have highlighted issues and challenges facing the department. In May 2005, we issued a

[7]DHS, *The National Infrastructure Protection Plan*.

[8]These include the *National Strategy to Secure Cyberspace*, the interim *National Infrastructure Protection Plan*, the Cyber Incident Annex to the *National Response Plan*, and Homeland Security Presidential Directive 7.

report on DHS's efforts to fulfill its cybersecurity responsibilities.[9] 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 noted in federal law and policy. We also reported 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. In this report, we also made recommendations to improve DHS's ability to fulfill its mission as an effective focal point for cybersecurity, including recovery plans for key Internet functions. DHS agreed that strengthening cybersecurity is central to protecting the nation's critical infrastructures and that much remained to be done, but it has not yet addressed our recommendations.

Although 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. Recent physical and cyber 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.

To date, cyber attacks have caused various degrees of damage. For example, 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. In 2003, the Slammer worm caused network outages, canceled airline flights, and automated teller machine failures. Slammer resulted in temporary loss of Internet access to some users, and cost estimates on the impact of the worm range from $1.05 billion to $1.25 billion. 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, because the

[9] GAO-05-434.

worm had propagated so quickly, most of these activities occurred after it had stopped spreading.

In 2002, a coordinated denial-of-service attack was launched against all of the root servers in the Domain Name System. At least nine of the thirteen root servers experienced degradation of service. However, average end users hardly noticed the attack. The attack became visible only as a result of various Internet health-monitoring projects. The response to the attacks was handled by the server operators and their service providers. The attack pointed to a need for increased capacity for servers at Internet exchange points to enable them to manage the high volumes of data traffic during an attack. If a massive disruptive attack on the domain name server system were successful, it could take several days to recover from. According to experts familiar with the attack, the government did not have a role in recovering from it.

Like cyber incidents, 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. For example, 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 serving 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. Efforts to recover Internet service were handled by the affected Internet service providers; however, local and federal officials responded to the immediate physical issues of extinguishing the fire and maintaining safety in the surrounding area, and they worked with telecommunications companies to reroute affected cables.

In addition, Hurricane Katrina caused substantial destruction of the communications infrastructure in Louisiana, Mississippi, and Alabama, but it had minimal affect on the overall functioning of the Internet outside of the immediate area. 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. 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. However, a substantial number of the networks that experienced service disruptions recovered relatively quickly.

Federal officials stated that the government took steps to respond to the hurricane, such as increasing analysis and watch services in the affected area, coordinating with communications companies to move personnel to safety, working with fuel and equipment providers, and rerouting communications traffic away from affected areas. However, private-sector representatives stated that requests for assistance, such as food, water, fuel, and secure access to facilities were denied for legal reasons; the government made time-consuming and duplicative requests for information; and certain government actions impeded recovery efforts.

Since its inception, the Internet has experienced disruptions of varying scale—including fast-spreading worms, denial-of-service attacks, and physical destruction of key infrastructure components—but the Internet has yet to experience a catastrophic failure. 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.

Specifically, the Homeland Security Act of 2002[10] and Homeland Security Presidential Directive 7[11] 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 physical and cyber-based systems that are essential to the operations of 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.

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

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

Regarding federal disaster response, the Defense Production Act[12] and the Stafford Act[13] 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. It is applicable to critical infrastructure protection and restoration but 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.

Other legislation and regulations, including the Communications Act of 1934[14] and the NCS authorities,[15] govern the telecommunications infrastructure and help to ensure communications during national emergencies. For example, the 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.[16] 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. Although these authorities remain in force 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.

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

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

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

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

[16]Executive Order 12472 § 2; Communications Act of 1934, § 706, 47 U.S.C § 606.

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 in Internet reconstitution following a disruption are not fully defined.

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

DHS has begun a variety of initiatives to fulfill its responsibility to develop 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 relationship between these initiatives is not evident. As a result, the nation is not prepared to effectively coordinate public/private plans for recovering from a major Internet disruption.

High-Level Response and Protection Plans

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. It contains two components that address issues related to telecommunications and the Internet, Emergency Support Function 2 and the Cyber Incident Annex. These components, however, are not complete; Emergency Support Function 2 does not directly address Internet recovery, and the annex does not reflect the National Cyber Response Coordination Group's current operating procedures. The other key document, the *National Infrastructure Protection Plan*, consists of both a base plan and sector-specific plans. The base plan, which was recently released, describes the importance of cybersecurity and networks such as the Internet to critical infrastructure protection and includes an appendix that provides information on cybersecurity responsibilities. The appendix restates DHS's responsibility to develop plans to recover Internet functions. However, the base plan is at a high level and the sector-specific plans that would address the Internet in more detail are not scheduled for release until December 2006.

Several representatives of private-sector firms supporting the Internet infrastructure expressed concerns about both plans, noting that they would be difficult to execute in times of crisis. Other representatives were uneasy about the government developing recovery plans, because they were not confident of 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.

Both the *National Response Plan and National Infrastructure Protection Plan* are 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. While these activities are promising, some initiatives are incomplete, others lack time lines and priorities, and still others lack an effective mechanism for incorporating lessons learned.

National Communications System Reorganization

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. A presidential advisory committee on telecommunications[17] established two task forces that recommended changes to NCS's role, mission, and functions to reflect this convergence, but DHS has not yet developed plans to address these recommendations.

National Cyber Response Coordination Group

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. DHS officials acknowledge 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 triggers 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.

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

Internet Disruption Working Group

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. According to DHS officials who organized the group, it 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; however, agency officials have not yet finalized plans, resources, or milestones for these efforts.

North American Incident Response Group

US-CERT officials formed the North American Incident Response Group, which includes both public and private-sector network operators that 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, programs, and incident response and to seek ways for the government and industry to work together operationally. 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.

Exercises

Over the last few years, DHS has conducted several broad inter-governmental exercises to test regional responses to significant incidents that could affect the critical infrastructure. 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. 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, milestones, or which group should be responsible for incorporating lessons learned from the regional and Cyber Storm exercises into its plans and initiatives.

While DHS has various initiatives under way, the relationships and interdependencies between these various efforts are not evident. For example, 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 between the groups have not been clearly established. Without a thorough understanding of the interrelationships between its various initiatives, DHS risks pursuing redundant efforts and missing opportunities to build on related efforts.

After our report was issued, a private-sector organization released a report that examined the nation's preparedness for a major Internet disruption.[18] The report stated that our nation is unprepared to reconstitute the Internet after a massive disruption. The report supported our findings that significant gaps exist in government response plans and that the responsibilities of the multiple organizations that would play a role in recovery are unclear. The report also made recommendations to complete and revise response plans such as the Cyber Incident Annex of the *National Response Plan*; better define recovery roles and responsibilities; and establish more effective oversight and strategic direction for Internet reconstitution.

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) 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 focal point for recovering the Internet from a major disruption.

First, the Internet's diffuse structure, vulnerabilities in its basic protocols, and the lack of agreed-upon performance measures make planning for and responding to a disruption more difficult. The components of the Internet are not all governed by the same organization. In addition, the Internet is international. According to private-sector estimates, only about 20 percent of Internet users are in the United States. Also, there are no well-accepted standards for measuring and monitoring the Internet infrastructure's

[18]Business Roundtable, *Essential Steps to Strengthen America's Cyber Terrorism Preparedness* (Washington D.C.: June 2006).

availability and performance. Instead, individuals and organizations rate the Internet's performance according to their own priorities.

Second, there is no consensus about the role DHS should play in responding to a major Internet disruption or about the appropriate trigger for its involvement. The lack of clear legislative authority for Internet recovery efforts complicates the definition of this role. DHS officials acknowledged that their role in recovering from an Internet disruption needs further clarification because private industry owns and operates the vast majority of the Internet.

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 us and the White House to need revision.[19] Since private-sector participation in DHS planning activities for Internet disruption is voluntary, agreement on the appropriate trigger for government involvement and the role of government in resolving an Internet disruption is essential to any plan's success.

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. There was no consensus on this issue. Many private-sector officials stated that the government did not have a direct recovery role, while others identified a variety of potential roles, including

- providing information on specific threats;
- providing security and disaster relief support during a crisis;
- funding backup communication infrastructures;
- driving improved Internet security through requirements for the government's own procurement;
- serving as a focal point with state and local governments to establish standard credentials to allow Internet and telecommunications companies

[19]See 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).

access to areas that have been restricted or closed in a crisis;

- providing logistical assistance, such as fuel, power, and security, to Internet infrastructure operators;
- focusing on smaller-scale exercises targeted at specific Internet disruption issues;
- limiting the initial focus for Internet recovery planning to key national security and emergency preparedness functions, such as public health and safety; and
- establishing a system for prioritizing the recovery of Internet service, similar to the existing Telecommunications Service Priority Program.

A third challenge to planning for recovery is that there are key legal issues affecting DHS's ability to provide assistance to help restore Internet service. As noted earlier, 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 which organization would be responsible in the case of a major Internet disruption. In addition, the Stafford Act, which authorizes the government to provide federal assistance to states, local governments, nonprofit entities, and individuals in the event of a major disaster or emergency, 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.

A fourth challenge is that a large percentage of the nation's critical infrastructure—including the Internet—is owned and operated by the private sector, meaning that 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. Many private-sector representatives questioned the value of providing information to DHS regarding planning for and recovery from Internet

disruption. In addition, DHS has identified provisions of the Federal Advisory Committee Act[20] as having a "chilling effect" on cooperation with the private sector. 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.

Finally, DHS has lacked permanent leadership while developing its preliminary plans for Internet recovery and reconstitution. In addition, the organizations with roles in Internet recovery (NCS and NCSD) have overlapping responsibilities and may be reorganized once DHS selects permanent leadership. As a result, it is difficult for DHS to develop a clear set of organizational priorities and to coordinate between the various activities necessary for Internet recovery planning. In May 2005, we reported that multiple senior DHS cybersecurity officials had recently left the department.[21] 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. Additionally, DHS officials acknowledge that the current organizational structure has overlapping responsibilities for planning for and recovering from a major Internet disruption.

In a July 2005 departmental reorganization, NCS and NCSD were placed in the Preparedness Directorate. NCS's and NCSD's responsibilities were to be placed under a new Assistant Secretary of Cyber Security and Telecommunications—in part to raise the visibility of cybersecurity issues in the department. However, almost a year later, this position remains vacant. 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.

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

[21]GAO-05-434.

Implementation of GAO Recommendations Should Improve DHS Internet Recovery Planning Efforts

Given the importance of the Internet infrastructure to our nation's communication and commerce, in our accompanying report we suggested matters for congressional consideration and made recommendations to DHS regarding improving efforts in planning for Internet recovery.[22] Specifically, we suggested that Congress 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 whether 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.

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

- Establish dates for revising the National Response Plan—including efforts to update key components that are relevant to the Internet.
- Use the planned revisions to the National Response Plan and the National Infrastructure Protection Plan as a basis to 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.

[22] GAO-06-672.

- 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 earlier in this testimony),
  - 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.

In written comments, DHS agreed with our recommendations and stated that it recognizes the importance of the Internet for information infrastructures. DHS also provided information about initial actions it is taking to implement our recommendations.

In summary, 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 do not specifically address roles and responsibilities for Internet recovery.

As the focal point for ensuring the security of cyberspace, DHS has initiated efforts to refine high-level disaster recovery plans; however, pertinent Internet components of these plans are not complete. While DHS has also undertaken several initiatives to improve Internet recovery planning, much remains to be done. Specifically, some initiatives lack clear timelines, lessons learned are not consistently being incorporated in recovery plans, and the relationships between the various initiatives are not clear.

DHS faces numerous challenges in 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.

To improve DHS's ability to facilitate public/private efforts to recover the Internet in case of a major disruption, our accompanying report suggested that Congress consider clarifying the legal framework guiding Internet recovery. We also made recommendations to DHS to establish clear milestones for completing key plans, coordinate various Internet recovery-related activities, and address key challenges to Internet recovery planning. Effectively implementing these recommendations could greatly enhance our nation's ability to recover from a major Internet disruption.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittee may have at this time.

If you have any questions on matters discussed in this testimony, please contact us at (202) 512-9286 and at (202) 512-6412 or by e-mail at pownerd@gao.gov and rhodesk@gao.gov. Other key contributors to this testimony include 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.

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