United States Government Accountability Office

GAO

Testimony

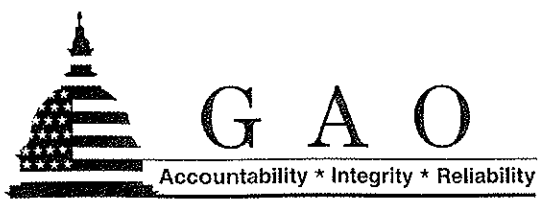
Before the Subcommittee on Information Policy, Census, and National Archives, House Committee on Oversight and Government Reform

For Release on Delivery
Expected at 2:00 p.m. EDT
Tuesday, October 23, 2007

INTERNET INFRASTRUCTURE

Challenges in Developing a Public/Private Recovery Plan

Statement of Gregory C. Wilshusen
Director, Information Security Issues



October 23, 2007

GAO
Accountability · Integrity · Reliability
Highlights

Highlights of GAO-08-212T, a testimony before the Subcommittee on Information Policy, Census, and National Archives, House Committee on Oversight and Government Reform

INTERNET INFRASTRUCTURE

Challenges in Developing a Public/Private Recovery Plan

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 on plans for recovering the Internet in case of a major disruption (GAO-06-672) and to provide an update on DHS's efforts to implement that report's recommendations. The 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 made recommendations to DHS to strengthen its ability to help recover from Internet disruptions. In written comments, DHS agreed with these recommendations.

To view the full product, including the scope and methodology, click on GAO-08-212T. For more information, contact Gregory C. Wilshusen, 202-512-6244, wilshuseng@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.

As of 2006, DHS had begun a variety of initiatives to fulfill its responsibility to develop an integrated public/private plan for Internet recovery, but these efforts were not yet comprehensive or complete. For example, the department had developed high-level plans for infrastructure protection and incident response, but the components of these plans that address the Internet infrastructure were not complete. As a result, the risk remained that the government was not 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 discuss public/private recovery plans for the Internet infrastructure. Since the early 1990s, the world community 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 computer systems of our government and our nation 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 cyber space—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] In June 2006, we issued a report[3] that (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's plans for facilitating recovery from Internet disruptions, and (4) assesses challenges to such efforts. The report includes matters for congressional consideration and recommendations to DHS for improving Internet recovery efforts.

As requested, this testimony summarizes our June 2006 report and provides an update of DHS's efforts to implement our recommendations. The report that this testimony was based on contains a detailed overview of our scope and methodology and was

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

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

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

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 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 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 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.

As of 2006, DHS had begun a variety of initiatives to fulfill its responsibility to develop an integrated public/private plan for Internet recovery, but these efforts were not yet comprehensive or complete. Specifically, the department had developed high-level plans for infrastructure protection and incident response, but the components of these plans that address the Internet infrastructure were not complete. In addition, DHS had 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 on these initiatives was limited, and other initiatives lacked timeframes for completion. Also, the relationships among these initiatives were not evident. As a result, the risk remained that the government was not 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 report that

Congress consider clarifying the legal framework guiding Internet recovery.[4] 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.

DHS agreed with our recommendations and has made progress in implementing them. Specifically, DHS has revised key plans in coordination with private industry infrastructure stakeholders, coordinated various Internet recovery-related activities, and worked to address key challenges in Internet recovery planning. However, further work remains to be done to complete these activities. For example, DHS has yet to complete recovery plans or to define the interdependencies among its various working groups and initiatives. Full implementation of these recommendations should enhance the nation's ability to recover from a major Internet disruption.

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, perform 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

[4]GAO-06-672.

increasing in frequency and complexity. Attacks against the Internet can come from a variety of sources, 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 key resource composed of assets within both the information technology and the telecommunications sectors.[5] 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 most 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 a response to major Internet disruptions.

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

Federal policies and plans[6] assign DHS with the lead responsibility for facilitating a public/private response to and recovery from major Internet disruptions. Within DHS, responsibilities reside in two divisions within the Office of the Under Secretary for National Protection and Program, Office of Cybersecurity and Communications: 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 cyber security responsibilities have highlighted issues and challenges facing the department. In May 2005, we issued a report on DHS's efforts to fulfill its cyber security responsibilities.[7] We noted that while DHS had initiated multiple efforts to fulfill its responsibilities, it had not fully addressed any of the 13 key cyber security 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 cyber security roles and capabilities, establishing effective partnerships with stakeholders, achieving two-way information sharing with stakeholders, and demonstrating the value that DHS can provide. In that report, we also made

[6]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.

[7]GAO-05-434.

recommendations to improve DHS's ability to fulfill its mission as an effective focal point for cyber security, including recovery plans for key Internet functions. DHS agreed that strengthening cyber security is central to protecting the nation's critical infrastructures and that much remained to be done.

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 these things. Disruptions to Internet service can be caused by cyber and physical incidents—both intentional and unintentional. Over the last few years, 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 worm had propagated so quickly, most of these activities occurred after it had stopped spreading.

In 2002 and again in 2007, coordinated denial-of-service attacks were launched against all of the root servers in the Domain Name System. In the 2002 attack, at least nine of the thirteen root servers experienced degradation of service, while in the 2007 attack, six of

the thirteen root servers experienced degradation of service. However, average end users hardly noticed the attacks. The attacks were efficiently handled by the server operators and their service providers. The 2002 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. The 2007 attack demonstrated that some of the improvements made since 2002 to improve the resilience of the Internet had worked.

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 another physical incident, Hurricane Katrina caused substantial destruction of the communications infrastructures 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 more than 3 million telephone customers, 38 emergency 9-1-1 call centers, hundreds of thousands of cable customers, and more than 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[8] and Homeland Security Presidential Directive 7[9] establish critical infrastructure protection as a national goal and describe a strategy for cooperative

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

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

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, they do not specifically address roles and responsibilities in the event of an Internet disruption.

Regarding federal disaster response, the Defense Production Act[10] and the Stafford Act[11] 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[12] and the NCS authorities,[13] 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

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

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

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

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

require any carrier subject to the Communications Act of 1934 to grant preference or priority to essential communications.[14] 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 seldom been 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 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 Relationships Among the Initiatives Are Not Evident

As of our June 2006 report, DHS had begun a variety of initiatives to fulfill its responsibility to develop an integrated public/private plan for Internet recovery, but these efforts were not complete or comprehensive. Specifically, DHS had developed high-level plans, including the *National Response Plan* and the *National Infrastructure Protection Plan*, for infrastructure protection and national disaster response, but the components of these plans that address the Internet infrastructure were not complete.

In addition, DHS had started a variety of initiatives to improve the nation's ability to recover from Internet disruptions, including establishing working groups to facilitate coordination, such as the *National Cyber Response Coordination Group* and *Internet Disruption Working Group*, and exercises in which government and

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

private industry practice responding to cyber events. While these activities were promising, the responsibilities and plans for selected working groups had not yet been defined, and key exercises lacked effective mechanisms for incorporating lessons learned. In addition, the relationships among the initiatives were not evident. For example, the National Cyber Response Coordination Group, the Internet Disruption Working Group, and the North American Incident Response Group were all meeting to discuss ways to address Internet recovery, but the interdependencies among the groups had not been clearly established. As a result, the nation was not prepared to effectively coordinate public/private plans for recovering from a major Internet disruption.

Multiple Challenges Exist to Planning for Recovery from Internet Disruptions

Although DHS has various initiatives to improve Internet recovery planning, there are 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 these challenges are addressed, DHS will have difficulty achieving results in its role as a 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 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.

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 does 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 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[15] 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 May 2005, we reported that multiple senior DHS cyber security officials had recently left the department.[16] 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. DHS officials acknowledge that the current organizational structure has overlapping responsibilities for planning for and recovering from a major Internet disruption.

DHS Has Taken Steps To Implement Recommendations, but More Work Remains To Be Done

Given the importance of the Internet infrastructure to our nation's communication and commerce, our June 2006 report suggested a matter for congressional consideration and made recommendations to DHS regarding improving efforts in planning for Internet recovery.[17] 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

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

[16]GAO-05-434.

[17]GAO-06-672.

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 nine actions (see table 1). The department agreed with our recommendations and has made progress in addressing many of them. Still, work remains to be done to ensure that our nation is prepared to effectively respond to a disruption of the Internet infrastructure.

Table 1: DHS's Progress in Addressing GAO Recommended Actions

Recommended Actions	Status	DHS Progress
Establish dates for revising the *National Response Plan*—including efforts to update key components that are relevant to the Internet.	In process	DHS revised its *National Response Plan* (the revised version is called the *National Response Framework*) and released it for public comment in September 2007. As part of this effort, the agency revised segments that are relevant to the Internet, including the Cyber Incident Annex. However, DHS did not provide a date for when it expects to complete the Framework.
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.	In process	As noted above, DHS's *National Response Framework* has been updated and released for public comment, but has not yet been completed. In addition, DHS released the National Infrastructure Protection Plan's base plan in June 2006 and the sector specific plans in May 2007. Because both documents have been made available for input from key infrastructure companies, DHS expects that they should serve as the basis for public/private plans for Internet recovery.
Review the NCS and NCSD organizational structures and roles in light of the convergence of voice and data communications.	In process	DHS officials stated that the creation of the Office of Cybersecurity and Communications acknowledges the increasing convergence of the IT and Communications Sectors. Further, DHS officials stated that NCS and NCSD are working closely together to ensure that activities are coordinated, issues are jointly addressed, and the resources and expertise of each organization are utilized. Moreover, the officials stated that the Office of Cybersecurity and Communications is working to co-locate the US-CERT and the NCC watch operations centers to ensure that IT and communications experts are working side-by-side to share situational awareness information and foster the early identification of attack trends, as well as the implications of these attacks, across all infrastructure sectors. We are currently evaluating DHS's efforts to restructure its organization in light of the convergence of voice and data communications.

Recommended Actions	Status	DHS Progress
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.	Not completed	DHS has reported the roles and responsibilities of its multiple working groups and initiatives, but has not fully described the relationships and interdependencies among the various Internet recovery-related activities currently under way.
Establish timelines and priorities for key efforts identified by the Internet Disruption Working Group (IDWG)	Not completed	DHS disbanded the IDWG because its functions are to be addressed by the IT and Communications Sector Specific Plans and the Cross-Sector Cyber Security Working Group. DHS officials reported that they may reconstitute the IDWG in the future if needed to address Internet resilience objectives that are not covered by other existing organizations.
Identify ways to incorporate lessons learned from actual incidents and during cyber exercises into recovery plans and procedures.	In process	DHS officials stated that they developed a Cyber Storm After Action Report, which was used to revise the NCRCG's operating documents, and the lessons learned were taken into account in the development of Cyber Storm II. DHS officials stated that exercises such as Cyber Storm and Cyber Tempest, as well as data from the Katrina After Action Report have been used in updating the *National Response Framework*. However, DHS has not yet developed a formal process for incorporating the lessons learned.
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 process	DHS officials stated that there are a number of ongoing initiatives within the department that seek to address the challenges to effective Internet recovery. • DHS reported that the strategic partnerships formed through the IDWG, the framework of the NIPP, implementation of the sector specific plans, the National Cyber Response Coordination Group, and operational activities conducted by US-CERT are helping to define the appropriate government functions in responding to a major Internet disruption. • An IDWG study examined the existence of incident triggers for responding to Internet disruptions and concluded that triggers or response thresholds vary from one private sector organization to another and that overall, the establishment of triggers would hold little value for infrastructure owners and operators. The study revealed that the development of triggers for the federal government could be useful if used across departments and agencies. Currently, US-CERT's incident levels provide the response categories that should guide department and agency involvement in responding to incidents. Moreover, the study demonstrated the need for greater understanding as to what the federal response would be in the event of an Internet disruption. • Agency officials stated that DHS is collaborating with the private sector to better understand existing operational and corporate governance policies. DHS acknowledges that more needs to be done to fully address these challenges.

Source: GAO analysis of DHS provided data.

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, much remains to be done.

DHS faces numerous challenges in developing integrated public/private recovery plans—not the least of which is 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, we 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. While DHS has made progress in implementing these recommendations, full implementation 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 me at (202) 512-6244, or by e-mail at wilshuseng@gao.gov. Other key contributors to this testimony include Scott Borre, Vijay D'Souza, Nancy Glover, Colleen Phillips, and Jeffrey Woodward.