



Highlights of [GAO-06-672](#), a report to congressional requesters

Why GAO Did This Study

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

What GAO Recommends

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

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

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

INTERNET INFRASTRUCTURE

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

What GAO Found

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

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

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

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