



Highlights of [GAO-08-113](#), a report to congressional requesters

Why GAO Did This Study

The nation's critical infrastructure sectors—such as public health, energy, water, and transportation—rely on computerized information and systems to provide services to the public. To fulfill the requirement for a comprehensive plan, including cyber aspects, the Department of Homeland Security (DHS) issued a national plan in June 2006 for the sectors to use as a road map to enhance the protection of critical infrastructure. Lead federal agencies, referred to as sector-specific agencies, are responsible for coordinating critical infrastructure protection efforts, such as the development of plans that are specific to each sector. In this context, GAO was asked to determine if these sector-specific plans address key aspects of cyber security, including cyber assets, key vulnerabilities, vulnerability reduction efforts, and recovery plans. To accomplish this, GAO analyzed each sector-specific plan against criteria that were developed on the basis of DHS guidance.

What GAO Recommends

To assist the sectors in securing their cyber infrastructure, GAO recommends that the Secretary of Homeland Security request that, by September 2008, the sector-specific agencies develop plans that address all of the cyber-related criteria. In written comments on a draft of this report, DHS concurred with GAO's recommendation and provided technical comments that have been addressed as appropriate.

To view the full product, including the scope and methodology, click on [GAO-08-113](#). For more information, contact David Powner at (202) 512-9286 or pownerd@gao.gov.

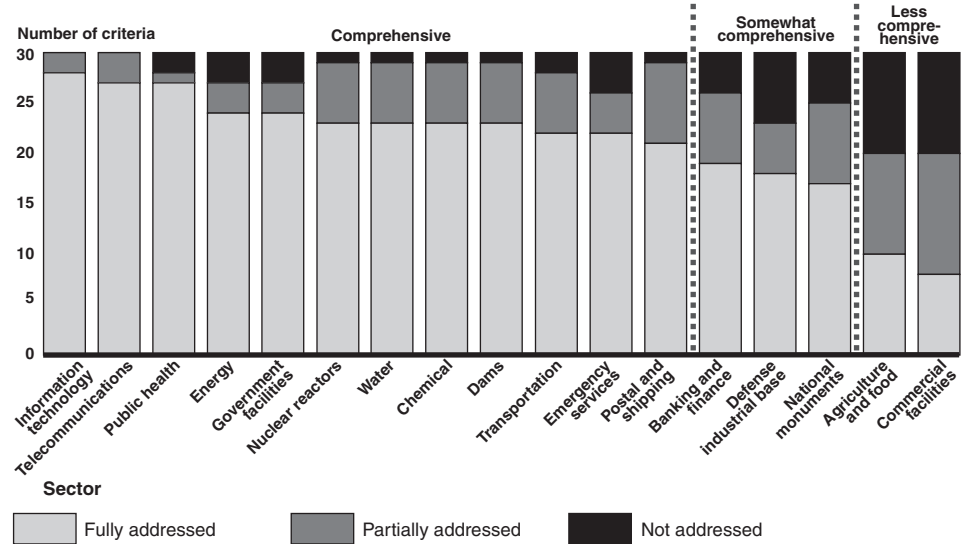
CRITICAL INFRASTRUCTURE PROTECTION

Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies

What GAO Found

The extent to which the sectors addressed aspects of cyber security in their sector-specific plans varied; none of the plans fully addressed all 30 cyber security-related criteria. Several sector plans—including the information technology and telecommunications sectors—fully addressed many of the criteria, while others—such as agriculture and food and commercial facilities—were less comprehensive. The following figure summarizes the extent to which each plan addressed the 30 criteria.

Comprehensiveness of Sector-Specific Plans



Source: GAO analysis of agency data.

In addition to the variations in the extent to which the plans covered aspects of cyber security, there was also variance among the plans in the extent to which certain criteria were addressed. For example, all plans fully addressed identifying a sector governance structure for research and development, but fewer than half of the plans fully addressed describing any incentives used to encourage voluntary performance of risk assessments. The varying degrees to which each plan addressed the cyber security-related criteria can be attributed in part to the varying levels of maturity in the different sectors.

DHS acknowledges the shortcomings in the plans, and officials stated that the sector-specific plans represent only the early efforts by the sectors to develop their respective plans. Nevertheless, until the plans fully address key cyber elements, stakeholders within the infrastructure sectors may not adequately identify, prioritize, and protect their critical assets. As the plans are updated, it will be important that DHS work with the sector representatives to ensure that the areas not sufficiently addressed are covered. Otherwise, the plans will remain incomplete and sector efforts will not be sufficient to enhance the protection of their computer-reliant assets.