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.

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. DHS 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, certain sectors may not be prepared to respond to a cyber attack against our nation’s critical infrastructure. 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.

To view the full product, including the scope and methodology, click on GAO-08-64T. For more information, contact David Powner at (202) 512-9286 or pownerd@gao.gov.