September 2009

CRITICAL INFRASTRUCTURE PROTECTION

Current Cyber Sector-Specific Planning Approach Needs Reassessment

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-969, a report to congressional requesters

Why GAO Did This Study

The nation's critical infrastructure sectors (e.g., energy, banking) rely extensively on information technology systems. The Department of Homeland Security (DHS) issued guidance in 2006 that instructed lead federal agencies, referred to as sector-specific agencies, to develop plans for protecting the sector's critical cyber and other (physical) infrastructure. These agencies issued plans in 2007, but GAO found that none fully addressed all 30 cyber security-related criteria identified in DHS's guidance and recommended that the plans be updated to address it by September 2008. GAO was asked to determine the extent to which sector plans have been updated to fully address DHS's cyber security requirements and assess whether these plans and related reports provide for effective implementation. To do this, GAO analyzed documentation, interviewed officials, and compared sector plans and reports with DHS cyber criteria.

What GAO Recommends

GAO recommends that DHS assess whether existing sector-specific planning processes should continue to be the nation's approach to securing cyber and other critical infrastructure and consider whether other options would provide more effective results. DHS concurred with the recommendation; however, it took exception with certain report facts and conclusions. GAO addressed these comments, but they did not result in substantive report revisions

View GAO-09-969 or key components.
For more information, contact David Powner, 202-512-9286, pownerd@gao.gov.

What GAO Found

Although DHS reported many efforts under way and planned to improve the cyber content of sector-specific plans, sector-specific agencies have yet to update their respective sector-specific plans to fully address key DHS cyber security criteria. For example, of the 17 sector-specific plans, only 9 have been updated. Of these 9 updates, just 3 addressed missing cyber criteria, and those 3 involved only a relatively small number (3 or fewer) of the criteria in question. Recently DHS issued guidance specifically requesting that the sectors address cyber criteria shortfalls in their 2010 sector-specific plan updates. Until the plans are issued, it is not clear whether they will fully address cyber requirements. Accordingly, the continuing lack of plans that fully address key cyber criteria has reduced the effectiveness of the existing sector planning approach and thus increases the risk that the nation's cyber assets have not been adequately identified, prioritized, and protected.

Most sector-specific agencies developed and identified in their 2007 sector plans those actions—referred to by DHS as implementation actions—essential to carrying out the plans; however, since then, most agencies have not updated the actions and reported progress in implementing them as called for by DHS guidance. Specifically, in response to 2006 guidance that called for agencies to address three key implementation elements (action descriptions, completion milestones, and parties responsible), most sectors initially developed implementation actions that fully addressed the key elements. However, while 2008 guidance called for implementation actions to be updated and for sector reports to include progress reporting against implementation action milestone commitments, only five sectors updated their plans and reported on progress against implementation actions. DHS attributed this in part to the department not following up and working to ensure that all sector plans are fully developed and implemented in accordance with department guidance.

The lack of complete updates and progress reports are further evidence that the sector planning process has not been effective and thus leaves the nation in the position of not knowing precisely where it stands in securing cyber critical infrastructures. Not following up to address these conditions also shows DHS is not making sector planning a priority. Further, recent studies by a presidential working group—which resulted in the President establishing the White House Office of Cybersecurity Coordinator—and an expert commission also identified shortfalls in the effectiveness of the current public-private partnership approach and related sector planning and offered options for improving the process. Such options include (1) prioritizing sectors to focus planning efforts on those with the most important cyber assets and (2) streamlining existing sectors to optimize their capacity to identify priorities and develop plans. Given this, it is essential that DHS and the to-be-appointed Cybersecurity Coordinator determine whether the current process as implemented should continue to be the national approach and thus worthy of further investment.