CRITICAL INFRASTRUCTURE PROTECTION

OMB Leadership Needed to Strengthen Agency Planning Efforts to Protect Federal Cyber Assets

What GAO Found

Key federal agencies developed and submitted cyber critical infrastructure protection plans or related documentation to OMB in response to the President’s direction (Homeland Security Presidential Directive 7) and associated OMB guidance. Specifically, of the 24 agencies, 18 submitted plans, while the remaining 6, as allowed by the guidance, provided documentation in lieu of plans stating that they neither owned nor operated any of the nation’s cyber critical infrastructure. The agencies submitted their plans and documentation to OMB by the July 31, 2004, deadline.

Agencies’ plans, in large part, did not fully address the 19 cyber and related requirements specified in OMB’s guidance. Specifically, only 4 of the 18 plans fully addressed all the criteria. While the other 14 plans fully addressed at least 8 or more criteria, they only partially addressed or did not address others—such as prioritizing key assets and documenting a strategy to protect them—that are essential for effectively planning for the protection of cyber assets. Since the development of these plans, 8 agencies whose plans did not fully meet OMB’s criteria have engaged in other critical infrastructure protection planning and related efforts that addressed some, but not all, of their shortfalls.

The shortfalls in meeting OMB’s guidance are attributable, in part, to OMB not making these plans a priority and managing them as such by, for example, following up on a regular basis to assess whether agencies are updating their plans to fully address the requirements and are effectively implementing them. When agencies submitted their initial plans, OMB reviewed and provided feedback on their adequacy, but did not follow up to verify that agencies had revised their plans to incorporate OMB feedback or to determine whether planning was being implemented and institutionalized. OMB attributed this to its attention being focused on other competing issues. In addition, OMB did not direct agencies to periodically update their plans. Without more sustained leadership, management, and oversight in this area, there is an increased risk that federal agencies individually, and the federal government collectively, will not effectively identify, prioritize, and protect their critical cyber assets, leaving them vulnerable to efforts to destroy, incapacitate, or exploit them.