September 2010

INFORMATION SECURITY

Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-916, a report to the Chairwoman, Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Historically, civilian and national security-related information technology (IT) systems have been governed by different information security policies and guidance. Specifically, the Office of Management and Budget and the Department of Commerce's National Institute of Standards and Technology (NIST) established policies and guidance for civilian non-national security systems, while other organizations, including the Committee on National Security Systems (CNSS), the Department of Defense (DOD), and the U.S. intelligence community, have developed policies and guidance for national security systems.

GAO was asked to assess the progress of federal efforts to harmonize policies and guidance for these two types of systems. To do this, GAO reviewed program plans and schedules, analyzed policies and guidance, assessed program efforts against key practices for cross-agency collaboration, and interviewed officials responsible for this effort.

What GAO Recommends

GAO is recommending that the Secretary of Commerce and the Secretary of Defense, among other things, update plans for future collaboration, establish timelines for implementing revised guidance, and fully implement key practices for interagency collaboration in the harmonization effort. In comments on a draft of this report, Commerce and DOD concurred with GAO's recommendations.

View GAO-10-916 or key components.
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Federal agencies have made progress in harmonizing information security policies and guidance for national security and non-national security systems. Representatives from civilian, defense, and intelligence agencies established a joint task force in 2009, led by NIST and including senior leadership and subject matter experts from participating agencies, to publish common guidance for information systems security for national security and non-national security systems. The harmonized guidance is to consist of NIST guidance applicable to non-national security systems and authorized by CNSS, with possible modifications, for application to national security systems. This harmonized security guidance is expected to result in less duplication of effort and more effective implementation of controls across multiple interconnected systems. The task force has developed three initial publications. These publications, among other things, provide guidance for applying a risk management framework to federal systems, identify an updated catalog of security controls and guidelines, and update the existing security assessment guidelines for federal systems. CNSS has issued an instruction to begin implementing the newly developed guidance for national security systems. Two additional joint publications are scheduled for release by early 2011, with other publications under consideration. Differences remain between guidance for national security and non-national security systems in such areas as system categorization, selection of security controls, and program management controls. NIST and CNSS officials stated that these differences may be addressed in the future but that some may remain because of the special nature of national security systems.

While progress has been made in developing the harmonized guidance, additional work remains to implement it and ensure continued progress. For example, task force members have stated their intent to develop plans for future harmonization activities, but these plans have not yet been finalized. In addition, while much of the harmonized guidance incorporates controls and language previously developed for use for non-national security systems, significant work remains to implement the guidance for national security systems. DOD and the intelligence community are developing agency-specific guidance and transition plans for implementing the harmonized guidance, but, according to officials, actual implementation could take several years to complete. Officials stated that this is primarily due to both the large number and criticality of the systems that must be reauthorized under the new guidance. Further, the agencies have yet to fully establish implementation milestones and lack performance metrics for measuring progress. Finally, the harmonization effort has been managed without full implementation of key collaborative practices, such as documenting identified needs and leveraging resources to address those needs, agreed-to agency roles and responsibilities, and processes to monitor and report results. Task force members stress that their informal, flexible approach has resulted in significant success. Nevertheless, further implementation of key collaborative practices identified by GAO could facilitate further progress.