GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-06-385, a report to congressional requesters

Why GAO Did This Study

A number of initiatives to improve information sharing have been called for, including the Homeland Security Act of 2002 and in the Intelligence Reform and Terrorism Prevention Act of 2004. The 2002 act required the development of policies for sharing classified and sensitive but unclassified homeland security information. The 2004 act called for the development of an Information Sharing Environment for terrorism information.

This report examines (1) the status of efforts to establish government-wide information sharing policies and processes and (2) the universe of sensitive but unclassified designations used by the 26 agencies that GAO surveyed and their related policies and procedures.

What GAO Recommends

To provide for information-sharing policies and procedures, GAO recommends that the Director of National Intelligence (DNI) assess progress, address barriers, and propose changes, and that OMB work with agencies on policies, procedures, and controls to help achieve more accountability. OMB said that once ODNI completed its work, OMB would work with ODNI and all agencies on additional steps, if needed. ODNI declined to comment on our report, indicating that the subject matter is outside GAO's purview. We disagree with this assessment because it does not accurately reflect the scope of GAO's statutory authorities.

www.gao.gov/cgi-bin/getrpt?GAO-06-385.

To view the full product, including the scope and methodology, click on the link above. For more information, contact David Powner, 202-512-9286, pownerd@gao.gov or Eileen Larence, 202-512-6510, larencee@gao.gov.

March 2006

INFORMATION SHARING

The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information

What GAO Found

More than 4 years after September 11, the nation still lacks governmentwide policies and processes to help agencies integrate the myriad of ongoing efforts, including the agency initiatives we identified, to improve the sharing of terrorism-related information that is critical to protecting our homeland. Responsibility for creating these policies and processes shifted initially from the White House to the Office of Management and Budget (OMB), and then to the Department of Homeland Security, but none has yet completed the task. Subsequently, the Intelligence Reform Act called for creation of an Information Sharing Environment, including governing policies and processes for sharing, and a program manager to oversee its development. In December 2005, the President clarified the roles and responsibilities of the program manager, now under the Director of National Intelligence, as well as the new Information Sharing Council and the other agencies in support of creating an Information Sharing Environment by December 2006. At the time of our review, the program manager was in the early stages of addressing this mandate. He issued an interim implementation report with specified tasks and milestones to Congress in January 2006, but soon after announced his resignation. This latest attempt to establish an overall information-sharing road map under the Director of National Intelligence, if it is to succeed once a new manager is appointed, will require the Director's continued vigilance in monitoring progress toward meeting key milestones, identifying any barriers to achieving them, and recommending any necessary changes to the oversight committees.

The agencies that GAO reviewed are using 56 different sensitive but unclassified designations (16 of which belong to one agency) to protect information that they deem critical to their missions—for example, sensitive law or drug enforcement information or controlled nuclear information. For most designations there are no governmentwide policies or procedures that describe the basis on which an agency should assign a given designation and ensure that it will be used consistently from one agency to another. Without such policies, each agency determines what designations and associated policies to apply to the sensitive information it develops or shares. More than half the agencies reported challenges in sharing such information. Finally, most of the agencies GAO reviewed have no policies for determining who and how many employees should have authority to make sensitive but unclassified designations, providing them training on how to make these designations, or performing periodic reviews to determine how well their practices are working. The lack of such recommended internal controls increases the risk that the designations will be misapplied. This could result in either unnecessarily restricting materials that could be shared or inadvertently releasing materials that should be restricted.