GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-08-91, a report to the Committee on Armed Services, U.S. Senate

Why GAO Did This Study

The Department of Defense (DOD) invests billions of dollars on sophisticated weapon systems and technologies. These may be at risk of exploitation when exported, stolen, or lost during combat or routine missions. In an effort to minimize this risk, DOD developed an anti-tamper policy in 1999, calling for DOD components to implement anti-tamper techniques for critical technologies.

In March 2004, GAO reported that program managers had difficulties implementing this policy, including identifying critical technologies. This follow-up report (1) describes recent actions DOD has taken to implement its anti-tamper policy and (2) identifies challenges facing program managers.

GAO reviewed documentation on actions DOD has taken since 2004 to implement its anti-tamper policy, and interviewed officials from the Anti-Tamper Executive Agent's Office, the military services, other DOD components, and a cross-section of program offices.

What GAO Recommends

To better ensure implementation of DOD's anti-tamper policy, GAO is recommending that DOD issue departmentwide direction for its policy and provide additional tools for program managers. DOD agreed to provide additional tools to assist program managers. However, DOD believes that a directive it is currently updating addresses GAO's other concern. GAO continues to call for immediate departmentwide direction.

To view the full product, including the scope and methodology, click on GAO-08-91.
For more information, contact Ann Calvaresi-Barr at (202) 512-4841 or calvaresibarra@gao.gov.

January 2008

DEFENSE ACQUISITIONS

Departmentwide Direction Is Needed for Implementation of the Anti-tamper Policy

What GAO Found

Since 2004, DOD has taken several actions to raise awareness about anti-tamper protection and develop resources that provide program managers with general information on its anti-tamper policy. These actions include developing a Web site with anti-tamper information and events, establishing an online learning module on anti-tamper protection, and sponsoring research on generic anti-tamper techniques. However, DOD lacks departmentwide direction for implementation of its anti-tamper policy. Without such direction, individual DOD components are left on their own to develop initiatives. For example, the Navy is developing a database that is intended to provide a horizontal view of what DOD components have identified as critical program information. While many officials we spoke with pointed to this database as a potential tool for identifying critical technologies that may need anti-tamper protection, the database is currently incomplete. Specifically, the Missile Defense Agency is not providing information because its information is classified at a level above what the database can support. Also, the Air Force is not currently providing information because not all commands have provided consent to participate.

At the same time, program managers face challenges implementing DOD's anti-tamper policy—due largely to a lack of information or tools needed to make informed assessments at key decision points. First, program managers have limited information for defining what is critical or insight into what technologies other programs have deemed critical to ensure similar protection across programs. Determining whether technologies are critical is largely left to the discretion of the individual program manager, resulting in an uncoordinated and stove piped process. Therefore, the same technology can be identified as critical in one program office but not another. Second, program managers have not always had sufficient or consistent information from the intelligence community to identify threats and vulnerabilities to technologies that have been identified as critical. The potential impact of inconsistent threat assessments is twofold: If the threat is deemed to be low but is actually high, the technology is susceptible to tampering; conversely, if the threat is deemed to be high and is actually low, an anti-tamper solution is more robust than needed. Finally, program managers have had difficulty selecting sufficient anti-tamper solutions—in part because they lack information and tools, such as risk and cost-estimating models, to determine how much anti-tamper protection is needed. As a result, program managers may select a suboptimal solution. Given these combined challenges, there is an increased risk that some technologies that need protection may not be identified or may not have sufficient protection.