March 2004

DEFENSE ACQUISITIONS

DOD Needs to Better Support Program Managers' Implementation of Anti-Tamper Protection

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-302, a report to the Senate Committee on Armed Services

Why GAO Did This Study

The U.S. government has invested hundreds of billions of dollars in developing the most sophisticated weapon systems and technologies in the world. Yet, U.S. weapons and technologies are vulnerable to exploitation, which can weaken U.S. military advantage, shorten the expected combat life of a system, and erode the U.S. industrial base's technological competitiveness. In an effort to protect U.S. technologies from exploitation, the Department of Defense (DOD) established in 1999 a policy directing each military service to implement anti-tamper techniques, which include software and hardware protective devices.

This report reviews DOD's implementation of the anti-tamper policy as required by the Senate report accompanying the National Defense Authorization Act for Fiscal Year 2004.

What GAO Recommends

GAO is recommending that the Secretary of Defense direct the Under Secretary of Acquisition, Technology, and Logistics and the anti-tamper Executive Agent to take several actions to improve oversight and assist program offices in implementing anti-tamper protection on weapon systems.

DOD concurred or partially concurred with the recommendations, but it suggested alternative language for several, which GAO incorporated when appropriate.

www.gao.gov/cgi-bin/getrpt?GAO-04-302.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Katherine V. Schinasi (202) 512-4841 or schinasik@gao.gov.

What GAO Found

Program managers have encountered difficulties in implementing DOD's anti-tamper policy on individual weapon systems. First, defining a critical technology—a basis for determining the need for anti-tamper—is subjective, which can result in different conclusions regarding what needs anti-tamper protection. While different organizations can check on program managers' assessments, no organization has complete information or visibility across all programs. Some program managers said they needed assistance in determining which technologies were critical, but resources to help them were limited or unknown and therefore not requested. Second, anti-tamper protection is treated as an added requirement and can affect a program's cost and schedule objectives, particularly if the program is further along in the acquisition process. Programs GAO contacted experienced or estimated cost increases, and some encountered schedule delays when applying anti-tamper protection. Officials from one program stated that their existing budget was insufficient to cover the added cost of applying anti-tamper protection and that they were waiting for separate funding before attempting to apply such protection. Finally, anti-tamper techniques can be technically difficult to incorporate in some weapon systems—particularly when the techniques are not fully developed or when the systems are already in design or production. One program that had difficulty incorporating the techniques resorted to alternatives that provided less security. While DOD is overseeing the development of generic anti-tamper techniques and tools to help program managers, many of these efforts are still in progress, and program managers ultimately have to design and incorporate techniques needed for their unique systems.