GAO
Accountability•Integrity•Reliability

Highlights

Highlights of GAO-04-678, a report to congressional requesters

May 2004

DEFENSE ACQUISITIONS

Knowledge of Software Suppliers Needed to Manage Risks

Why GAO Did This Study

The Department of Defense (DOD) is increasingly reliant on software and information systems for its weapon capabilities, and DOD prime contractors are subcontracting more of their software development. The increased reliance on software and a greater number of suppliers results in more opportunities to exploit vulnerabilities in defense software. In addition, DOD has reported that countries hostile to the United States are focusing resources on information warfare strategies. Therefore, software security, including the need for protection of software code from malicious activity, is an area of concern for many DOD programs.

GAO was asked to examine DOD's efforts to (1) identify software development suppliers and (2) manage risks related to foreign involvement in software development on weapon systems.

What GAO Recommends

To address software vulnerabilities and threats, GAO recommends that DOD better define software security requirements and require program managers to mitigate associated risks accordingly.

DOD agreed with the findings but only partially concurred with the recommendations over concerns that they place too much responsibility for risk mitigation with program managers. GAO has broadened the recommendations to address DOD's concerns.

www.gao.gov/cgi-bin/getrpt?GAO-04-678.

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

What GAO Found

DOD acquisition and software security policies do not fully address the risk of using foreign suppliers to develop weapon system software. The current acquisition guidance allows program officials discretion in managing foreign involvement in software development, without requiring them to identify and mitigate such risks. Moreover, other policies intended to mitigate information system vulnerabilities focus mostly on operational software security threats, such as external hacking and unauthorized access to information systems, but not on insider threats, such as the insertion of malicious code by software developers. Recent DOD initiatives may provide greater focus on these risks, but to date have not been adopted as practice within DOD.

While DOD has begun to recognize potential risks from foreign software content, this is not always the case within the weapon programs where software is developed or acquired. Program officials for the systems in this review did not make foreign involvement in software development a specific element of their risk identification and mitigation efforts. As a result, program officials' knowledge of the foreign developed software included in their weapon systems varied. In addition, risk mitigation efforts emphasized program level risks, such as meeting program cost and schedule goals, instead of software security risks. Further, program officials often delegated risk mitigation and source selection to contractors who are primarily concerned with software functionality and quality assurance, rather than specifically addressing software security for development risks associated with foreign suppliers. Unless program officials provide specific guidance, contractors may favor business considerations over potential software development security risks associated with using foreign suppliers.

As the amount of software on weapon systems increases, it becomes more difficult and costly to test every line of code. Further, DOD cannot afford to monitor all worldwide software development facilities or provide clearances for all potential software developers. Therefore, the program manager must know more about who is developing software and where early in the software acquisition process, so that it can be included as part of software source selection and risk mitigation decisions.

United States General Accounting Office