March 2006

INFORMATION ASSURANCE

National Partnership Offers Benefits, but Faces Considerable Challenges

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-392, a report to the Honorable William Lacy Clay, House of Representatives

Why GAO Did This Study

In 1997, the National Security Agency and the National Institute of Standards and Technology formed the National Information Assurance Partnership (NIAP) to boost federal agencies' and consumers' confidence in information security products manufactured by vendors. To facilitate this goal, NIAP developed a national program that requires accredited laboratories to independently evaluate and validate the security of these products for use in national security systems. These systems are those under control of the U.S. government that contain classified information or involve intelligence activities.

GAO was asked to identify (1) the governmentwide benefits and challenges of the NIAP evaluation process on national security systems, and (2) the potential benefits and challenges of expanding the requirement of NIAP to non-national security systems, including sensitive but unclassified systems.

What GAO Recommends

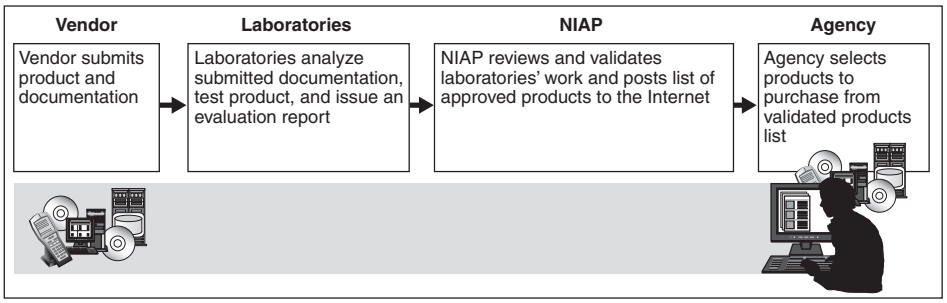
GAO is making two recommendations to address challenges with the NIAP evaluation process, including establishing and documenting performance measures on process effectiveness. The Department of Defense concurred with one of our recommendations and partially concurred with the other.

www.gao.gov/cgi-bin/getrpt?GAO-06-392. To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

While NIAP process participants—vendors, laboratories, and federal agencies—indicated that the process (see figure below) offers benefits for use in national security systems, its effectiveness has not been measured or documented, and considerable challenges to acquiring and using NIAP-evaluated products exist. Specific benefits included independent testing and evaluation of products and accreditation of the performing laboratories, the discovery and correction of product flaws, and improvements to vendor development processes. However, process participants also face several challenges, including difficulty in matching agencies' needs with the availability of NIAP-evaluated products, vendors' lack of awareness regarding the evaluation process, and a lack of performance measures and difficulty in documenting the effectiveness of the NIAP evaluation process. Collectively, these challenges hinder the effective use of the NIAP evaluation process by vendors and agencies.

Simplified Overview of NIAP Evaluation Process



Source: GAO analysis of NIAP data.

Expanding the requirement of the NIAP evaluation process to non-national security systems is likely to yield similar benefits and challenges as those experienced by current process participants. For example, a current benefit—independent testing and evaluation of IT products—gives agencies confidence that validated features of a product will perform as claimed by the vendor. However, federal policy already allows agencies with non-national security systems to consider acquiring NIAP-evaluated products for those systems, and requiring that they do so may further exacerbate current resource constraints related to the evaluation and validation of products. In the absence of such a requirement, agencies seeking information assurance (measures that defend and protect information and information systems by ensuring their confidentiality, integrity, authenticity, availability, and utility) for their non-national security systems have other federal guidance and standards available to them.