

GAO

Report to the Honorable William Lacy
Clay, House of Representatives

March 2006

INFORMATION
ASSURANCE

National Partnership
Offers Benefits, but
Faces Considerable
Challenges



G A O

Accountability * Integrity * Reliability

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 wilshusen@gao.gov.

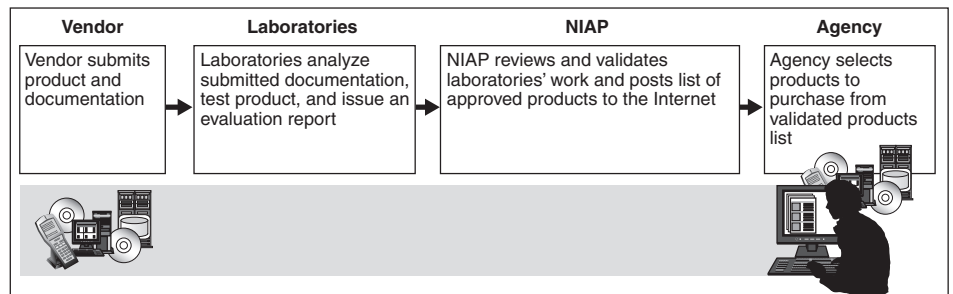
INFORMATION ASSURANCE

National Partnership Offers Benefits, but Faces Considerable Challenges

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.

Contents

Letter		1
	Results in Brief	2
	Background	4
	NIAP Offers Benefits for Use in National Security Systems, but Process Faces Considerable Challenges	11
	Expanding NIAP Requirement to Non-national Security Systems May Yield Many of the Same Benefits and Challenges and Could Exacerbate Resource Constraints	21
	Conclusions	22
	Recommendations for Executive Action	23
	Agency Comments and Our Evaluation	23

Appendixes

Appendix I: Objectives, Scope, and Methodology	25
Appendix II: Common Criteria Evaluation Assurance Levels	27
Appendix III: Comments from the Department of Defense	28
Appendix IV: GAO Contact and Staff Acknowledgments	31

Table

Table 1: Summary of the Common Criteria Evaluation Assurance Levels	27
---	----

Figures

Figure 1: The NIAP Evaluation Process	7
Figure 2: Range of Sample Cost of NIAP Evaluations to Vendors by Evaluation Assurance Level	8
Figure 3: Laboratory Accreditation Process	13
Figure 4: Range of Time Required for Completing Product Evaluations at Various Evaluation Assurance Levels	19

Abbreviations

IT	information technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, D.C. 20548

March 24, 2006

The Honorable William Lacy Clay
House of Representatives

Dear Mr. Clay:

The sophistication and effectiveness of cybersecurity attacks have advanced steadily over the past few years and have drastically changed the way we think about protecting our information and information systems, including national security systems.¹ Commercial-off-the-shelf information assurance products and information assurance-enabled products or technologies² are readily available to agencies as well as consumers providing needed security services. Acquiring such products for use on national security systems that perform as claimed by the vendors who manufacture these products is a governmentwide challenge.

In 1997, the National Information Assurance Partnership (NIAP) was formed by the National Security Agency and the National Institute of Standards and Technology (NIST) to boost federal agencies' and consumers' confidence in commercial-off-the-shelf products. To facilitate this goal, NIAP developed a national program that uses accredited laboratories to independently evaluate and validate the security of vendor products using standardized processes. The NIAP program allows the U.S. to meet federal agency needs by participating in an international arrangement to validate security products using standardized processes. In addition, the Committee on National Security Systems established a federal policy which mandates, among other things, the use of NIAP-evaluated products for national security systems. Further, the policy allows but does

¹National security systems are telecommunications and information systems under control of the United States government which contain classified information or the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapon system; or is critical to the direct fulfillment of military or intelligence missions.

²An information assurance product is an information technology (IT) product or technology that primarily provides security services (such as confidentiality and integrity), corrects known vulnerabilities, and provides layered defense against various categories of non-authorized and malicious penetration of information systems or networks. An information assurance-enabled product is an IT product or technology that provides security services as an associated feature of its intended operating capabilities, rather than as its primary role.

not require users of non-national security systems to acquire NIAP-evaluated products.

Our objectives were to identify (1) the governmentwide benefits and challenges of the NIAP evaluation process for national security systems and (2) the potential benefits and challenges of expanding the requirement of using NIAP-evaluated products for non-national security systems, including sensitive but unclassified systems. To address these objectives, we obtained perspectives from selected industry groups and various NIAP process participants, such as vendors, accredited laboratories, and government officials. We also developed and submitted a survey questionnaire to the 24 federal agencies—also process participants—cited in the Chief Financial Officer's Act of 1990 (Public Law 101-576) to determine their use of, and perspectives on, NIAP-evaluated products. In addition, we analyzed documentation related to NIAP evaluation and validation policies and processes, test and evaluation criteria, and laboratory accreditation processes. We conducted our work in Washington, D.C., from May 2005 through February 2006, in accordance with generally accepted government auditing standards. See appendix I for more details about our objectives, scope, and methodology.

Results in Brief

While the NIAP process offers benefits to national security systems, its effectiveness has not been measured or documented, and considerable challenges to acquiring and using NIAP-evaluated products exist. Specific benefits include

- independent testing and evaluation of products and accreditation of the performing laboratories, which can increase agencies' confidence that products will perform as claimed;
- the ability to participate in an international arrangement of recognized products, which gives agencies broader product selection and reduces vendor workload;
- the discovery and correction of product flaws, which help to give agencies greater confidence that the product will perform as claimed; and
- improvements to vendor development processes, which can result in quality improvements to current and future products.

However, the NIAP process also faces several challenges, including

- difficulty in matching agencies' needs with the availability of NIAP-evaluated products;
- vendors' lack of awareness regarding the evaluation process;
- a reduction in the number of validators to certify products; and
- a lack of performance measures and difficulty in documenting the effectiveness of the NIAP process.

Collectively, these challenges hinder the effective use of the NIAP process by vendors and agencies.

Expanding the requirement of the NIAP evaluation process to non-national security systems is likely to yield the same benefits and challenges as those experienced by current process participants. While federal policy allows agencies with non-national security systems to consider using the NIAP process to acquire evaluated and validated products, 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 for their non-national security systems have other federal guidance and standards available to them.

We are making recommendations to assist NIAP officials in addressing process challenges, including developing awareness training workshops for program participants and establishing and documenting performance measures on process effectiveness.

In providing written comments on a draft of this report, the Deputy Assistant Secretary of Defense (Deputy Chief Information Officer) partially agreed with one of our recommendations, agreed with the other, and described ongoing and planned efforts to address them. The Deputy Assistant Secretary's comments are reprinted in appendix III. The Department of Defense and the Department of Homeland Security also provided technical comments, which we considered and addressed in our report, as appropriate.

Background

The growing sophistication and effectiveness of cyber attacks, and the increase of information assurance and information assurance-enabled information technology (IT) products available for use on national security systems, have heightened federal attention to the need for information assurance.³ As a result of these trends, acquiring commercial IT products that perform as vendors claim on national security systems has become a governmentwide challenge. While not a complete solution, an important way to increase confidence in commercial IT products is through independent testing and evaluation of their security features and functions during design and development.

Federal Partnership Formed to Promote the Use of Evaluated IT Products

In 1997, NIST and the National Security Agency⁴ collaborated to form the NIAP. The purpose of the partnership is to boost consumers' and federal agencies' confidence in information security products and enhance the ability of U.S. companies to gain international recognition and acceptance for their products. The five main goals of NIAP are to:

- promote the development and use of evaluated IT products and systems;
- champion the development and use of national and international standards for IT security;
- foster research and development in IT security requirements definition, test methods, tools, techniques, and assurance metrics;
- support a framework for international recognition and acceptance of IT security testing and evaluations; and
- facilitate development and growth of a commercial security testing industry within the U.S.

³Information assurance refers to measures that defend and protect information and information systems by ensuring their confidentiality, integrity, authenticity, availability, and utility.

⁴The Director of the National Security Agency is the Department of Defense focal point for National Information Assurance Partnership (NIAP).

To facilitate achievement of these goals, NIAP developed a national program called the Common Criteria Evaluation and Validation Scheme. The program is based on an international standard of general concepts and principles of IT security evaluations⁵ for the international community. The program evaluates, through various evaluation assurance levels (see app. II),⁶ commercial-off-the-shelf information assurance and information assurance-enabled products for the federal government. These products can be items of hardware, software, or firmware.⁷ As part of the evaluation, agencies can specify a degree of confidence desired in a product through protection profiles.⁸ While a protection profile is not required in order to have a product evaluated, a vendor is required to develop a security target.⁹

NIAP evaluations are performed by accredited Common Criteria testing laboratories.¹⁰ While a product is undergoing evaluation, the NIAP validation body—an activity currently managed by the National Security Agency—approves participation of security testing laboratories in accordance with accreditation policies and procedures.¹¹ It also reviews the results of the security evaluations performed by the laboratories and

⁵Known as the Common Criteria, the international standard contains IT security requirements, constructs for describing IT security objectives, and a framework for writing high-level security specifications for a product. It specifies functional security requirements and seven predefined assurance packages, referred to as evaluation assurance levels.

⁶Evaluation assurance levels provide a reference for the amount of analysis and testing performed on a product.

⁷Computer programs that are stored in read-only memory are called firmware.

⁸Protection profiles define a security problem for a given collection of systems or products and delineate security requirements to address that problem without specifying how these requirements will be implemented. U.S. government protection profiles are developed into one of three robustness levels—basic, medium, and high.

⁹A security target is a specifications document that describes the security functionality of a product and the environment in which it will operate. The security target details the desired evaluation assurance levels that the vendor wants the product to be tested against. Vendors can also claim conformance to a protection profile in their security targets.

¹⁰The National Voluntary Laboratory Accreditation Program (NVLAP) is administered by the National Institute of Standards and Technology (NIST), and operates as an unbiased third-party to accredit testing and calibration laboratories in many fields. NVLAP operates on a cost-reimbursable basis from fees paid by participating laboratories.

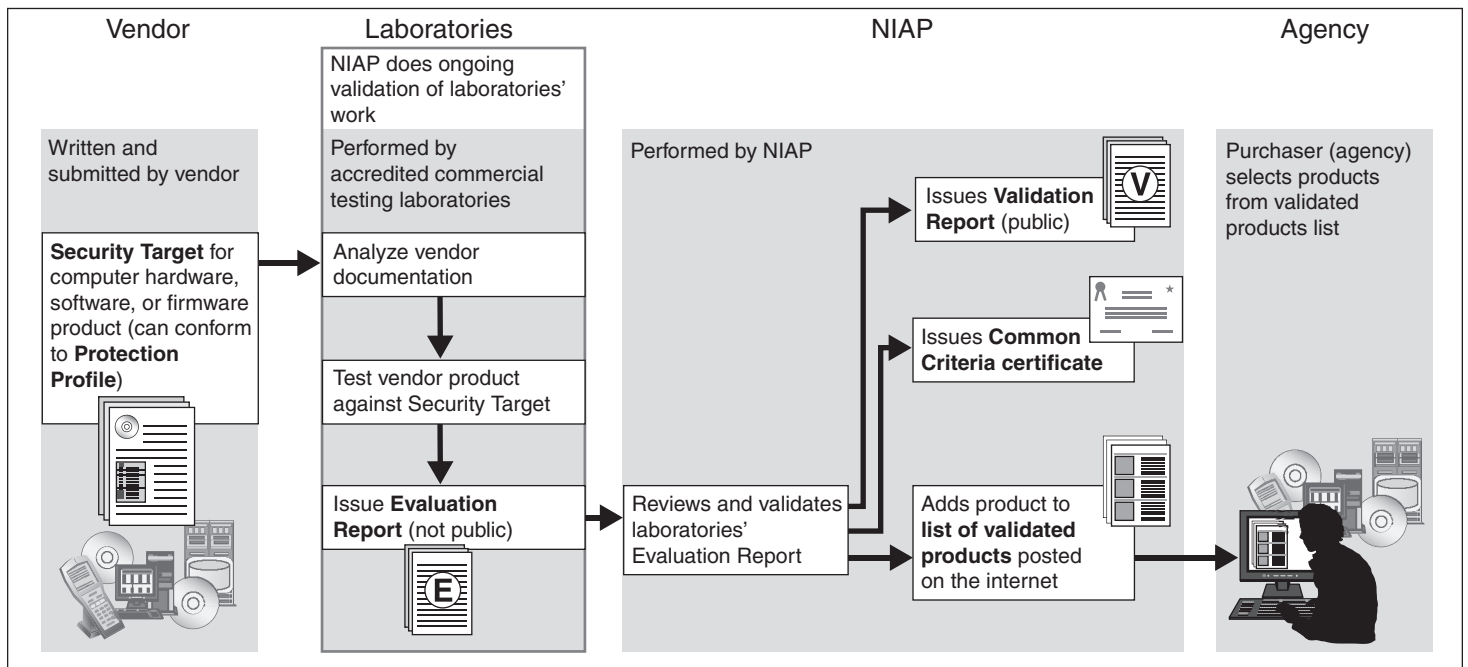
¹¹According to NIAP, as the initiative has evolved, the National Security Agency has assumed all of the validation responsibilities; NIST no longer participates in discharging these responsibilities.

issues a validation report, which summarizes and provides independent validation of the results. A product is considered NIAP-certified only after it is both evaluated by an accredited laboratory and validated by the validation body. Upon successful completion of these requirements, the validation body issues a Common Criteria certificate for the evaluated product. All evaluated products that receive a NIAP Common Criteria certificate appear on a validated products list available on NIAP's Web site. According to the Committee on National Security Systems¹²—a forum for the discussion of policy issues that sets federal policy and promulgates direction, operational procedures, and guidance for the security of national security systems—the fact that a product appears on the validated products list does not by itself mean that it is secure. A product's listing on any Common Criteria validated products list means that the product was evaluated against its security claims and that it has met those claims.¹³ Figure 1 outlines the NIAP evaluation process.

¹²The Committee on National Security Systems consists of representatives from 20 U.S. government departments and agencies who are given voting privileges on all committee activities. National Security Directive 42 specifies the membership of the committee. The Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer serves as the chair of the committee.

¹³Federal agencies and consumers should review the security targets that describe the threats, objectives, and requirements against which the product has been tested to determine if the product is appropriate for a particular application or system and that it provides adequate information security protections for the intended operational environment.

Figure 1: The NIAP Evaluation Process

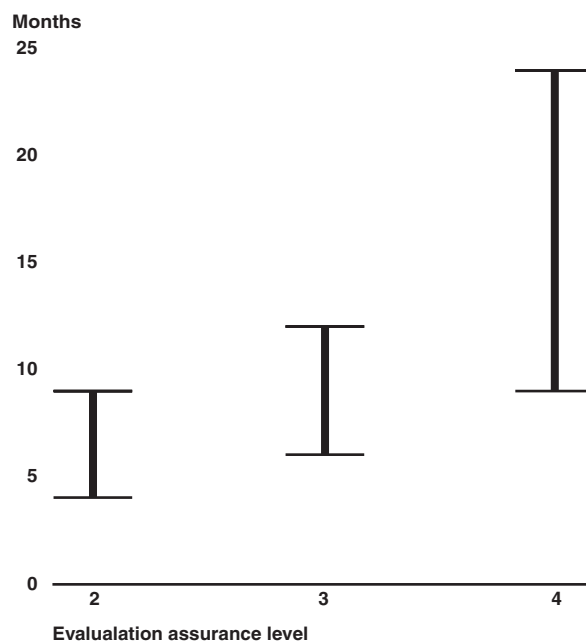


Source: GAO analysis of NIAP data.

In order to maintain the validity of an evaluation when a product upgrades to its next version, a vendor can request either a re-evaluation of the entire new product version or validation of only the changes in the product. To request the latter, a vendor must participate in the NIAP Assurance Maintenance Program. To participate in this program, a vendor must submit a request that addresses how it plans to maintain the product and a report of what will be maintained.

Vendors can select any one of the 10 accredited commercial testing laboratories to perform product evaluations.¹⁴ The vendor and testing laboratory negotiate evaluation costs, which can vary according to the laboratory and the assurance level the product is tested against¹⁵ (see fig. 2).

Figure 2: Range of Sample Cost of NIAP Evaluations to Vendors by Evaluation Assurance Level



Source: GAO analysis of data provided by laboratories.

Other factors that influence the overall cost of NIAP product evaluations include

¹⁴Products whose evaluations have assurance components above assurance level 4 must be tested by the National Security Agency for that portion of the product's features and function that are above level 4.

¹⁵NVLAP identifies NVLAP-accredited laboratories on its Web site. Accreditation criteria are established in accordance with the U.S. Code of Federal Regulations (CFR, Title 15, Part 285), NVLAP Procedures and General Requirements, and encompass the requirements of ISO/IEC 17025 and the relevant requirements of ISO 9002.

-
- the scope of evaluation—the tendency of vendors to include elements in their security target that agencies may not require introduces additional costs; and
 - the design of the product—if a product is designed so that its security functions are performed by a small number of modules, it may be possible to limit the portion of the product that must be examined.

Federal Policy Requires Evaluated Products for National Security Systems

In January 2000, as revised in June 2003, a federal policy was established that required the use of evaluated products for national security systems. Specifically, the Committee on National Security Systems established National Security Telecommunications and Information Systems Security Policy Number 11.¹⁶ The policy required, effective July 1, 2002, that all commercial-off-the-shelf information assurance and information assurance-enabled IT products acquired for use on national security systems be evaluated and validated in accordance with one of the following criteria:

1. The International Common Criteria for Information Security Technology Evaluation Recognition Arrangement,¹⁷
2. The NIAP Common Criteria Evaluation and Validation Scheme,
3. The NIST Federal Information Processing Standards Cryptographic Module Validation Program.¹⁸

¹⁶The Committee on National Security Systems was formerly known as the National Security Telecommunications and Information Systems Security Committee.

¹⁷In October 1998, the U.S., Canada, France, Germany, and the United Kingdom signed an arrangement for Common-Criteria-based security evaluations covering evaluated assurance levels 1-4 known as the Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security. The arrangement sought to create a situation in which IT products and protection profiles that earn a Common Criteria certificate in one arrangement member country can be procured or used without the need for further evaluation in other arrangement member countries.

¹⁸The policy requires that any commercial off-the-shelf information assurance or information assurance-enabled product using cryptographic technology be certified by the Cryptographic Module Validation Program, which evaluates products for conformance to FIPS 140-2, Security Requirements for Cryptographic Modules.

The objective of the policy is to ensure that these products, which are acquired by the federal government, undergo a standardized evaluation validating that a product either performs as its claims or meets the user's security requirements. The policy requires that the evaluation and validation of such products be conducted by accredited commercial laboratories or by the National Security Agency for government off-the-shelf products. It does not require mandatory compliance for information assurance products acquired prior to July 1, 2002, and includes a provision for deferred compliance, on a case-by-case basis, when information assurance-evaluated products do not cover the full range of potential user application, or do not incorporate the most current technology.

Moreover, while not a requirement, the federal policy includes provisions for departments and agencies who may wish to consider using the NIAP process for the acquisition and appropriate implementation of evaluated and validated products for non-national security systems.

NIAP Evaluation Process Contributes to System Security, but Is Not a Complete Solution

The use of commercial products that have been independently tested and evaluated is only a part of a security solution that contributes to the overall information assurance of a product. Other complementary controls are needed, including sound operating procedures, adequate information security training, overall system certification and accreditation,¹⁹ sound security policies, and well-designed system architectures. According to the Committee on National Security Systems, the protection of systems encompasses more than just acquiring the right product. The committee notes that once acquired, these products must be integrated properly and subjected to a system accreditation process, as discussed above, which will help to ensure the integrity of the information and systems to be protected.

For federal agencies, such an overall security solution is spelled out by the Federal Information Security Management Act. The act requires federal agencies to protect and maintain the confidentiality, integrity, and availability of their information and information systems. Among other

¹⁹Certification is a comprehensive evaluation of security controls that provides the necessary information for a designated approving authority to formally declare that a system is approved to operate at an acceptable level of risk. Accreditation is the authorization of an information system to process, store, or transmit information that provides a form of quality control. The accreditation decision, which is supported by the certification, provides the necessary information for a designated approving authority to formally declare that a system is approved to operate.

things, the act requires each agency (including agencies with national security systems) to develop, document, and implement agencywide information security programs to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

More specifically, the Federal Information Security Management Act stipulates that the head of each agency operating or exercising control of a national security system is responsible for providing information security protections commensurate with the risk and magnitude of harm that could result should a security breach occur. The act also stipulates that agency heads are responsible for implementing information security policies and practices as required by standards and guidelines for national security systems. The Department of Defense and the Director of Central Intelligence have authority under the act to develop policies, guidelines, and standards for national security systems.

The Federal Information Security Management Act also requires NIST, among other things, to provide technical assistance to agencies; to evaluate private sector security policies and practices; to evaluate commercially available IT, as well as practices developed for national security systems; and to assess the potential application by agencies to strengthen information security for non-national systems.

NIAP Offers Benefits for Use in National Security Systems, but Process Faces Considerable Challenges

While the NIAP evaluation process offers benefits to national security systems, its effectiveness has not been measured or documented, and considerable challenges to acquiring and using NIAP-evaluated products exist.

NIAP Evaluation Process Offers Benefits

NIAP process participants—vendors, laboratories, federal agencies, and NIAP officials—identified benefits to using the process for use in national security systems, including

-
- independent testing and evaluation of IT products and accreditation of the performing laboratories, which can give agencies confidence that the products will perform as claimed;
 - international recognition of evaluated products, which provides agencies broader product selection and reduces vendor burden;
 - discovery of software flaws in product security features and functions, which can cause vendors to fix them; and
 - improvements to vendor development processes, which help to improve the overall quality of current and future products.

Independent Testing and Evaluation of Products and Accreditation of Laboratories Can Increase Product Assurance

Independent testing and evaluation of commercial IT products and accreditation of the laboratories that perform the test and evaluations can give agencies increased assurance that the products will perform as vendors claim. Independent testing is a best practice for assuring conformance to functional, performance, reliability, and interoperability specifications—especially for systems requiring elevated levels of security or trust. As discussed previously, NIAP requires vendors to obtain independent testing and evaluation of specific security features and functions that are built into their products. Agencies are able to use the results of validation reports to distinguish between competing products and thus make better-informed IT procurement decisions. Further, the Committee on National Security Systems encourages agencies to review the security target of a product and determine its appropriateness for the environment in which the product will operate.

In our survey, 15 of 18 federal agencies²⁰ reported that they have derived benefits from acquiring and using products evaluated by the NIAP process. Of these 15 agencies,

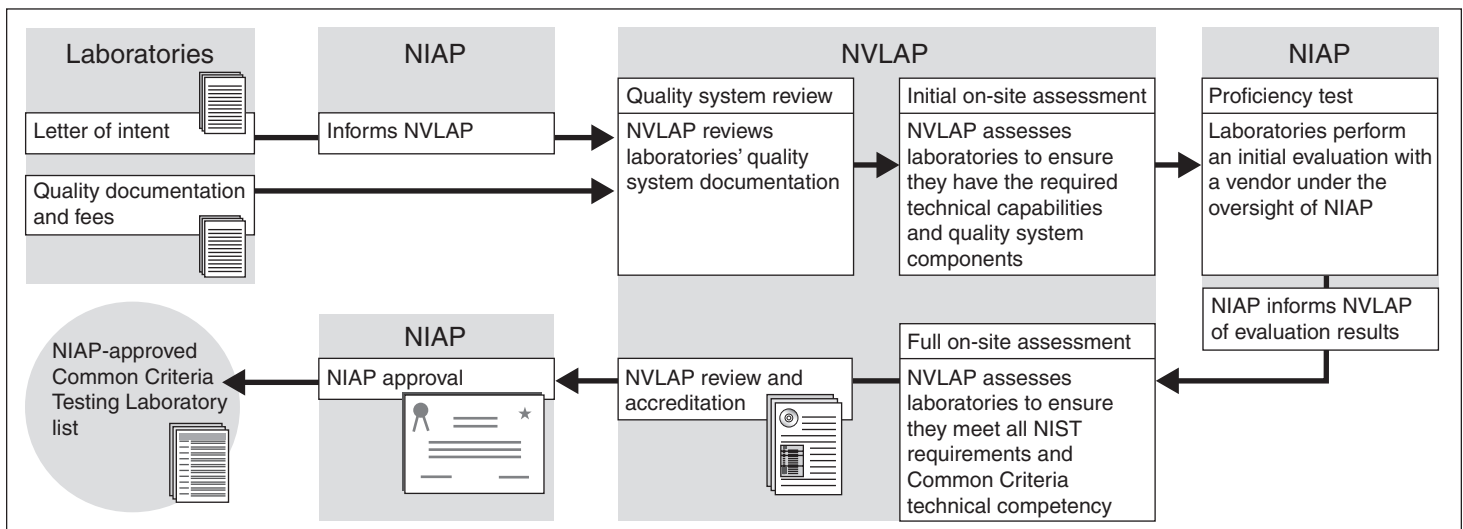
- 11 reported that the availability of evaluated products helped the agency make IT procurement decisions;
- 9 reported that the process provided their agency with thorough and accurate product documentation; and

²⁰Twenty-four agencies completed the survey: fifteen agencies identified benefits; three did not; the remaining six agencies did not purchase any NIAP-evaluated products.

- I reported that evaluated products provided a common method of performing a particular security service that is implemented in different types of security or security-enabled devices, potentially resulting in a greater degree of standardization of elements (such as audit entries).

Moreover, the NIST-administered National Voluntary Laboratory Accreditation Program (NVLAP) reviews laboratories annually to ensure competence and compliance with standards. Accreditation is granted to laboratories following their successful completion of a process that includes an application submission and fee payment by the laboratory, an on-site assessment, participation in proficiency testing, resolution of any deficiencies identified during the process, and a technical evaluation. The issuance of a certificate formally signifies that a laboratory has demonstrated that it meets all NVLAP requirements and operates in accordance with management and the technical requirements of the relevant standards. However, the accreditation does not imply any guarantee of laboratory performance or test and calibration data; it is solely a finding of laboratory competence and compliance with standards. Figure 3 shows the laboratory accreditation process.

Figure 3: Laboratory Accreditation Process



Source: GAO analysis of NIST Handbook 150-20.

NIAP Membership in International Recognition Arrangement Gives Agencies Broader Product Selection and Reduces Vendor Burden

Another benefit of the NIAP evaluation process is NIAP's membership in the Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security. As part of the goals of the arrangement, members can increase the availability of evaluated IT products and protection profiles for national use and eliminate duplicate evaluations of IT products and protection profiles, thus giving agencies a broader selection of evaluated products from which to choose. Agencies have the ability to acquire products that have been evaluated at evaluation assurance levels 1 through 4 from any of the countries that have an evaluation scheme. As of February 2006, there were 22 global signatories²¹ to the recognition arrangement, and 247 evaluated products available.

The recognition arrangement also reduces the burden on vendors by limiting the number of criteria to which their products must conform and the number of evaluations that a vendor needs to complete in order to sell a product internationally. Because NIAP evaluations (evaluation assurance levels 1-4) are accepted by the arrangement, vendors that go through the NIAP process can sell their evaluated products in any of the 22 member countries. Vendors are able to save time and money since they do not need to complete multiple evaluations to sell their product in different countries.

Product Evaluations Can Uncover Flaws and Cause Vendors to Fix Them

Another benefit of the NIAP process is that it uncovers flaws during product evaluations and can cause vendors to fix them. NIAP, vendor, and laboratory officials stated that the NIAP evaluation process has uncovered flaws and vulnerabilities in evaluated products. According to NIAP officials, software flaws are found in nearly all evaluated products, with an evaluation resulting in an average of two to three fixes. According to the four vendors included in our review, the NIAP evaluation process discovered flaws or vulnerabilities in their products or their product documentation. Also, officials from one of the laboratories included in our review stated that out of the 90 products they have evaluated, all of them had documentation flaws. Although vendors have the option of removing from the evaluation security features or functions in which flaws have been identified, any flaws in the remaining security features or functions must be

²¹The 22 countries include the certificate-authorizing countries—Australia, Canada, France, Germany, Japan, New Zealand, The Netherlands, United Kingdom, and the United States; and certificate-consuming countries—Austria, Czech Republic, Finland, Greece, Hungary, India, Israel, Italy, Norway, Republic of Singapore, Spain, Sweden and Turkey. Of the 22 signatories, 9 have evaluation schemes that authorize them to certify products in accordance with the arrangement. The remaining signatories do not have a scheme but have agreed to accept the certificates authorized by countries with schemes.

fixed in order to successfully complete the product evaluation. Nonetheless, agencies procuring NIAP-evaluated products have a higher level of assurance that the product's security features and functions will perform as claimed in the validation report.

Product Evaluations Can Result in Improvements to Vendors' Development Processes

Product evaluations can influence vendors to make improvements to their development processes that raise the overall quality of their current and future products. To complete a successful evaluation, vendors submit to laboratories their development documentation, which describes various processes related to security, such as software configuration controls. Officials at six of the seven vendors we visited stated that product evaluations had a positive influence on their development process. According to one of the six vendors, completed product evaluations that result in improvements to their development process would likely transfer to the development process of other products and help improve the overall quality of their products. Laboratory officials also stated that NIAP evaluations often result in vendors improving their software development process because vendors adopt some of the methodologies used to pass evaluation, such as test methods and documentation, for their own quality assurance processes. Additionally, we previously reported that vendors who are proactive and adopt effective development processes and practices can drastically reduce the number of flaws in their products.²²

NIAP Evaluation Process Faces Challenges

NIAP process participants—NIAP officials and selected vendors, laboratories, and federal agencies—identified challenges to acquiring and using NIAP-evaluated products.

- NIAP-evaluated products do not always meet agencies' needs, which limit agencies' acquisition and use of these products.
- A lack of vendor awareness of the NIAP evaluation process impacts the timely completion of the evaluation and validation of products.
- A reduction in the number of validators available to certify products could contribute to delays in validating products for agency use; and

²²GAO, *Information Security: Continued Action Needed to Improve Software Patch Management*, [GAO-04-706](#) (Washington, D.C.: June 2004).

-
- A lack of performance measures and difficulty in documenting the effectiveness of the NIAP process makes it difficult to demonstrate the program's usefulness or improvements made to products' security features and functions or improvements to vendors' development processes.

Collectively, these challenges hinder the effective use of the NIAP evaluation process by vendors and agencies.

NIAP-Evaluated Products Do Not Always Meet Agencies' Needs

Meeting agency needs for NIAP-evaluated products for use in national security systems can be a challenge. According to agency responses to our survey, 10 of 18 agencies²³ that purchased NIAP-evaluated products reported experiencing challenges in acquiring those products. Specifically,

- 10 agencies noted that products on the NIAP-evaluated product list were not the most current versions; and
- 7 agencies noted that products needed by their agency were not included on the NIAP-evaluated product list.

Agencies also reported additional challenges for acquiring NIAP--evaluated products. Specifically,

- choices for evaluated products are somewhat limited compared to the general product marketplace; and
- the length of time required for a product to complete the evaluation process can delay availability of the most up-to-date technology.

However, opportunities exist to better match agency needs with the availability of NIAP-evaluated products:

- Agencies can write protection profiles to define the exact security parameter specifications that they need. For example, two of the vendors we visited stated that they had their products evaluated against the Controlled Access Protection Profile, which provides agencies with a set of security functional and assurance requirements for their IT

²³Although 24 agencies completed the survey, 18 purchased NIAP-evaluated products; the remaining 6 agencies did not.

products and also provides a level of protection against threats of inadvertent or casual attempts to breach the system security.

- Vendors can enter the evaluation process before their products are publicly released, which can allow consumers to acquire the most up-to-date technology. One vendor we visited had taken such a proactive approach.
- Agencies can use the NIAP-validated products list to identify products that meet their needs. Because the number of available NIAP-evaluated products is increasing, agencies now have a variety of products from which to choose. In January 2002, there were about 20 evaluated products. As of February 2006, there were 127 evaluated products and 142 products in evaluation. These evaluated products span across 26 categories of information assurance products and information assurance-enabled products from which to choose, including operating systems and firewalls. As products continue to enter evaluation, agencies' needs may be better met.
- Vendors can, by participating in the NIAP Assurance Maintenance Program, maintain the validity of an evaluation when a product upgrades to its next version by either requesting a re-evaluation of the entire new product version or validation of only the changes in the product. Vendors' participation in this program may allow agencies to have the most recent products available to them.
- Agencies can increase their selection of products through the Common Criteria Recognition Arrangement—available on the Common Criteria portal Web site—which currently has 247 evaluated products available. The products listed on the Web site give agencies more choices of products evaluated at evaluation assurance levels 4 and below.

Lack of Vendors Awareness of NIAP Evaluation Process Affects Efficiency of Evaluations

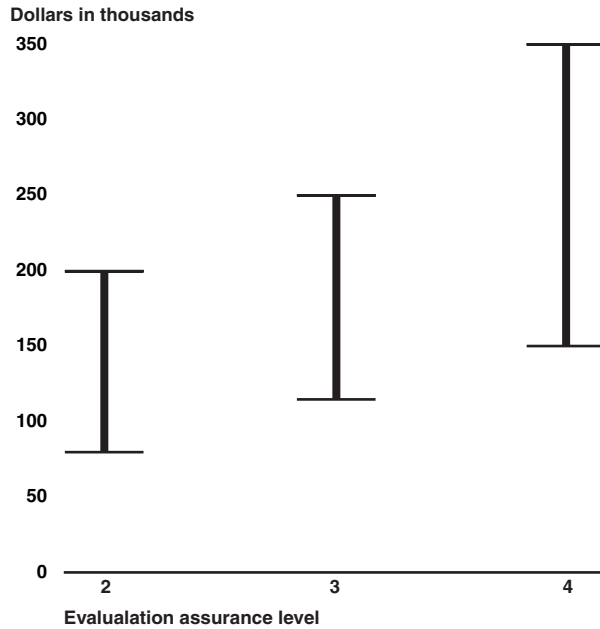
Another challenge faced by the NIAP process is the lack of vendor awareness regarding the requirements of the evaluation process. For example, vendors who are new to the evaluation process are not aware of the extensive documentation requirements. Creating documentation to meet evaluation requirements can be an expensive and time-consuming process. According to laboratory officials, about six months is the average time for vendors to complete the required documentation before test and evaluation can begin. However, if vendors consistently maintain their documentation, subsequent evaluations can be faster and less expensive

since the vendor has previously produced the documentation and is already familiar with the process.

Also, some vendors are not as active as others in the evaluation process, which can cause varying lengths of time for completing the evaluation. Vendors who are actively involved in the process are usually able to complete the process more quickly, including fixing flaws, than those who are not actively involved. According to one laboratory, the more active a vendor is in the evaluation process, the faster and less expensive it will be for the vendor. As such, the amount of involvement by the vendor during the process and the timeliness with which it fixes discovered flaws affects the length of time the product is in evaluation.

Furthermore, some vendors and laboratories do not have the same perception of the length of time required to perform the evaluation. According to laboratory officials, the length of time needed for conducting product evaluations varies depending on the type of product being evaluated and the evaluation assurance level (see fig. 4). Vendors are often not aware of these requirements and tend to underestimate the length of time required for evaluations.

Figure 4: Range of Time Required for Completing Product Evaluations at Various Evaluation Assurance Levels



Source: GAO analysis of data provided by laboratories.

Vendors and laboratories also perceive the length of evaluations differently because they punctuate start and end dates differently. Vendors measure the length of an evaluation from the day they decide to go into evaluation to the day they receive their product certificate. Their measurement includes selecting and negotiating with a laboratory, preparing required documentation, and testing the security features and functions. Laboratories, on the other hand, consider the length of an evaluation to be from the day they sign a contract with the vendor to the day they complete testing.

While Common Criteria user forums for program participants have been held, which NIAP participated in, NIAP itself has not developed education and training workshops that focus on educating participants on specific requirements—such as the documentation requirements. These workshops could help ensure that vendors and laboratories are aware of the NIAP process and could contribute to the efficiency of product evaluations. NIAP officials acknowledge that such educational offerings could be beneficial.

Reduction in the Number of
Validators May Affect Timeliness
of Certifications

Over the last year, NIAP has seen a reduction in the number of qualified validators. NIAP officials stated that one of the most significant challenges the NIAP process faces is hiring and maintaining qualified personnel to validate products. In fiscal year 2005, the NIAP program lost approximately four government validators and six contractor validators. According to the NIAP Director, maintaining qualified personnel to perform validation tasks is difficult largely because many validators are nearing retirement age and the job is not an attractive position for recent college graduates. Validators have a complex job with tasks that span the entire evaluation process; they incrementally review the results of the various tests of functional and assurance requirements as they are completed by the laboratory. As a result, once validators are hired, it typically takes 12 to 24 months to train new validators to become proficient in performing validation tasks.

If the NIAP program continues to see a reduction in validators, there could be an increased risk that a backlog of products needing to obtain NIAP certifications will develop, which could also impact the already lengthy evaluation process. The number of products entering evaluation is steadily increasing (in fiscal year 2002 there were approximately 20 products in evaluation and as of February 2006, there were 142 products in evaluation). Additionally, approximately five to seven products enter into evaluation each month. To address the widening gap between the number of products entering the process and the number of validators available to review products, NIAP intends to pursue legislation allowing it to recoup the costs of validations and hire additional staff.

Lack of Performance Measures
and Difficulty in Documenting
the Effectiveness of the NIAP
Process

A best practice in public and private organizations is the use of performance measurements to gain insight into—and make adjustments to—the effectiveness and efficiency of programs, processes, and people.²⁴ Performance measurement is a process of assessing progress toward achieving predetermined goals, and includes gathering information on the efficiency with which resources are transformed into goods and services, the quality of those outputs, and the effectiveness of government operations in terms of their specific contributions to program objectives. Establishing, updating, and collecting performance metrics to measure and track progress can assist organizations in determining whether they are fulfilling their vision and meeting their customer-focused strategic goals.

²⁴National Performance Review, *Serving the American Public: Best Practices in Performance Measurement*, June 1997, <http://govinfo.library.unt.edu/npr/library/papers/benchmrk/nprbook.html>.

The NIAP program lacks performance metrics to measure process effectiveness and thus faces difficulty in documenting its effectiveness. The program has not collected and analyzed data on the findings, flaws, and fixes resulting from product tests and evaluations. NIAP officials pointed out that nondisclosure agreements between laboratories and vendors make it difficult to collect and document such data. According to NIAP officials, there is existing laboratory information on findings, flaws, and fixes, but it has not been collected because of nondisclosure agreements. Nondisclosure agreements are important for protecting vendors' proprietary data from being released to the public and competitors. However, releasing summary laboratory information on findings, flaws and fixes, while at the same time considering the requirements of nondisclosure agreements, could be beneficial to determining the effectiveness of the NIAP program. Without this type of information, NIAP will have difficulty demonstrating its effectiveness and will be challenged to know and to demonstrate whether the process is meeting its goals.

Expanding NIAP Requirement to Non-national Security Systems May Yield Many of the Same Benefits and Challenges and Could Exacerbate Resource Constraints

While the National Security Telecommunications and Information Systems Security Policy Number 11 already allows agencies with non-national security systems to acquire NIAP-evaluated products, expanding the policy to mandate that such systems acquire NIAP-evaluated products may yield many of the same benefits and challenges experienced by current process participants, and could further exacerbate resources. For example, one identified benefit for national security systems—independent testing and evaluation of IT products—gives agencies confidence that validated features of a product, whether acquired for national or non-national security systems, will perform as claimed by the vendor. Similarly, one challenge—a reduction in the number of validators for certifying products—could contribute to delays in validating products, whether for national or non-nation security systems. Further, expanding the requirement to mandate the policy for non-national security systems may further exacerbate current resource constraints, related to hiring and maintaining qualified personnel to validate products.

Nevertheless, agencies with non-national security systems have in fact acquired NIAP-evaluated products. Specifically, ten of the federal agencies we surveyed indicated that they have used the NIAP process to acquire evaluated products for non-national security systems, even though they are not required to do so. One agency is considering the use of NIAP-evaluated products during its product reviews, and is also considering including NIAP-evaluated products as part of its procurement strategy.

Moreover, agencies seeking information assurance for their non-national security systems, but who do not acquire NIAP-evaluated products, have guidance and standards available to them. Specifically, as required by the Federal Information Security Management Act, NIST has developed and issued standards and guidelines, including minimum information security requirements, for the acquisition and use of security-related IT products for non-national security systems.²⁵ These standards and guidelines are to be complementary with those established for the protection of national security systems and information contained in such systems. Further, NIST issued additional guidance to agencies for incorporating security into all phases of the system development life cycle process²⁶ as a framework for selecting and acquiring cost-effective security controls. In August 2000, NIST also issued guidance on security assurance for non-national security systems in NIST Special Publication 800-23: *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*.

Conclusions

While a range of controls are needed to protect national security systems against increasingly sophisticated cyber attacks, establishing effective policies and processes for acquiring products that have been validated by an independent party is important to the federal government's ability to procure and deploy the right technologies. Acquiring NIAP-evaluated products can increase the federal government's confidence that its IT products and systems will perform security features and functions as claimed. Despite the benefits of acquiring and using IT products that have gone through the rigorous tests and evaluations of NIAP, the program faces considerable challenges that hinder its effective use by vendors and agencies. These challenges include the difficulty in matching agencies' needs with the availability of NIAP-evaluated products, vendors' lack of awareness regarding the evaluation process, a reduction in the number of validators to certify products, and difficulty in measuring and documenting the effectiveness of the NIAP process. Until these challenges are

²⁵In February 2005, NIST issued "*Recommended Security Controls for Federal Information Systems*" (Special Publication 800-53) to provide guidelines for selecting and specifying security controls for information systems categorized in accordance with FIPS Publication 199, "*Standards for Security Categorization of Federal Information and Information Systems*," issued in February 2004.

²⁶The phases of a system life cycle, as defined by NIST, are: initiation, development/acquisition, implementation, operation and maintenance, and disposition.

addressed, they will continue to undermine the efficacy of NIAP. Regarding expanding the NIAP requirement to non-national security systems, pursuing this approach may further exacerbate current resource constraints.

Recommendations for Executive Action

To assist the NIAP in documenting the effectiveness of the NIAP evaluation process, we recommend that the Secretary of Defense direct the Director of the National Security Agency, in coordination with NIST under the provisions of the NIAP partnership, to take the following two actions:

1. Coordinate with vendors, laboratories, and various industry associations that have knowledge of the evaluation process to develop awareness training workshops for program participants.
2. Consider collecting, analyzing, and reporting metrics on the effectiveness of NIAP tests and evaluations. Such metrics could include summary information on the number of findings, flaws, and associated fixes.

Agency Comments and Our Evaluation

In providing written comments on a draft of this report (reprinted in app. III), the Deputy Assistant Secretary of Defense (Deputy Chief Information Officer), partially agreed with one of our recommendations, agreed with the other, and described ongoing and planned efforts to address them. While the Deputy Assistant Secretary agreed with our recommendation to develop awareness training workshops for NIAP program participants, she stated that the NIAP must also live with the realities of the challenges that we identified in our report. The Deputy Assistant Secretary noted that, as our report highlights, the NIAP program is facing considerable challenges with resources and funding to sustain the current day-to-day running of the program and that it is not feasible for the NIAP office to increase its current efforts in developing and hosting the recommended training and education. Nonetheless, she also noted that the Secretary of Defense should direct the Director of the National Security Agency, in coordination with the NIST under the provisions of the NIAP, to coordinate with the vendors, laboratories, and various industry associations that have knowledge of the evaluation process to develop awareness training workshops for program participants within the current constraints and to work with the commercial laboratories, vendors, and others to identify ways that organizations outside of NIAP can further this initiative. We agree that

NIAP should continue its efforts in awareness and education training, and endorse increasing such efforts as resources permit.

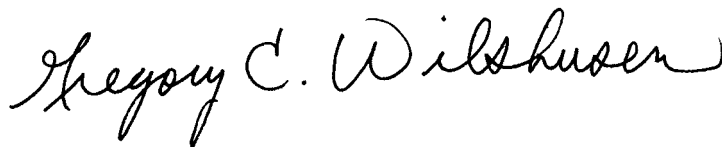
The Deputy Assistant Secretary agreed with our recommendation to collect, analyze, and report metrics on the effectiveness of NIAP tests and evaluations, and stated that the NIAP has already started researching ways to institute metrics to help determine the effectiveness of the evaluation program. She noted that the goal of collecting metrics is to demonstrate to the NIAP constituency that NIAP evaluations do provide value by improving the security of the evaluated products and by providing the end customer with assurance that these products perform their security functions as intended even when faced with adverse conditions.

The Department of Defense and the Department of Homeland Security also provided technical comments, which we considered and addressed in our report, as appropriate.

We are sending copies of this report to the Departments of Commerce (National Institute of Standards and Technology), Defense, and Homeland Security; the Office of Management and Budget; the General Services Administration, and to other interested parties. In addition, the report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.

Sincerely yours,



Gregory C. Wilshusen
Director, Information Security Issues

Objectives, Scope, and Methodology

Our objectives were to identify (1) the governmentwide benefits and challenges of the National Information Assurance Partnership (NIAP) evaluation process; and (2) the potential benefits and challenges of expanding the requirement of NIAP to non-national security systems, including sensitive but unclassified systems.

To determine the benefits and challenges for both objectives, we analyzed and reviewed a number of policy documents and reports from both industry and government. We also reviewed relevant federal policies relating to information security issues. To gain insight into the NIAP evaluation process, we met with software vendors and certification laboratories to discuss their experiences with NIAP, their applicable processes, and reviewed their relevant documentation. We selected vendors based on broad or distinguishing product capabilities demonstrating a range of features, brand recognition based on high ratings received in reviews conducted by information security magazines, and vendors mentioned more frequently in various discussions with industry experts and in information security literature. Vendors selected represented different information technology (IT) market sectors, are considered leaders in their field, and varied in size.

To determine the industrywide perspective on NIAP, we met with two IT industry groups: The Information Technology Association of America and Cyber Security Industry Alliance. We selected these industry groups because they represent a cross-section of the IT industry as a whole. To gain insight into the program's functions and usefulness to agencies, we spoke with government officials from the Department of Commerce (specifically the National Institute of Standards and Technology), Department of Defense, Department of Homeland Security, General Services Administration, and the Office of Management and Budget. We also surveyed officials from the 24 federal agencies designated under the Chief Financial Officers Act of 1990 to determine their current use of NIAP-evaluated products, the perceived usefulness of the program, and the benefits and challenges associated with acquiring and using NIAP-evaluated products.

For each agency survey, we identified the office of the chief information officer, notified them of our work, and distributed the survey instrument to each via an e-mail attachment. In addition, we discussed the purpose and content of the survey instrument with agency officials when requested. All 24 agencies responded to our survey. We did not verify the accuracy of the agencies' responses; however, we reviewed supporting documentation that

agencies provided to validate their responses. We contacted agency officials when necessary for follow-up information. We then analyzed the agencies' responses.

Although this was not a sample survey, and, therefore, there were no sampling errors, conducting any survey may introduce other kinds of errors. For example, difficulties in how a particular question is interpreted, in the sources of information that are available to respondents, or in how the data are entered into a database (or were analyzed) can introduce unwanted variability into the survey results.

We took steps in the development of the survey instrument, the data collection, and the data analysis to minimize these survey-related errors. For example, we developed the questionnaire in two stages. First, we had a survey specialist design the survey instrument in collaboration with subject-matter experts. Then, we pretested the instrument at two federal departments and internally at GAO to ensure that questions were relevant, clearly stated, and easy to answer.

We conducted our work in Washington, D.C., from May 2005 through February 2006, in accordance with generally accepted government auditing standards.

Common Criteria Evaluation Assurance Levels

Table 1: Summary of the Common Criteria Evaluation Assurance Levels

Evaluation assurance level	What is tested	Description
1	Functionality	Evaluation provides independent testing against a specification and an examination of the guidance documentation. Used when confidence in correct operation is required but the threats to security are not viewed as serious.
2	Structure	Evaluation provides a low to moderate level of independently assured security as required by vendors or users.
3	Methodology	Evaluation provides an analysis supported by testing, selective independent confirmation of the vendor test results, and evidence of a vendor search for obvious vulnerabilities.
4	Methodology and Design	Evaluation provides a moderate to high level of independently assured security in conventional commodity products. Testing is supported by an independent search for obvious vulnerabilities.
5	Semiformal Design	Evaluation provides a high level of independently assured security in a planned development, with a rigorous development approach. The search for vulnerabilities must ensure resistance to penetration attackers with a moderate attack potential.
6	Semiformal Verified Design	Used for the development of specialized security products, for application in high risk situations. The independent search for vulnerabilities must ensure resistance to penetration attackers with a high attack potential.
7	Formal Design	Used in the development of security products for application in extremely high risk situations. Evidence of vendor testing and complete independent confirmation of vendor test results are required.

Source: GAO analysis of Common Criteria data.

Comments from the Department of Defense



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

March 21, 2006

CHIEF INFORMATION OFFICER

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Wilshusen:

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-06-392, "INFORMATION ASSURANCE: National Partnership Offers Benefits, but Faces Considerable Challenges," dated March 10, 2006, GAO Code 310551. The DoD has reviewed the report and concurs with the findings, partially concurs with Recommendation 1, and concurs with Recommendation 2.

Enclosure 1 contains the DoD response and rationale for the report's two recommendations to the Secretary of Defense. Enclosure 2 contains general administrative comments offered by the DoD reviewers of the draft report.

Sincerely,

for Priscilla E. Guthrie
Priscilla E. Guthrie
Deputy Assistant Secretary of Defense
(Deputy CIO)

Enclosure:
as



GAO DRAFT REPORT DATED MARCH 10, 2006
GAO-06-392 (GAO CODES 310551)

"INFORMATION ASSURANCE: NATIONAL PARTNERSHIP
OFFERS BENEFITS, BUT FACES CONSIDERABLE
CHALLENGES"

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The GAO recommended that the Secretary of Defense direct the Director of the National Security Agency, in coordination with the National Institute of Standards and Technology under the provisions of the National Information Assurance Partnership (NIAP) to coordinate with the vendors, laboratories, and various industry associations that have knowledge of the evaluation process to develop awareness training workshops for program participants. (p. 29/GAO Draft Report)

DOD RESPONSE: Partial Concur

While DoD agrees with the recommendation to promote awareness training and understanding of the NIAP CCEVS, we also must live with the realities of the challenges identified in the GAO report. NIAP has and will continue to work with vendors, labs and industry associations to provide awareness training and education. Over the past year, the NIAP has provided briefings at a wide variety of for a, such as the Federal Information Assurance Conference, the DoD Identity Management Conference, the Cross Domain Solutions Workshop, and the Annual Computer Security Applications Conference. The NIAP has also been working closely with the Common Criteria User's Forum and the newly established Common Criteria Vendor's Forum on education and awareness efforts. Unfortunately, as the report highlights, the NIAP program is facing considerable challenges with resources and funding to sustain the current day-to-day running of the program. When coupled with the significant loss of support for the NIAP from NIST due to higher priorities within NIST, and increasing pressures on DoD resources to support current military operations supporting the Global War On Terrorism, it is not feasible for the NIAP office to increase its current efforts in developing and hosting the recommended awareness training and education. The Secretary of Defense should direct the Director of the National Security Agency, in coordination with the NIST, under the provisions of the NIAP, to coordinate with the vendors, laboratories, and various industry associations that have knowledge of the evaluation process to develop awareness training workshops for program participants within the current constraints and to work with the commercial labs, vendors, and others to identify ways that organizations outside of NIAP can further this initiative.

Enclosure 1

1

RECOMMENDATION 2: The GAO recommended that the Secretary of Defense direct the Director of the National Security Agency, in coordination with the National Institute of Standards and Technology under the provisions of the NIAP to consider collecting, analyzing, and reporting metrics on the effectiveness of NIAP tests and evaluations; such metrics could include summary information on the number of findings, flaws, and associated fixes. (p. 29/GAO Draft Report)

DOD RESPONSE: Concur.

NIAP CCEVS has already started researching ways to institute metrics to help determine the effectiveness of the evaluation program. NIAP CCEVS has already begun collecting metrics on the effectiveness of NIAP testing. In CY 2004 and 2005, most of the metrics collected were based on informal queries to the NIAP labs and were gathered to provide some general statistics during NIAP presentations. Since that time, based on requests from the Committee for National Security Systems, NIAP CCEVS has begun collecting additional general metrics and anecdotes from their commercial labs on how evaluations have improved vendor products. NIAP CCEVS has also begun collecting specific detailed metrics through their NIAP Monthly Status Reports, which are required for each evaluation in progress. In addition, NIAP CCEVS is developing a template for a comprehensive end-of-evaluation report which will detail all changes or improvements made to the product or the vendor's processes during the evaluation process. This will include fixes to critical user documentation, improvements to vendor processes, and changes to the product itself. The goal of collecting these metrics is to demonstrate to the NIAP constituency that NIAP evaluations provide value by improving the security of the evaluated products and by providing the end customer with assurance that these products perform their security functions as intended, even when faced with adverse conditions.

Enclosure 1

2

GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, Director, Information Security Issues, (202) 512-6244

Staff Acknowledgments

In addition to the individual named above, Jenniffer Wilson (Assistant Director), Neil Doherty, Jennifer Franks, Joel Grossman, Matthew Grote, Min Hyun, Anjalique Lawrence, J. Paul Nicholas, Karen Talley, and Amos Tevelow were key contributors to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548