United States General Accounting Office

GAO

Report to the Committee on Armed Services, U.S. Senate

March 2004

DEFENSE ACQUISITIONS

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

GAO-04-302

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.

Contents

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

March 31, 2004

The Honorable John W. Warner
Chairman
The Honorable Carl Levin
Ranking Minority Member
Committee on Armed Services
United States Senate

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 can be exposed to the risk of compromise when they are exported, stolen, lost during combat, or damaged during routine missions. When U.S. technologies are compromised, it 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 the international marketplace.

In an effort to protect U.S. technologies from exploitation, the Under Secretary of Defense for Acquisition, Technology, and Logistics[1] in 1999 directed each military service to implement anti-tamper techniques.[2] Program managers are responsible for applying the techniques on individual weapon systems. The Senate report accompanying the National Defense Authorization Act for Fiscal Year 2004[3] required us to review the Department of Defense's (DOD) implementation of the anti-tamper policy. We conducted our work between February 2003 and August 2003 in accordance with generally accepted government auditing standards.

Results in Brief

Program managers have encountered difficulties in implementing DOD's anti-tamper policy. First, defining a critical technology—a basis for determining the need for anti-tamper protection—is subjective, which can result in different conclusions regarding what needs protection. While different organizations can check on program managers' critical

[1]Formerly this position was referred to as the Under Secretary of Defense for Acquisition and Technology.

[2]Anti-tamper techniques are applied through a systems engineering activity. Examples of techniques include software encryption and hardware protective coatings.

[3]S. Rept. No. 108-46, at 345 (May 13, 2003).

technology 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 for those programs that are further along in the acquisition process. Programs we contacted experienced or estimated a cost increase, 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 the 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. 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 unique techniques needed for their individual systems.

We make five recommendations to DOD to better oversee and assist program managers in implementing anti-tamper protection on weapon systems. In written comments on a draft of this report, DOD partially concurred with one recommendation and offered an alternative solution, which we did not incorporate because it did not fully address the problem. DOD concurred with our remaining four recommendations and provided alternative language for two, which we incorporated as appropriate.

Background

DOD increasingly relies on advanced technology in its weapons for effectiveness on the battlefield and actively seeks to include foreign partners in weapon system development and acquisition. DOD's policy also encourages the sale of certain weapons to foreign governments through the Foreign Military Sales Program and direct commercial sales made by companies. While these efforts have the potential to enhance coalition operations and reduce weapons' unit costs, DOD has acknowledged that the efforts also risk making U.S. technologies potentially vulnerable to exploitation. DOD reported that an increasing number of countries have reverse engineering capability and actively seek to obtain U.S. technology through various means.

As a method to protect critical technologies, the Under Secretary of Defense for Acquisition, Technology, and Logistics directed the military services in 1999 to implement anti-tamper techniques. While the

techniques will not prevent exploitation, they are intended to delay or discourage attempts to reverse engineer critical technologies in a weapon system or develop countermeasures to a system or subsystem.

In 2001, the Under Secretary of Defense for Acquisition, Technology, and Logistics designated the Air Force as the Executive Agent responsible for implementing DOD's anti-tamper policy. The Executive Agent oversees an annual budget of about $8 million per year to implement policy and manage anti-tamper technology projects through the Air Force Research Laboratory. DOD, in conjunction with the Air Force Research Laboratory and the Department of Energy's Sandia National Laboratories, also holds periodic information sessions to educate the acquisition community about anti-tamper policy, guidance, and technology developments. In addition, military services and defense agencies, such as the Missile Defense Agency, have an anti-tamper focal point to coordinate activities.

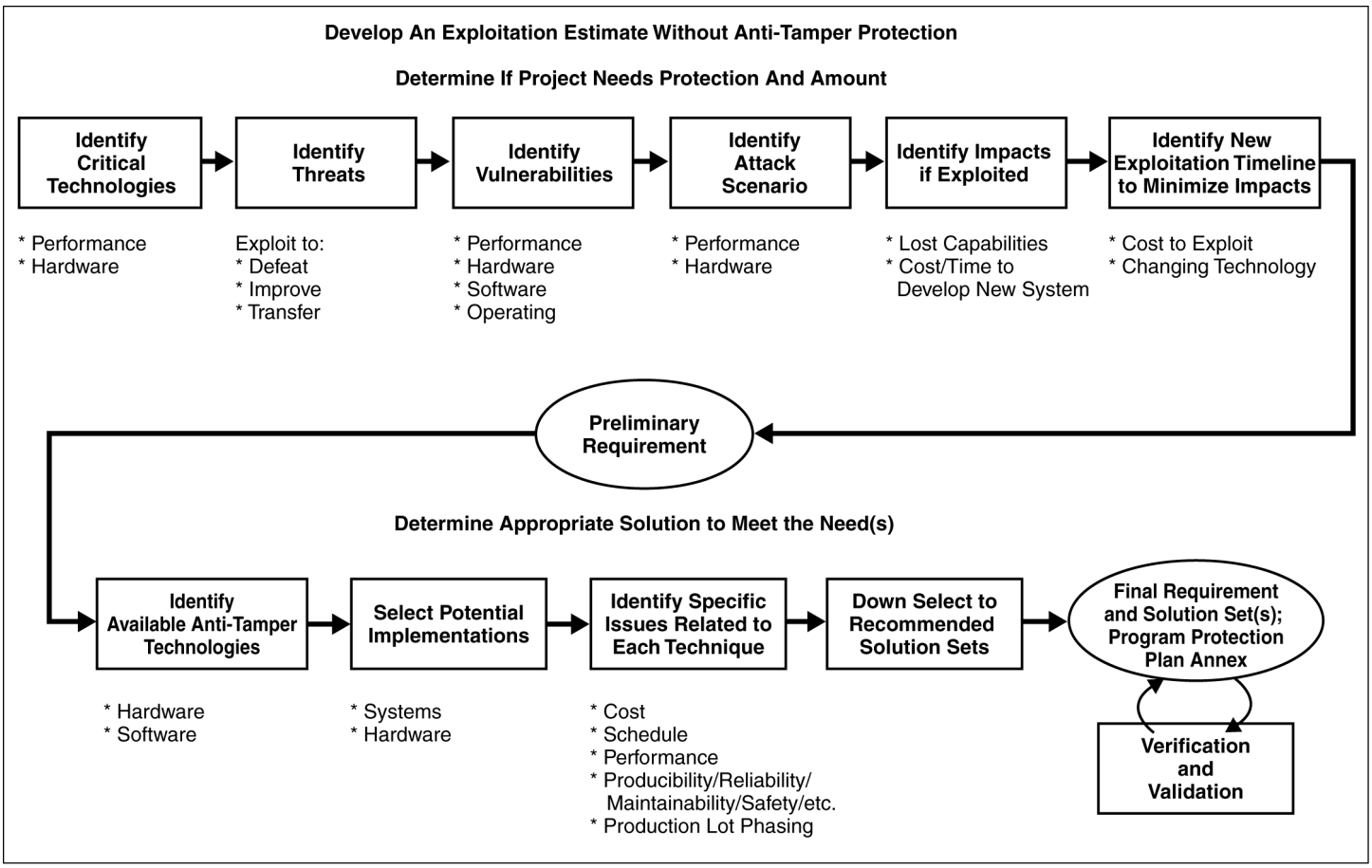
Program managers are responsible for considering anti-tamper measures on any weapon system with critical technologies.[4] Since it is not feasible to protect every technology, program managers are to conduct an assessment to determine if anti-tamper protection is needed. The first step of the decision process is to determine if the system has critical technologies. If program managers determine the system has no critical technologies, they are to document that decision according to draft guidance.[5] Program managers of systems that contain critical technologies complete the remaining steps of the process. Based on draft guidance, program managers are to conceptually address how they will implement anti-tamper measures at system development, otherwise known as milestone B. DOD's anti-tamper decision process is illustrated in figure 1.[6]

[4]According to the implementation guidelines of 2000, anti-tamper measures should be included in requirements development for all new and upgraded programs and be considered for systems that are developed with allied partners or exported. Anti-tamper protection is not required for programs beyond the design phase or those in full production, unless the responsible decision authority determines otherwise.

[5]Mandatory Procedures for Research and Technology Protection within the DOD (5200.39-R), draft, March 2002.

[6]Variations of DOD's anti-tamper decision process can be found in different DOD documents.

Figure 1: DOD Anti-Tamper Decision Process



Source: DOD's Program Managers Anti-Tamper Handbook.

Program managers can obtain assistance on their assessments from government laboratories, contractors, and the intelligence community. They are required to document the decision to use or not to use anti-tamper techniques in a classified annex of the program protection plan,[7]

[7]The program protection plan documents the program's approach for protecting critical program information and should include a prioritized list of critical information and an assessment of the threats and vulnerabilities to that information.

which is subject to approval from the program's milestone decision authority.[8]

Anti-tamper techniques vary depending on the type of protection the system requires.[9] An example of an anti-tamper technique is software encryption, which scrambles software instructions to make them unintelligible without first being reprocessed through a deciphering technique. Another example is a thin opaque coating placed on microelectronic components, which makes it difficult to extract or dissect the components without great damage. Programs can apply multiple anti-tamper techniques to a critical technology. For example, a program could encrypt critical data on a microelectronic chip that is also covered with a protective coating. Each layer of protection could act as an obstacle to reverse engineering.

Anti-Tamper Implementation Has Been Hampered by Several Factors, and Support to Address Them Has Been Limited

Implementation of the anti-tamper policy has been hampered by several factors. First, identification of critical technology is subject to interpretation and program managers and DOD officials can and have arrived at different conclusions about what needs to be protected. Second, applying anti-tamper protection can take time and money, which may compete with a program manager's cost and schedule objectives. Finally, some programs found it difficult to apply anti-tamper techniques when the techniques were not fully developed, and others were unsure which techniques were available to them. In general, the later anti-tamper techniques are applied, the more difficult and costly it can be to implement. Thus far, support to help program managers address some of these factors has been limited.

Different Interpretations of Critical Technologies May Increase the Risk of Some Going Unprotected

DOD officials acknowledged that the identification of critical technologies—a basis for determining if anti-tamper protection is needed—is subjective, which can result in different conclusions regarding what needs protection. DOD's Program Managers Anti-Tamper Handbook defines technology as critical if compromise results in degrading combat

[8]The milestone decision authority is the individual designated to approve entry of an acquisition program to the next phase.

[9]Information regarding the specific anti-tamper techniques used on an individual system is typically classified because disclosure could aid exploitation. In some cases, anti-tamper information is restricted at the special access level.

effectiveness, shortening the expected combat life of the system, or significantly altering program direction. While a broad definition allows for flexibility to determine what is critical on individual systems, it may increase the risk that the same technology is protected on some systems but not on others or that different conclusions can be reached on whether programs have critical technologies. For example:

- An official from an intelligence agency described a case where two services used the same critical technology, but only one identified the technology as critical and provided protection. The intelligence agency official speculated that if exploited, knowledge gained from the unprotected system could have exposed the technology on both systems to compromise. While both systems were ultimately protected, the intelligence agency official stated that the situation could occur again.

- Officials from the Executive Committee[10] told us that two program managers stated that their systems had no critical technologies and therefore were not subject to the anti-tamper policy. Both managers were directed by the Executive Committee to reconsider their determination and apply anti-tamper protection. As a result, one program is in the process of determining which technologies are critical, and the other program is applying anti-tamper protection as a condition to export the system.

While different conclusions can be reached regarding what is critical, various organizations can serve as a check on a program manager's assessment. However, no organization has complete information or visibility of all programs across the services and agencies. For example, the anti-tamper Executive Agent and the military service focal points do not have full knowledge about which program offices have or have not identified critical technologies or applied anti-tamper protection.[11] In 2001, DOD attempted to collect such information,[12] but not all programs

[10] The Low Observable/Counter Low Observable Executive Committee establishes security guidelines to protect stealth technology and ensures exports are consistent with DOD policy.

[11]The Counterintelligence Field Activity and the Defense Intelligence Agency are developing a database that will contain information regarding critical program information for programs across the services.

[12]This effort was in response to the Under Secretary of Defense's direction in 1999 that the acquisition executives determine the extent to which anti-tamper protection was incorporated in weapon systems.

provided data and DOD did not corroborate what was provided to ensure that program officials were consistently assessing critical technologies. The Executive Agent stated that there are no plans to update this data. Conducting oversight over program managers' assessments may be difficult because of limited resources. Specifically, the Executive Agent has two full-time staff and the military service focal points perform duties other than anti-tamper management. Furthermore, according to a military official, program offices that determine they have no critical technologies are not required to obtain the focal points' concurrence. While other organizations can review a program manager's critical technology assessment as part of various acquisition and export processes, they may not have a full perspective of the assessments made by all programs across the services and the agencies. For example, different milestone decision authorities only review an individual program manager's critical technology decisions for programs coming under their responsibility. Also, the Executive Committee may weigh in on the determinations, but it only reviews exports involving stealth technology.

While it was apparent that the systems had critical technologies, some program managers needed assistance to determine which specific technologies were critical. For example, a program office tasked the contractor to identify critical technologies, and it has worked for months with the contractor to agree upon and finalize a list of critical technologies on the system. Also, an intelligence official, who is available to assist program managers in assessing their systems' criticality, found that some program managers identified too many technologies as critical and that others did not identify all of the systems' critical elements. In one instance, a program manager indicated that a system had 400 critical technologies, but an intelligence agency narrowed down the list to about 50 that it considered critical. In another case, a program manager concluded that an entire system was one critical technology, but the intelligence agency recommended that the system's technologies be broken down and identified approximately 15 as critical.

Although there are various resources to help program managers identify critical technologies, they may have limited utility, or may not be known, and therefore not requested. For example, the Militarily Critical Technologies List—cited in guidance as a primary reference for program managers—may not be up to date and may not include all technologies, according to some DOD officials. Another resource—the Program

Managers Anti-Tamper Handbook—contains information regarding critical technology determinations, but program managers are not always aware that the handbook exists, in part because it is not widely distributed.[13] In addition, the Defense Intelligence Agency can conduct an independent assessment of a system's critical elements and technologies, if requested by the program manager. However, many officials we interviewed were unaware that the agency provides this assistance. According to a military official, the focal points are available to review a program manager's assessment if requested.

In some instances, program managers may have differing perceptions of what constitutes a critical technology. According to DOD's guidance, critical technologies can be either classified or unclassified. However, an anti-tamper focal point stated that there is a perception that the anti-tamper policy only applies to classified programs. We found in one instance that the manager for a weapon program stated that the program did not require anti-tamper protection because it had no critical technologies that were classified.[14]

Applying Anti-Tamper Protection Can Affect Cost and Schedule Objectives

Applying anti-tamper protection takes money and time, which can affect a program manager's cost and schedule objectives. Generally, anti-tamper implementation is treated as an added requirement that is not separately funded for most programs.[15] Program officials acknowledged that anti-tamper costs can be difficult to estimate and isolate because they are intertwined with other costs, such as research and development or production costs. As we have found in prior work, the later a requirement is identified, the more costly it is to achieve.[16]

[13]According to DOD officials, the handbook contains classified information and they need to verify that a program office can accept and store classified information before they distribute it.

[14]This program office estimated that 30 systems had been lost during military operations. In addition, DOD reported that this technology has been targeted for reverse engineering.

[15]One program we contacted was authorized separate congressional funding for anti-tamper costs.

[16]*Best Practices: Setting Requirements Differently Could Reduce Weapon Systems' Total Ownership Costs*, GAO-03-57 (Washington, D.C.: Feb. 11, 2003).

Most programs we visited experienced or estimated cost increases, and some encountered schedule delays as they attempted to apply anti-tamper techniques. For example:

- A program official told us the anti-tamper protection for a program upgrade increased both design and production costs for the receiver unit. The program official stated that the anti-tamper protection increased total unit cost by an estimated $31 million, or 10 percent. Program officials expressed concern that unit cost increases may affect procurement decisions, particularly for one service, which is the largest acquirer of units and may be unable to purchase the proposed number.

- A program office estimated that it needs a budget increase of $56 million, or 10 percent, to fund the desired anti-tamper protections. Officials from that program told us that the existing program budget was inadequate to fund the added anti-tamper requirements. As a result, the program manager requested, and is waiting for, separate funding before attempting to apply anti-tamper protection to the system.

- One program office awarded a contract modification for the design, implementation, and testing of anti-tamper techniques valued at $12.5 million. Initially, the contractor had estimated the anti-tamper costs to be $35 million, but the program office did not approve all techniques suggested by the contractor. In addition, the contractor estimated that the recurring unit price for anti-tamper protection on future production lots may be $3,372 per unit. The U.S. government and the contractor have not completed unit price negotiations. Program officials told us that anti-tamper implementation contributed to a 6-month schedule delay.

- Another program office estimated that $87 million is needed to protect two critical technologies with multiple anti-tamper techniques. The program office expects that half of the anti-tamper budget will be used to test the techniques. The anti-tamper protection will only be applied if the system is approved for export. At that time, program officials will reexamine the anti-tamper cost estimates. In addition, it may take 5 years to adequately apply the techniques.

- Officials from an international program stated that, thus far, they have experienced a 60-day schedule delay while they wait for the contractor to estimate the system's anti-tamper cost. Program officials stated that the potential for increased costs and additional schedule delays is high.

Program officials and representatives from the Executive Committee stated that the cost of anti-tamper protection can be significantly higher for an international program for various reasons, including that the U.S. version and the international version of the system may require different anti-tamper techniques.

Cost and schedule impacts may also be more significant if the programs are further along in the acquisition process when program offices first attempt to apply anti-tamper protection. Several programs that have experienced significant cost increases or delays were in or beyond the program development phase when they attempted to apply anti-tamper techniques. For example, when the anti-tamper policy was issued, one program had just obtained approval to begin system development and program officials believed it was too late to implement anti-tamper protection. As a result, the program received an interim waiver[17] of the anti-tamper policy, and it only plans to apply anti-tamper techniques if the system is approved for export. While DOD has not systematically collected cost data for anti-tamper application across programs, DOD officials have stated that it is more cost-effective for programs to consider anti-tamper requirements at program inception, rather than later in the acquisition process. An official from a program that applied anti-tamper techniques in the production phase stated that ideally a program should identify its anti-tamper needs, including cost and technology, as early as possible. Recent Army anti-tamper guidance indicates that programs should receive approval for their preliminary anti-tamper plans at the concept stage.

Needs Outpace Availability of Techniques and Tools

Anti-tamper techniques can be technically difficult to incorporate on a weapon system, such as when the technology is immature. DOD is working to oversee the development of generic anti-tamper techniques and tools to help program managers identify potential techniques, but many of these efforts are still in progress and it is uncertain how they will help program managers. While program managers want knowledge about generic techniques, they ultimately have to design and incorporate techniques needed for their unique systems to ensure protection of critical technologies and to meet performance objectives.

[17]According to representatives from the Executive Committee, DOD can waive the anti-tamper requirement when a program can make a compelling reason for forgoing the policy.

Problems in applying anti-tamper techniques typically arose when the programs were already in design or production or when the techniques were not fully developed or specifically designed for the system. For example:

- Officials from a program told us that they experienced problems when applying an anti-tamper protective coating. Because the team applying the coating did not coordinate with teams working on other aspects of the system, the problems with the coating were not discovered until just before production. Prior to an initial development test, the program office received a temporary waiver to test the system without the anti-tamper technique because the coating caused malfunctioning. The program office and its contractor are working to resolve issues with the anti-tamper technique.

- A program office was not able to copy anti-tamper techniques used by a similar program and, therefore, attempted to apply a generically developed anti-tamper coating, which resulted in problems. Specifically, the coating caused the system to malfunction, so the program office requested assistance from a national laboratory, but the laboratory's solution melted key components of the system. Therefore, the program office requested that the contractor develop a new coating and other methods of protection for the system. The contractor's anti-tamper techniques were successfully applied to the system.

- One program required advanced anti-tamper techniques to protect miniaturized internal components, but the technology was still in development and not available for immediate application. According to program officials, research and development of the anti-tamper technique was originally expected to be completed in 2002 and is now estimated to be available in 2006. Currently, officials are uncertain that the technique will meet their needs because the technique is being generically developed. In the absence of being able to apply the anti-tamper technique, the program received approval from DOD to use procedural protections, whereby U.S. military personnel provide physical security of the system when it is used in foreign countries, which includes locking the unit in a protected room to restrict access by foreign nationals. DOD officials stated that physical security can be less reliable than actual anti-tamper protection.

Some program managers told us that they need more help in deciding what anti-tamper techniques they should apply to their individual systems. To provide information, DOD has a classified database that describes current anti-tamper techniques. An Air Force Research Laboratory official

stated that they are in the process of updating this database, developing a rating system on the value of various techniques to be included in the database, and creating a classified technology road map that will prioritize the needs for various anti-tamper techniques. These tools are currently unavailable.[18] DOD and Sandia National Laboratories also have provided information on anti-tamper techniques and tools to program managers at periodic workshops where attendance is voluntary.

To further assist program managers, DOD is in the process of overseeing the development of generic anti-tamper techniques, but it is uncertain to what extent such techniques address a program's specific needs. In 2001, DOD issued several contracts to encourage anti-tamper technology development. To date, several defense contractors have provided anti-tamper technology concepts, but according to the Executive Agent, programs need to further develop the technology before it can be applied to and function on a particular system. According to Air Force Research Laboratory and Sandia National Laboratories officials, generic anti-tamper techniques can be considered, but program managers have to design and incorporate the techniques needed for their unique systems. Program managers ultimately have to ensure that the techniques protect critical technologies and do not adversely affect performance objectives for the system.

Conclusions

Anti-tamper protection is one of the key ways DOD can preserve U.S. investment in critical technologies, while operating in an environment of coalition warfare and a globalized defense industry. However, implementation of the anti-tamper policy, thus far, has been difficult—in part because DOD has not developed an implementation strategy to ensure success. For program managers expected to implement anti-tamper protection, the policy can compete with their goals of meeting cost and schedule objectives, particularly when the anti-tamper requirement is identified late in the system development process. Without providing more oversight and guidance about what needs to be protected and how to do so, DOD is at risk of program managers making decisions on individual programs that can result in unprotected technologies and have negative consequences for maintaining the military's overall technological advantage.

[18]According to a laboratory official, an initial prototype of an updated database is estimated to be available in 2004.

Recommendations for Executive Action

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

To better oversee identification of critical technologies for all programs subject to the anti-tamper policy, we recommend that the Secretary of Defense direct the Under Secretary for Acquisition, Technology, and Logistics, in coordination with the Executive Agent and the focal points, to (1) collect from program managers information they are to develop on critical technology identification and (2) appoint appropriate technical experts to centrally review the technologies identified for consistency across programs and services.

To better support program managers in the identification of critical technologies, the Secretary of Defense should direct the Under Secretary for Acquisition, Technology, and Logistics, in coordination with the Executive Agent and the focal points, to (1) continue to identify available anti-tamper technical resources, (2) issue updated policy identifying roles and responsibilities of the technical support organizations, and (3) work with training organizations to ensure training includes practical information on how to identify critical technologies.

To help minimize the impact to program cost and schedule objectives, the Secretary of Defense should direct the Under Secretary for Acquisition, Technology, and Logistics to work with program managers to ensure that the cost and techniques needed to implement anti-tamper protection are identified early in a system's life cycle and to reflect that practice in guidance and decisions.

To maximize the return on investment of DOD's anti-tamper technology efforts, the Secretary of Defense should direct the Executive Agent to monitor the value of developing generic anti-tamper techniques and evaluate the effectiveness of the tools, once deployed, in assisting program managers to identify and apply techniques on individual programs.

To ensure successful implementation of the anti-tamper policy, the Secretary of Defense should direct the Under Secretary for Acquisition, Technology, and Logistics to develop a business case that determines whether the current organizational structure and resources are adequate to implement anti-tamper protection and if not, what other actions are needed to mitigate the risk of compromise of critical technologies.

Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD partially concurred with one recommendation and offered an alternative solution, which we did not incorporate. DOD concurred with our remaining four recommendations and provided alternative language for two, which we incorporated as appropriate. DOD's letter is reprinted in the appendix.

DOD partially concurred with our recommendation to collect and centrally review the program's critical technology identifications and proposed, instead, that it develop a standardized process to minimize subjectivity, incorporate that process into anti-tamper policy, and monitor subsequent implementation. As part of its rationale, DOD stated that technical representatives in the services currently work with program managers to implement the anti-tamper policy and that quarterly conferences and seminars are ways to disseminate important information to program managers. We believe DOD's proposal is an improvement over the current process given that program managers need more technical support and guidance to identify critical technologies. However, we do not believe DOD's proposal is sufficient because a central review mechanism is needed to ensure consistent critical technology identification across the services and the agencies. Without central visibility over program managers' critical technology identifications, the risk exists that the same technology is protected on some systems but not on others. Knowledge gained from unprotected systems can expose critical technology to compromise, which minimizes the impact of anti-tamper protection. In addition, DOD's dissemination of information at conferences may be limited because conference attendance is voluntary and all program managers may not attend and receive the information. Given the need for consistency and a central review, we did not revise our recommendation.

DOD concurred with our remaining recommendations, but offered alternative language for two, which we incorporated. Specifically, for our recommendation aimed at better supporting program managers in identifying critical technologies, DOD proposed adding language that underscored the need for identifying technical resources and maintaining up-to-date policies on technical support organizations' roles and responsibilities. While DOD has identified some resources and listed them in several documents, it has not developed a comprehensive list of resources to assist program managers. Therefore, we added to our recommendation that DOD continue to identify available anti-tamper technical resources. For our recommendation that DOD evaluate generic anti-tamper techniques, DOD proposed language that offered greater flexibility, which seemed reasonable and we incorporated.

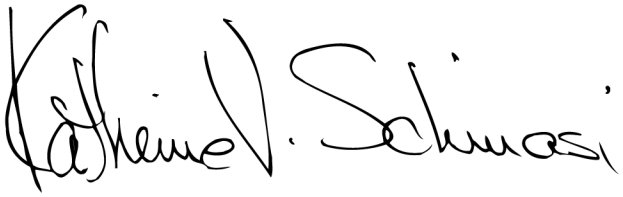
Scope and Methodology

To determine how DOD implemented the anti-tamper policy, we collected data and interviewed officials from 17 programs, which were identified by DOD as having experience with implementing the policy or by us through our review. Twelve of the 17 programs reported that their systems had critical technologies, and most were in various stages of implementing the anti-tamper policy. From those programs we selected six for an in-depth review. We conducted structured interviews with the six programs that had identified critical technologies on their systems to understand their experiences with applying anti-tamper techniques. We selected systems that represented a cross-section of acquisition programs and various types of systems in different phases of development. To the extent possible, when selecting the programs for an in-depth review, we considered factors that may increase a system's vulnerability and exposure to exploitation. We also considered whether the system was approved for export by examining the Defense Security Cooperation Agency's data on foreign military sales. In addition, we analyzed available program information from the anti-tamper Executive Agent and the military focal points to determine programs reporting critical technologies and anti-tamper plans. DOD acknowledged that the information was incomplete, and we did not independently verify the reliability of the data.

We supplemented the program information by interviewing the Executive Agent, the military focal points, representatives from the intelligence community, DOD's Executive Committee, the Department of Energy's Sandia National Laboratories, the Air Force Research Laboratory, defense contractors, and an electronic security specialist. We also discussed DOD's anti-tamper policy with current and former officials from the Office of the Secretary of Defense. To observe DOD's training of program managers, we attended a DOD anti-tamper information workshop and a quarterly review. We analyzed pertinent DOD policies, directives, instructions, and guidance governing anti-tamper protection on systems. We also conducted a literature search to obtain information on program protection and industry practices related to anti-tamper measures.

We are sending copies of this report to interested congressional committees; the Secretary of Defense; and the Director, Office of Management and Budget. We will make copies available to others upon request. In addition, this 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 concerning this report, please call me at (202) 512-4841. Others making key contributions to this report were Anne-Marie Lasowski, Yelena T. Harden, Gregory K. Harmon, and Holly Ciampi.



Katherine V. Schinasi
Managing Director
Acquisition and Sourcing Management

Appendix: Comments from the Department of Defense

ACQUISITION, TECHNOLOGY AND LOGISTICS

OFFICE OF THE UNDER SECRETARY OF DEFENSE

3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

OCT 28 2003

Ms. Katherine V. Schinasi
Director, Acquisition and Sourcing Management
U.S. General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. Schinasi:

I have enclosed the Department of Defense (DoD) response to the GAO draft report, "DEFENSE ACQUISITIONS: DoD Needs to Better Support Program Managers' Implementation of Anti-Tamper Protection," dated September 11, 2003 (GAO Code 820037/GAO-04-46C).

It includes minor revisions that add further clarity and accuracy to your five recommendations.

We appreciate the opportunity to comment on the draft report. My action officer for this effort is COL Joseph Durso, 703-697-3279.

Sincerely,

Glenn F. Lamartin
Director
Defense Systems

Enclosure

GAO DRAFT REPORT – DATED SEPTEMBER 11, 2003
GAO CODE 820037/GAO-04-46C

"DEFENSE ACQUISITIONS: DoD Needs to Better Support Program Managers' Implementation of Anti-Tamper Protection"

DEPARTMENT OF THE DEFENSE COMMENTS TO THE RECOMMENDATIONS

RECOMMENDATION 1: To better oversee identification of critical technologies for all programs subject to the anti-tamper policy, the Secretary of Defense should direct the Under Secretary for Acquisition, Technology and Logistics in coordination with the Executive Agent and focal points to (1) collect from program managers information they are to develop on critical technology identification and (2) appoint appropriate technical experts to centrally review the technologies identified for consistency across programs and services.

DoD RESPONSE: GAO identified an issue concerning how consistent the Services are when identifying critical technologies and applying the appropriate Anti-Tamper protection to those technologies. The GAO determined that the methods used for identifying critical technologies were somewhat inconsistent from one Service, or program, to another. The GAO addressed a concern that the Services may lack lack sufficient technical expertise to consistently identify critical technologies. DoD partially concurs and offers the following re-write of their recommendation:

RECOMMENDATION 1: To ensure consistent identification of critical technologies throughout the Department of Defense, the Secretary of Defense should direct the Under Secretary for Acquisition, Technology, and Logistics, in coordination with the Executive Agent and focal points throughout the Services and Agencies, to continue developing a more comprehensive, standardized, and consistent critical technology identification processes, and incorporate that process into Anti-Tamper policy and monitor subsequent implementation.

Rationale:
The early, and accurate, identification of critical technologies drives key decisions that directly impact a program's cost, schedule, and performance goals. While DoDI-S 5230.28 instructs program managers on identifying critical technologies, program managers must also identify Critical Program Information (CPI), Critical Information (CI), and Critical System Resources (CSR) according to OPSEC guidance and Service-wide instructions. The processes for identifying these critical features are somewhat similar, but the guidance provided is diverse. Therefore, establishing a more comprehensive and consistent critical technology identification process will minimize much of the subjective nature of the current process. Currently, each Service has an

assigned technical representative who acts as the focal point for providing technical expertise and advice for program managers. This Service representative works closely with the Executive Agent and a variety of technical representatives to ensure each program manager has the appropriate expertise and guidance to implement the Anti-Tamper initiative. Furthermore, the Executive Agent has sponsored quarterly conferences and education seminars to communicate and disseminate important information to Service program managers, government personnel, and industry partners. The Executive Agent continues to build a resource library of available techniques, successful methodologies, and lessons learned. The Executive Agent continues to provide the center of gravity and support necessary to educate the Acquisition community.

RECOMMENDATION 2: To better support Program Managers in the identification of critical technologies, the Secretary of Defense should direct the Under Secretary for Acquisition, Technology and Logistics in coordination with the Executive Agent and focal points to (1) update the implementation guidelines to include a comprehensive list of organizations that provide information on critical technologies or offer technical expertise and (2) work with training organizations to ensure training includes practical information on how to identify critical technologies.

DoD RESPONSE: GAO identified the need for program managers to become more aware of the available organizational and technical expertise supporting critical technology assessment and protection. DoD concurs and offers the following re-write of the recommendation:

RECOMMENDATION 2: To better support Program Managers in the identification of critical technologies, the Secretary of Defense should direct the Under Secretary for Acquisition, Technology and Logistics, in coordination with the Executive Agent and its focal points, to (1) identify available Anti-Tamper technical resources and (2) issue updated policy identifying roles and responsibilities of the technical support organizations, and (3) work with training organizations to ensure training includes practical information on how to identify and protect critical technologies.

Rationale:
Providing an updated list of technical resources available, to include technical experts and organizations, relevant documents, and education seminars and conferences is essential. Improving the flow of information throughout the Executive Agent, DoD, industry, and the government labs will enhance our ability to implement the Anti-Tamper initiative. Information flow must be consistent and constant. The quarterly conferences and education seminars held at Sandia National Lab constitute the primary means to educate Acquisition professionals and the technical community. Furthermore, the Defense Acquisition University program management curricula provide useful and timely information. Methodologies to enable program managers to identify Service-unique critical technologies and initiate protection measures are currently available. The Executive Agent is continuing to develop an active Anti-Tamper data base and

centralized library to ensure consistency and that the DoD has a mechanism to capture essential lessons learned.

RECOMMENDATION 3: To help minimize impact to program cost and schedule objectives, the Secretary of Defense should direct the Under Secretary for Acquisition, Technology and Logistics to work with program managers to ensure that the cost and techniques needed to implement anti-tamper protection are identified early in the system's life cycle and to reflect that practice in guidance and decisions.

DoD RESPONSE: GAO identified an issue with effective program management integration of appropriate critical technology protection into more mature programs that typically results in cost and schedule objective instability. DoD concurs with this issue identification and proposed recommendation.

RECOMMENDATION 4: To maximize the return in investment of DoD's Anti-Tamper technology efforts, the Secretary of Defense should direct the Executive Agent and the Air Force Research Laboratory to monitor the value of developing generic Anti-Tamper techniques and evaluate the effectiveness of the tools, once deployed, in assisting program managers to identify and apply techniques on individual programs.

DoD RESPONSE: GAO identified an issue concerning how effective the DoD is in leveraging and assessing the utility of proven Anti-Tamper techniques. DoD concurs with the issue and offers the following re-write of the recommendation:

RECOMMENDATION 4: To maximize the return of investment on DoD's Anti-Tamper initiative, the Secretary of Defense should direct the Executive Agent to assess the value of developing generic Anti-Tamper techniques and to evaluate the effectiveness of these techniques and tools in assisting program managers to identify and apply them on individual programs.

Rationale:
The Services and DoD agencies are best positioned to evaluate the techniques and tools for protecting critical technologies. Sharing best practices and lessons learned across the Services and the DoD is critical to efficient and affordable implementation. The Services and the Executive Agent monitor the various contractual efforts of participating defense contractors to determine overall effectiveness of the Anti-Tamper techniques being applied to a specific program.

RECOMMENDATION 5: To ensure successful implementation of the Anti-Tamper policy, the Secretary of Defense should direct the Under Secretary of Defense for Acquisition, Technology and Logistics to develop a business case that determines whether the current organizational structure and resources are adequate to implement Anti-Tamper protection, and if not, what other actions are needed to mitigate the risk of compromise of critical technologies.

DoD RESPONSE: GAO identified an issue concerning insufficient resources being applied to protecting critical technologies. DoD concurs with this recommendation and offers the following comments.

Rationale:
Current Anti-Tamper requirements are out-pacing the current availability of resources, such as tools and techniques, to protect critical technologies. Additional funding should be provided to support both the Executive Agent and the Services technical representatives and program managers. The funding provided by the DoD to the Anti-Tamper Executive Agent is sufficient only to provide the most basic research, development, and implementation of the Anti-Tamper initiative. The Services are required to fund specific Anti-Tamper applications and to validate and verify those applications. Now that the Anti-Tamper initiative has matured and the Services are addressing and embracing Anti-Tamper initiatives, we are reviewing the funding as part of the Presidential Budget for the FY 05 build.

GAO's Mission

The General Accounting 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

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. General Accounting 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

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548