Audit Report

OFFICE OF THE INSPECTOR GENERAL

SOFTWARE TESTING DURING POST-DEPLOYMENT SUPPORT OF WEAPON SYSTEMS

Report No. 94-175 August 15, 1994

20000316 066

Department of Defense

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

DTIC QUALITY INSPECTED 3

AQI00-06-1523

Additional Copies

To obtain additional copies of this report, contact the Secondary Reports Distribution Unit, Audit Planning and Technical Support Directorate, at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch, Audit Planning and Technical Support Directorate, at (703) 604-8939 (DSN 664-8939) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

Inspector General, Department of Defense
OAIG-AUD (ATTN: APTS Audit Suggestions)
400 Army Navy Drive (Room 801)
Arlington, Virginia 22202-2884

DoD Hotline

To report fraud, waste, or abuse, call the DoD Hotline at (800) 424-9098 or write to the DoD Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of writers and callers is fully protected.

Acronyms

GAO	General Accounting Office
OPNAV	Office of the Chief of Naval Operations
OSD	Office of the Secretary of Defense
PDSS	Post-Deployment Software Support

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

Report No. 94-175 August 15, 1994

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND TECHNOLOGY
ASSISTANT SECRETARY OF NAVY (FINANCIAL MANAGEMENT)
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit Report on Software Testing During Post-Deployment Support of Weapon Systems (Project No. 4RE-0007)

Introduction

We are providing this final audit report for your information and use. The report discusses policies, procedures, and methodologies for software testing during post-deployment support of weapon systems. Comments on a draft of the report were considered in preparing this final report.

Post-deployment software support (PDSS) organizations (commonly referred to within DoD as PDSS activities) modify weapon system software after delivery to correct errors, improve performance, or adapt to a changed operational or mission requirement. The DoD spent an estimated $21.7 billion in FY 1993 for post-deployment software support of weapon systems. Because software errors can cause a system to fail, possibly with life-threatening consequences, weapon system software should be thoroughly tested before being released. DoD management of software development has been the subject of numerous audits and reviews; however, none of the audits or reviews have focused on software testing of weapon systems during post-deployment support.

Audit Results

The results of our audit are similar to the conclusions and recommendations reached by the DoD Task Force on Improving Software Test and Evaluation. Although the DoD Task Force studies concentrated on software testing during the development of a weapon system, the studies identified conditions and made recommendations that are also applicable to software testing during PDSS.

The DoD has not established procedures to provide insight into the extent of or the cost allocated to post-deployment software support. Consequently, the auditors were unable to define the PDSS universe, and the cost data submitted by the Military Departments accounted for only about 2.2 percent of the estimated $21.7 billion the DoD spent in FY 1993 on weapon system software support. The DoD has not established a disciplined management approach for testing software in weapon systems during post-deployment support. High-level policy and guidance were inadequate, and testing management and practices

were often based on levels of expertise rather than on quantifiable processes. Also, software working groups were active within the Military Departments, and PDSS activities used both commercial and special-purpose software testing tools, but no formal network existed for sharing information. Overall, the audit identified no problems that had not already been identified in a number of previous or current studies, even though only few study results discussed PDSS. As a result, we terminated the audit at the completion of the audit survey.

We commend the four PDSS activities (see Discussion section of report) that identified software testing tools and processes to produce high-quality software and the Air Force for establishing the Software Technology Support Center to promote the exchange of related information throughout DoD.

Objective

The objective of the audit was to evaluate the process for testing software during post-deployment software support of weapon systems and to evaluate applicable internal controls.

Scope and Methodology

To accomplish the objective, we focused on the software change process from unit testing through system integration. Because PDSS activities are not centrally controlled or accounted for by the DoD, we asked each Military Department to provide a list of its PDSS activities. The Military Departments identified a total of 30 activities: 4 Army, 17 Navy, and 9 Air Force. We audited four Army PDSS activities and one Army contractor that performed PDSS. Using physical locations and reported expenditures, we judgmentally selected and audited four Navy and two Air Force PDSS activities. Although operational testing was not within the scope of this audit, we visited an Army, Navy, and Air Force operational test and evaluation organization to gain a better perspective of the quality of software produced by PDSS activities. The organizations visited or contacted are listed in Enclosure 3.

We interviewed managers and technical specialists about software testing and innovative approaches to producing quality software. We reviewed and evaluated DoD and organizational policy related to software development, configuration management, and quality assurance. The documents examined were dated from August 1974 to December 1993.

We performed this economy and efficiency audit from October 1993 through March 1994 in accordance with auditing standards issued by the Comptroller General of the United States as implemented by the Inspector General, DoD. The Audit Planning and Technical Support Directorate provided technical assistance. The audit did not rely on computer-processed data.

Internal Controls

We limited our review of internal controls to those controls related to software testing policy, funding, management, and documentation. We found indications of material internal control weaknesses, as defined by DoD Directive 5010.38, "Internal Mangement Control Program," April 14, 1987, in the areas of PDSS software testing policy and documentation. However, we believe the potential internal control weaknesses will be alleviated if the recommendations of the DoD Task Force on Improving Software Test and Evaluation are implemented. We did not review the implementation of the DoD Internal Management Program by the PDSS activities.

Prior Audits and Other Reviews

The Inspector General, DoD, and the General Accounting Office have made numerous audits of software development and testing. Also, DoD has performed several related studies. Major studies include the Draft DoD Software Master Plan, February 9, 1990, and the Working Group Reports to the Chairman, DoD Task Force on Improving Software Test and Evaluation, November 1, 1993. Additionally, on December 6, 1993, the Under Secretary of Defense for Acquisition (now the Under Secretary of Defense for Acquisition and Technology) issued a memorandum to the Chairman, Defense Science Board, to form the Task Force on Acquiring Defense Software Commercially.

Although none of the audits or studies focused specifically on software testing during post-deployment, the Task Force findings closely parallel the results of our audit. The six studies most relevant to the objective of this audit are summarized in Enclosure 1 and the recommendations of the Task Force on Improving Software Test and Evaluation are in Enclosure 2.

Background

Weapon systems have become increasingly reliant on software. For example, the F-16A fighter aircraft introduced in the mid-1970's had about 125,000 lines of code.[1] A later modification, the F-16C, produced in the late 1980s, required about 230,000 lines of code. The next generation fighter aircraft, the F-22, will require an estimated 4.5 to 6 million lines of code.

Software is critical to a modern weapon system's ability to communicate as well as detect, track, and engage enemy targets. Frequently, mission-critical software must be changed to correct system deficiencies, improve system effectiveness, and keep up with new doctrines and threats. Failure of software to function correctly and in a timely manner can endanger lives and equipment and can threaten national security. The PDSS activities are responsible for making software changes.

---

[1]Generally, a line of code is considered a single computer program command, declaration, or instruction.

The DoD has not tracked software costs as a distinct item and, therefore, does not know how much is spent on this critical technology. The Defense Systems Management College estimated the DoD spent about $31 billion on software in 1993 and that PDSS accounts for 70 percent of the life-cycle cost of software. Using those estimates, we calculated the DoD spent $21.7 billion in FY 1993 just to maintain, upgrade, and modify software in deployed weapon systems.

DoD budget constraints will result in the procurement of fewer new weapon systems. With fewer procurements, many new and changing threats will require that existing systems provide additional functionality and a longer life-span. Therefore, the cost of PDSS is expected to continue growing.

Discussion

Software Testing Standards. DoD lacks a comprehensive software testing policy. The DoD has not adopted a core set of software metrics[2] or uniform standards for software testing tools. The PDSS activity managers developed local practices and determined the type and extent of use of each software testing tool acquired. Consequently, we could not establish a basis for evaluating software testing management throughout the Military Departments. Four PDSS activities (one Army, two Navy, and one Air Force) had developed superior processes for improving software quality. In addition, the Air Force Software Technology Support Center has promoted the exchange of software information within DoD through the use of publications, conferences, and an electronic bulletin board.

PDSS Activity Universe. We were unable to determine the number of PDSS activities within the DoD. The Army reported 4 activities supporting 357 software systems, the Navy identified 17 activities supporting 116 systems, and the Air Force reported 9 activities supporting 107 systems. However, the Military Departments did not include some of their subordinate PDSS organizations and did not report the extent of PDSS work done by contractors. Additionally, the Military Departments did not use a consistent definition of a weapon system.

Defining PDSS. DoD Instruction 5000.2, part 15, "Defense Acquisition Management Policies and Procedures," February 23, 1991, defines PDSS as support that occurs during the deployment phase of the system's life cycle. At the time of our audit, the Navy and Air Force operated in accordance with that concept. However, some Army components did not consider PDSS to begin until production of the weapon system was completed. As a result, the Army categorized systems that had been deployed for 10 years or longer as still being in production.

---

[2]Metrics provide a method of measuring the elements of the development process, such as time, cost, and resources, which allow organizations to better understand and manage the relationships among resource decisions, development schedules, and the cost of software projects.

Defining a Weapon System. DoD Instruction 5000.2, part 15, defines a weapon system as an item that can be used directly by the armed forces to conduct combat missions and that costs more than $100,000 per item or more than $10 million in total procurement. However, the definition and interpretation of a weapon system differed among the Military Departments. For instance, Army and Air Force personnel generally viewed a weapon system as a subsystem of a weapon platform, such as a tank or aircraft, while Navy personnel generally equated a weapon platform to a weapon system. Because the interpretations differed among the Military Departments, we were unable to establish a standard methodology as to how the systems should be counted.

Cost of Post-Deployment Software Support. The cost to DoD for PDSS is undefined primarily because DoD has not established uniform guidelines for collecting and reporting PDSS cost data or other related information regarding software support during post-deployment. PDSS represents about 70 percent of the system's software life-cycle costs; therefore, DoD officials should have reasonable assurance that the information collected and maintained by the PDSS activities account for the resources expended. However, our analysis showed that the $483 million reported by the Military Departments to operate their PDSS activities during FY 1993 represented only about 2.2 percent of an estimated $21.7 billion spent by the DoD for weapon system software support.

We believe one reason for the disparity between the estimated and reported costs is that the PDSS activities are funded through various appropriations. Post-deployment is considered to be a maintenance function, which requires Operation and Maintenance funds. However, a PDSS activity may legitimately use Research, Development, Test and Evaluation; Procurement; or Operation and Maintenance funds, depending on the type of work performed and funds appropriated. PDSS funding data captured and documented under uniform guidelines would provide needed insight into actual costs.

Software Testing Policy. The DoD policy for software testing during post-deployment support needs to be improved. The following policy documents contain guidance on the testing process:

o DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures," February 23, 1991;

o DoD Standard 2167A, "Defense System Software Development," February 29, 1988;

o DoD Standard 2168, "Defense System Software Quality Program," April 29, 1988; and

o Military Handbook 347, "Mission-Critical Computer Resources Software Support," May 22, 1990.

References to software testing in those documents generally related to the acquisition process. For example, DoD Instruction 5000.2 applies to the management of major and nonmajor defense acquisition programs that provide a new or improved capability in response to a validated need. DoD

Standard 2167A may be applied to PDSS activities, but is primarily intended to provide a standardized process and other requirements for contractors' software development, testing, and evaluation efforts. In addition, a program manager can tailor the provisions of DoD Standard 2167A to meet special program requirements. Only Military Handbook 347 discusses software support activities and requirements throughout a system's life cycle. However, a handbook does not establish policy; it merely implements or supplements a directive that establishes policy.

Lacking specific, enforceable policy guidance at the DoD level, the Military Departments also have not developed comprehensive software testing policy applicable to post-deployment support. For example, Navy policy on test and evaluation is found in Office of the Chief of Naval Operations (OPNAV) Instruction 5000.42, "OPNAV Role and Responsibilities in the Acquisition Process." The Instruction relates to the acquisition process, not software testing.

Management of Software Testing. The DoD has not adopted a core set of software metrics for monitoring and managing the software development process. Lacking a common quantifiable basis for measuring the elements of the software development process, the Military Departments based testing management and practices primarily on the expertise of individual managers. Consequently, the auditors could not assess the management of software testing throughout the Military Departments.

Further, communication among the PDSS activities was not fully effective. Although software working groups existed within the Military Departments, no formal network existed to enhance and encourage information sharing within or among the Military Departments. Even when PDSS activities were located in close proximity, one activity was not necessarily aware of improved software testing processes or procedures used by the other activity. The lack of an information exchange network causes many valuable lessons learned in software development to be lost and limits the overall growth and performance of the PDSS activities.

On the other hand, a majority of the PDSS activities recognized the need for process improvements. Two activities each in the Army, Navy, and Air Force were using the Capability Maturity Model (the Model) developed by the Software Engineering Institute. The Model helps to identify existing or potential productivity problems that can be alleviated through a more effective software engineering process. The Model could be applied to all DoD organizations engaged in life-cycle software support. The evaluations that result from using the Model could help maximize DoD's scarce resources and could help emphasize the need for productivity improvements. Additionally, uniform application of the Model would provide a common reference for evaluating PDSS activities.

Software Testing Tools. Software testing tools were in use at all PDSS activities. The tools spanned the range from commercial off-the-shelf tools, such as text editing software, to special-purpose simulators designed to test a

particular system under development. Software testing tools can be used, for example, to analyze compliance with standards, to generate inputs for test cases, or to test the execution of software.

However, the types of testing tools acquired and the degree to which they were used during the post-deployment software support process was unique to each PDSS activity. Standardization did not exist because the PDSS activity managers determined the type and extent of the use of each software testing tool acquired and because DoD has not adopted uniform practices or standards for software testing tools. Additionally, the costs of software testing tools were uniformly borne by the PDSS activity or one of the activity's software projects. Moreover, no easily accessible data base exists for testers to learn about software testing tools used throughout the DoD. Also, DoD lacks a centralized source of funding for acquiring needed tools or for evaluating promising tools.

Better Software Practices. At each organization and PDSS activity audited, we asked senior management to identify software tools and practices that produced high-quality software or that significantly reduced software support costs. We considered five responses to be especially noteworthy.

Cleanroom Software Engineering. The Army's Life-Cycle Software Engineering Center at Picatinny Arsenal, Dover, New Jersey, employed a software development process called Cleanroom Software Engineering for reengineering the software for the Mortar Ballistic Computer. The Army selected Picatinny Arsenal as a test site to determine whether Cleanroom Software Engineering practices could be transferred to project teams at a typical PDSS activity. Although the reengineering effort was ongoing during the audit, initial results showed more than a 300-percent gain in productivity and an error rate of only about 1 per 4,000 lines of code.

Software Reuse and Database Tracking. The Fleet Combat Direction Systems Support Activity at Dam Neck, Virginia, maintains the Advanced Combat Direction Systems for the Navy. That activity uses a relational data base and a common reusable software library to help create operational software programs for multiple classes of ships with divergent capabilities. The Fleet Combat Direction Systems Support Activity created 90 to 95 percent of new software versions without modification from a single set of source software components retrieved from the common reusable library. The improved process for software reuse has saved an estimated $7.3 million since 1988.

Integration Testing with Other Software Systems. The Navy's Integrated Combat Systems Test Facility at San Diego, California, verifies that subsystem software operates in an environment that is detailed in performance and design specifications. Operationally realistic tests conducted at the facility evaluated functional, interface, stress, and endurance factors. Since 1984, improved processes have reduced integration testing time from about 10 to 15 months to about 4 to 5 months.

Use of Commercially Available Testing Software. The Common Modular Environment system at Hill Air Force Base, Utah, used for integration testing of software developed for the F-16 aircraft, was designed to maximize

the use of commercially available hardware and software. Also, the Common Modular Environment design features the capability to support the testing of software in other weapon systems and platforms, such as tanks, helicopters, and ships. Air Force management stated that the Common Modular Environment system costs $21 million less than originally estimated, primarily due to the use of commercial products and in-house development.

Air Force's Software Technology Support Center. A function of the Software Technology Support Center (the Center), located at Hill Air Force Base, Utah, is to demonstrate the advantages and viability of emerging software development products and processes. One of the Center's demonstration projects, the development and enhancement of a software tool set to facilitate the reengineering of embedded software, is expected to save the Air Force Materiel Command an estimated $20 million in software maintenance costs from 1994 through 2003.

The Center also promotes an information exchange throughout DoD. The Center publishes and distributes a monthly journal for DoD software engineering professionals, manages an annual software technology conference, and administers its own electronic bulletin board to provide customers with access to and feedback on emerging software practices and processes.

As illustrated above, some PDSS activities have incorporated adaptable software development and testing tools, software reuse, and integration testing into routine business practices. Although the tools and processes had been developed to support specific requirements, the tools and processes have the potential for improving life-cycle software support throughout DoD and illustrate the need for a formal DoD-wide platform in which to share information on better software tools, methodologies, and associated benefits.

DoD Software Test and Evaluation Task Force

Many DoD studies have been conducted on improving software practices. Of particular relevance to our audit was the study done by the DoD Task Force on Improving Software Test and Evaluation (the Task Force). The Task Force, composed primarily of representatives from the Office of the Secretary of Defense and the Military Departments, was divided into three working groups on policy, procedures, and tools. Each working group submitted a report to the Task Force chairman on November 1, 1993. A summary of each working group's study results is presented below, and recommended solutions to identified problems are in Enclosure 2.

Software Test and Evaluation Policy. The Software Test and Evaluation Policy Working Group identified several policy deficiencies. The group found that software acquisition, life-cycle management, and interoperability are discussed in three DoD policy documents and that each document uses different terminology and applies different processes to similar software development efforts. The group also concluded that DoD policy does not sufficiently emphasize the development and documentation of software requirements and does not effectively guide DoD Components in defining requirements during

evolutionary software development efforts. The group found that the test and evaluation function is involved too late in the software development process to help avoid software defects and to economically remedy the defects discovered. The group found no clear and concise policy for operational test and evaluation in evolutionary software development. The working group also noted policy deficiencies for operational test and evaluation in systems heavily composed of software previously developed by DoD or obtained from commercial sources. Additionally, the group members determined that stronger policy was needed to improve software configuration management and to strengthen the education and skills of the software acquisition work force.

Software Test and Evaluation Procedures. The Software Test and Evaluation Procedures Working Group determined that the software test and evaluation function could be more effectively used and could better support the software development process. The group found that software requirements and capabilities were not well-defined or testable because the test and evaluation function did not usually participate during the requirements definition phase of software development. The group also determined that error correction costs were unnecessarily high because errors were not identified and repaired early in the development process. Further, test and evaluation functions were not performed in accordance with the inherently incremental nature of software development and that criteria related to the need for and intensity of operational test and evaluation were not established at the beginning of software development. The working group also found that test and evaluation during PDSS was not always tailored to reflect the scope and significance of software changes made. Additionally, configuration management practices did not consistently identify and control test planning documents and system baselines.

Software Test and Evaluation Software Tools. The Software Test and Evaluation Software Tools Working Group explored the roles of software tools in improving test and evaluation during the life cycle of DoD software. Overall, the working group concluded that tool-based methodologies had not been sufficiently exploited to improve the software test and evaluation function. Available software tools had not been used to enable early and continuous involvement in the software development process. Software tools also had not been used to effectively track and manage software requirements. The working group found that DoD had expended scarce resources in trying to establish software tool standards and practices instead of adopting established standards and practices used in the commercial marketplace. The group also determined that practitioners were not educated in software tool methodologies or use and that formal training in software tools usage and testing methodologies was neither emphasized nor widely available. Additionally, the working group concluded that funding cycles and limitations, coupled with a general lack of knowledge of software development processes and tools, provide insufficient incentive for program managers to change existing software development procedures.

Summary

No common criteria existed on which to assess performance among or within the Military Departments. DoD has established no standards for collecting or reporting cost data, developing and using software tools, measuring quality, or sharing knowledge of software testing during PDSS. In short, our survey identified many of the problems already identified by the Task Force.

We agree with the Draft DoD Software Master Plan that it is time for action and that the DoD does not need another study of software problems. Without comprehensive policy and procedures, objective measures cannot be established for the life-cycle software support process. We believe that implementation of the recommendations of the Task Force on Improving Software Test and Evaluation would provide a workable baseline. Until a baseline is in place, an accurate evaluation of the life-cycle software support process will be difficult.

Management Comments and Audit Response

Under Secretary of Defense for Acquisition and Technology Comments. The Director, Test and Evaluation, Office of the Under Secretary of Defense for Acquisition and Technology, concurred with our survey results and agreed that many of the findings in previous audits and reports that focused on the development phase of weapon system software also applied to software in the post-deployment phase. The complete text of the comments is in Enclosure 4.

Department of the Army Comments. The Director, Test and Evaluation Management Agency, Department of the Army, generally concurred with the report, but took exception to statements on when PDSS began, on PDSS software testing policy, and on the use of software metrics. The Army stated it was not aware of specific Army programs that delayed planning PDSS until after production was completed. Also, the Army referred to comprehensive software testing policy applicable to post-deployment support in Army Regulation 73-1, "Test and Evaluation Policy," October 15, 1992. Additionally, the Army stated that it had identified a set of metrics and established software testing procedures in Army Pamphlet 73-1 (Draft), September 30, 1992. The complete text of the Army's comments is in Enclosure 5.

Audit Response. The report does not state that the Army delayed PDSS planning, but that some Army components considered the actual phase of post-deployment support to begin after production of a weapon system was completed. We recognize that the Army has a testing policy that discusses post-deployment software support. However, as indicated in the report, the DoD and Military Department testing policies focus on the acquisition process rather than on a comprehensive life-cycle process that includes post-deployment support. For example, Army Regulation 73-1 implements the policies and procedures of DoD Instruction 5000.2, which focuses on the acquisition process, not post-deployment support. We also recognize that the Army has a set of software metrics unique to the Army. However, the DoD has not

established a uniform quantifiable basis for measuring the elements of the software managed by the Military Departments. A complete and core set of software metrics should consist of software management metrics, which are primarily indicators that help measure planned development progress; quality metrics, which focus on performance, supportability, and ease of software change; and process metrics, which relate to the development and delivery of software.

Department of the Navy Comments. The Department of the Navy verbally responded that it had no comments.

Department of the Air Force Comments. The Director, Test and Evaluation, Department of the Air Force, generally nonconcurred with the report and suggested that we delete all nonsoftware testing discussions, such as software development practices, cleanroom software engineering, software quality programs, and software reuse programs, from the report. The comments further stated that the report incorrectly states that the DoD does not have a standard set of software metrics, many software tools would not be applicable for all software applications, and PDSS activities require the flexibility to select which software tools best fit their needs. Also, the estimate of $21.7 billion a year for post-deployment software support of weapon systems is inaccurate. Finally, the Air Force questioned why its Air Force operational test and evaluation agency was not included in the survey. The complete text of the Air Force comments is in Enclosure 6.

Audit Response. We did not delete discussions relating to software quality assurance, software configuration management, and improved software practices because they are relevant to the software testing process. Software testing is an integral element of the support of a weapon system. The DoD Task Force on Improving Software Test and Evaluation also evaluated software testing from an overall perspective of the software life cycle. Further, the Task Force recommended policy that would include test and evaluation as part of a cooperative team effort involved in reducing the risk of failure throughout the weapon system's life cycle.

On May 23, 1994, the Director, Test and Evaluation, Office of the Under Secretary of Defense for Acquisition and Technology, provided policy guidance on software metrics. However, the guidance discussed only software management metrics for major defense programs early in the development phase and approved at the Milestone II review. The guidance discusses neither quality metrics nor process metrics nor PDSS, the longest phase of a weapon system's life cycle.

This report states that DoD has not adopted uniform practices or standards concerning software testing tools and does not state that a standard set of tools be adopted. Also, the DoD Task Force on Improving Software Test and Evaluation concluded in its final report that the DoD should adopt national practices and commercial standards and ". . . should not expend valuable resources in insisting on tools that no one else seems to want or need."

The DoD does not know the specific amount spent on software and relies on estimates since aggregate software line items are not in the budget. The Deputy Director for Command, Control, Communications, and Intelligence, and Major Automated Information Programs, Office of the Under Secretary of Defense for Acquisition and Technology, estimated that software costs for the FY 1993 defense budget totaled at least $50 billion and that post-deployment software support accounted for 70 to 80 percent of software expenditures. The report shows a more conservative estimate, provided by the Defense Systems Management College, of $31 billion in total software costs and 70 percent of expenditures for post-deployment software support.

Finally, the auditors visited selected operational test and evaluation organizations to gain a better perspective of the quality of testing performed during post-deployment software support. The auditors visited the 57th Test Group, Nellis Air Force Base, Nevada, which performs operational tests and evaluations. However, the focus of the audit was on software testing during PDSS rather than on operational test and evaluation.

Written comments on the final report are not required. If you choose to comment, please do so by September 15, 1994.

The courtesies extended to the audit staff are appreciated. If you have questions on this audit, please contact Ms. Mary Lu Ugone, Audit Program Director, at (703) 604-9539 (DSN 664-9539) or Mr. James W. Hutchinson, Audit Project Manager, at (703) 604-9530 (DSN 664-9530). The distribution of this report is listed in Enclosure 7. The audit team members are listed inside the back cover.

Robert J. Lieberman

Robert J. Lieberman
Assistant Inspector General
for Auditing

Enclosures

Prior Audits and Other Reviews

Defense Science Board Task Force on Acquiring Defense Software Commercially. The then Under Secretary of Defense for Acquisition requested on December 6, 1993, that a Defense Science Board task force be formed to develop a strategy for defense software procurement. The Under Secretary asked that the task force determine the conditions under which the procurement of software and software tools could use commercial practices. The study was ongoing as of the completion of our audit.

General Accounting Office (GAO) Report No. NSIAD-93-198 (Office of the Secretary of Defense [OSD] Case No. 9439), "Test and Evaluation - DoD Has Been Slow in Improving Testing of Software-Intensive Systems," September 1993. The report focused on problems in DoD's Operational Test and Evaluation process. GAO stated that software intensive systems do not meet user requirements, barriers exist to effectively test and evaluate software, and previously identified solutions to software problems had not been implemented. The GAO recommended that the Secretary of Defense issue and implement a software test and evaluation policy, define criteria for determining when a system is ready for operational test and evaluation, and require the development of a common core set of software management metrics. The DoD concurred with the GAO recommendations and is drafting software test and evaluation policy.

GAO Report No. IMTEC-93-13 (OSD Case No. 9274), "Mission-Critical Systems - Defense Attempting to Address Major Software Challenges," December 1992. The report reiterated problems with DoD mission-critical computer systems identified in prior GAO reports. GAO categorized these problems into three areas: lack of management attention, ill-defined requirements, and inadequate testing. The report contained no recommendations and recognized two ongoing DoD efforts to ameliorate the problems: the software action plan working group formed by the Director of Defense and Engineering and the DoD Corporate Information Management initiative.

Draft Defense Acquisition Board DoD "Software Master Plan," February 9, 1990. The Master Plan recommended specific improvements in research, development, test, deployment, and maintenance of software in defense systems. The improvements included a revised acquisition structure, updated policy and standards, improved training, and improved management of the software technology base. Implementation of the Master Plan was discontinued after coordination with the Military Departments failed to produce full concurrence with its recommendations.

Inspector General, DoD, Report No. 89-068, "Management of Software for Mission-Critical Computer Resources," April 18, 1989. The report states that procurement officials were not consistently requiring contractors to follow current software development and quality assurance standards. In addition, software documentation reviews did not meet the oversight requirements of the Federal Acquisition Regulation and the Defense Quality Assurance Program.

The report recommended that project management offices be required to cite current DoD software standards in contracts for mission-critical computer resources. DoD management, the Military Departments, and the Defense Logistics Agency agreed with most of the report conclusions and with most of the recommendations. DoD issued guidance for overseeing the implementation of DoD Standard 2168, "Defense Systems Software Quality Program," on December 14, 1990. In addition, DoD Directive 5000.1, "Defense Acquisition," February 23, 1991, and DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures," February 23, 1991, were revised to mandate the use of current software standards in contracts.

Inspector General, DoD, Report No. 88-126, "Summary Report on the Defense-Wide Audit of Support for Tactical Software," April 7, 1988. The report states that the adequacy of planning, support, and guidance for tactical software and the implementation of the Ada computer programming language needed to be improved. The report recommended establishing new, expanded guidance on the planning and support of tactical software and better implementation of the Ada programming language. The then Under Secretary of Defense for Acquisition generally concurred with the report and the recommendations. To enhance the planning and support for tactical software, DoD issued revised software development procedures (DoD Standard 2167A, "Military Standard Defense System Software Development," February 2, 1988). DoD also provided guidance for assuring the quality of that software through the issuance of DoD Standard 2168, "Defense Systems Software Quality Program," April 29, 1988.

DoD Task Force on Improving Software Test and Evaluation

The Director, Test and Evaluation, announced in a December 17, 1992, memorandum the establishment of the Task Force on Improving Software Test and Evaluation (the Task Force). The Task Force focused on the ability to better test software in automated information systems; in command, control, communications, computers, and intelligence systems; and in software embedded in weapon systems. The Task Force was divided into three working groups to examine software test and evaluation policy, procedures, and software tools.

Software Test and Evaluation Policy Working Group. The Policy Working Group focused on the current software test and evaluation process and on policy initiatives to harmonize the process with evolving approaches to DoD acquisitions. The Software Policy Working Group made recommendations to the Task Force on Improving Software Test and Evaluation in the following areas.

o Software Requirements. Provide a coherent and consistent policy that details the iterative and evolutionary nature of requirements generation for software intensive systems and that encourages the evaluation and implementation of new technologies that support those efforts.

o Policy for Software Intensive Systems. Provide a single source of policy for the acquisition of software intensive systems, life-cycle management, and interoperability.

o Software Test and Evaluation. Establish policy that makes test and evaluation a value-added, risk-reduction process that results from the cooperative efforts of a team of development, maintenance, and operational testers.

o Defect Prevention. Establish policy that requires the early application of defect prevention techniques.

o Configuration Management. Provide a process that directs implementation of continuous and integrated system-level configuration management throughout the life cycle of software intensive systems.

o Operational Test and Evaluation. Develop a logical process that provides for the identification of criteria regarding the frequency and intensity of Operational Test and Evaluation on evolutionary or incremental acquisitions, and develop policy that implements that process.

o Operational Test and Evaluation. Develop a logical process that provides for the identification of criteria regarding the need for and intensity of

Operational Test and Evaluation on systems composed primarily of previously developed software or software readily available from commercial sources, and develop policy that implements that process.

o Acquisition Personnel Capability. Educate and improve the performance of the entire software acquisition work force.

Software Test and Evaluation Procedures Working Group. The focus of the Procedures Working Group was to describe procedural improvements for software development beginning with the software requirements process and continuing through post-deployment software support. The working group identified an improved software development process consisting of the following elements:

o development of a user functional description or Operational Requirements Document,

o user involvement throughout the software development process,

o incremental development and testing of software capability,

o a decision mechanism that authorizes incremental deployment of the software,

o a decision point for certification of an operationally tested representative sample, and

o a post-deployment software support capability that minimizes the formal processing required and that avoids disruption in the deployed system.

Software Test and Evaluation Tools Working Group. The goal of the Software Tools Working Group was to reduce software life-cycle costs, schedules, and technical risk through the use of software tools. The Working Group formulated six recommendations.

o Enforce early and continuous involvement by test and evaluation personnel based on available software tools.

o Use appropriate software tools to manage software requirements and to trace specific software tests to those requirements.

o Adopt national practices and commercial standards for software tools and software development methods.

o Educate practitioners on the existence and benefits of software tools and the methodologies underlying tool use.

o Promote an interactive distributed knowledge base concerning and involving software tools.

o Educate program managers and provide incentives to use software tools.

Organizations Visited or Contacted

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology, Washington, DC
Director, Test and Evaluation, Washington, DC
Director, Defense Research and Engineering, Washington, DC
Deputy Assistant Secretary of Defense for Production Resources, Assistant Secretary of Defense (Economic Security), Washington, DC

Department of the Army

Assistant Secretary of the Army for Research, Development, and Acquisition, Washington, DC
- Program Executive Office, Armored Systems Modernization, Warren, MI
- Program Executive Office, Combat Support Vehicles, Warren, MI
- Program Executive Office, Tactical Missiles, Redstone Arsenal, Huntsville, AL
- Program Executive Office, Aviation, St. Louis, MO

U.S. Army Operational Test and Evaluation Command, Alexandria, VA
Army Materiel Command, Alexandria, VA
- U.S. Army Tank-Automotive Command, Warren, MI
- Aviation Troop Command, St. Louis, MO
- Armament Research and Development Engineering Center, Picatinny Arsenal, Dover, NJ
- U.S. Army Test and Evaluation Command, Washington, DC
- Communications and Electronics Command, Fort Monmouth, NJ
- Missile Command, Redstone Arsenal, Huntsville, AL
- Armament, Munition and Chemical Command, Rock Island, IL
- Army Materiel Systems Analysis Agency, Aberdeen, MD

Department of the Navy

Assistant Secretary of the Navy for Research, Development, and Acquisition, Washington, DC
Headquarters, Naval Air Systems Command, Arlington, VA
- Naval Aviation Depot, San Diego, CA

Headquarters, Naval Sea Systems Command, Arlington, VA
- Naval Surface Warfare Center, Arlington, VA
  - Fleet Combat Direction Software Support Activity, Dam Neck, VA
  - Integrated Combat Systems Test Facility, San Diego, CA
- Naval Undersea Warfare Center, Newport, RI

Headquarters, Space and Naval Warfare Systems Command, Arlington, VA
Headquarters, Operational Test and Evaluation Force, Norfolk, VA

Department of the Navy (cont'd)

Headquarters, U.S. Marine Corps, Washington, DC
Marine Corps Systems Command, Quantico, VA
Marine Corps Tactical Systems Support Activity, Camp Pendleton, CA

Department of the Air Force

Director, Air Force Test and Evaluation, Washington, DC
Headquarters, Air Force Materiel Command, Wright-Patterson Air Force Base, OH
Ogden Air Logistics Center, Hill Air Force Base, UT
Warner-Robins Air Logistics Center, Robins Air Force Base, GA
Oklahoma City Air Logistics Center, Tinker Air Force Base, OK
Sacramento Air Logistics Center, McClellan Air Force Base, CA
San Antonio Air Logistics Center, Kelly Air Force Base, TX
Headquarters, Air Combat Command, Langley Air Force Base, VA
57th Test Group, Nellis Air Force Base, NV

Contractor

McDonnell-Douglas Helicopter Systems, Mesa, AZ

Under Secretary of Defense for Acquisition and Technology Comments

OFFICE OF THE UNDER SECRETARY OF DEFENSE

3000 DEFENSE PENTAGON
WASHINGTON DC 20301-3000

ACQUISITION AND TECHNOLOGY

11 JUL 1004

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL (DIRECTOR, READINESS AND OPERATIONAL SUPPORT DIRECTORATE)

SUBJECT: Draft Audit Report on Software Testing During Post-Deployment Support of Weapon Systems (Project No. 4RE-0007)

We have reviewed the DoD IG draft audit report. Since this report contained no findings or recommendations, we reviewed the survey results and found them to be consistent with the conclusions and recommendations of previous audits and reviews in this area. Furthermore, we agree with the DoD IG assertion that many of the findings and recommendations contained in earlier audits and reports were focused on the development phase of weapon system software, but these findings apply equally to the post-deployment phase.

Subsequent to the DoD IG audit survey completion date the Director, Test and Evaluation and the Director, Operational Test and Evaluation provided a core set of metrics requirements. These memoranda are attached for your information.

John A. Burt
Director
Test and Evaluation

Attachments

OFFICE OF THE UNDER SECRETARY OF DEFENSE

3000 DEFENSE PENTAGON
WASHINGTON DC 20301-3000

ACQUISITION AND TECHNOLOGY

23 MAY 1994

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Development Test and Evaluation (DT&E) Policy Guidance for Software-Intensive Systems in Support of Recommendations from the General Accounting Office (GAO)

The GAO report GAO/NSIAD-93-198, "Test and Evaluation: DoD Has Been Slow in Improving Testing of Software-Intensive Systems," dated September 29, 1993, made four recommendations:

1) Establish testing requirements for software maturity, regression testing, and temporary software fixes;

2) The results of Developmental Test and Evaluation must demonstrate an appropriate level of software maturity prior to the start of Operational test and evaluation;

3) Define software related exit criteria for certifying a system's readiness for operational testing at Milestone II; and

4) A common core set of management metrics are to be developed and approved at Milestone II.

The attached Guidance for GAO recommendations 1,3, and 4 is intended to implement the three recommendations addressed by OUSD(A&T) T&E. This guidance will be implemented in revisions to the DoD 5000 and 8120 policy documents. The Director, Operational Test and Evaluation will provide guidance for GAO recommendation 2.

The attached guidance incorporates the comments received from the DoD Components on the Draft Guidance attached to the OUSD (A&T) memorandum, subject: "Developmental Test and Evaluation (DT&E) Criteria for Software-Intensive Systems, dated April 4, 1994. The guidance is meant to augment, but not replace, the existing Service and Agency guidance on software testing in order to improve the effectiveness of DT&E.

John A. Burt
Director
Test and Evaluation
OUSD (A&T)

Attachment

Distribution:

JOINT STAFF, DIRECTOR FOR FORCE STRUCTURE, RESOURCES AND ASSESSMENT (J-8)
ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE
DEPUTY UNDER SECRETARY OF THE ARMY (OPERATIONS RESEARCH)
DIRECTOR, TEST AND EVALUATION, HEADQUARTERS USAF
DIRECTOR, NAVY TEST AND EVALUATION
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENCY
DIRECTOR, DEFENSE MAPPING AGENCY
DSMC
DOTE

DoD Test and Evaluation Policy Guidance
for Software-Intensive Systems

1. Implementation of GAO Recommendation 1: Testing requirements are established for software maturity, regression testing and the use of temporary software fixes during testing.

   a. The program management office for a software-intensive system shall propose a maturity metric, for use in monitoring and managing the program throughout the Development Phase, and shall submit the metric for approval by the appropriate acquisition authority. The quality metrics listed by the Army's Software Test and Evaluation Panel (STEP) may be used as a basis for obtaining the maturity metric.

   b. All DoD Components shall, prior to any government system-level developmental testing, establish and freeze the software configuration. Any changes proposed during system-level testing, to include software fixes, shall be kept to a minimum and shall be reviewed and approved by the Component's configuration control board for the respective acquisition program using MIL-STD-973 as guidance. All software development shall be fully documented.

   c. Sufficient regression testing shall be conducted for all software changes, throughout the development cycle and after implementation of configuration control, to ensure that changes designed to correct specific problems do not result in additional defects. The scope of regression testing is determined by the developer/contractor prior to freezing the configuration, and determined by the test organization, developer and independent evaluator after the configuration is frozen. Changes made to the software, during system-level testing or later, can impact the resources and schedule of a Component's test organization and therefore impact the testing of other programs. All software configuration changes shall be documented using MIL-STD-973 as guidance.

   d. The DoD Component shall ensure that the proper levels of testing have been accomplished and determine if additional testing is required before certification for independent operational tests.

2. Implementation of GAO Recommendation 3: Program management officials shall define software related exit criteria for certifying a system's readiness for Operational Testing at Milestone II.

   Department of Defense Instruction 5000.~~8~~2, Part 8, requires certification that the system is ready for the dedicated phase of operational test and evaluation to be conducted by the DoD Component operational test activity. In order to

comply with this policy,

a. Each DoD Component shall develop a process, or modify an existing process, for program management officials to define software related exit criteria at Milestone II for software-intensive systems for the purpose of certifying the system's readiness for operational testing.

b. These exit criteria are required to be defined at Milestone II. These criteria may be modified and/or criteria may be added as appropriate during the system's development phase.

3. Implementation of GAO Recommendation 4: A common core set of management metrics for software shall be developed by the services for major defense programs early in the development cycle to be approved at Milestone II.

The following core set of management metrics shall be implemented by DoD Components for major software-intensive defense programs. These metrics comprise a minimum set for information gathering over the life cycle of a program, and must be developed to support program approval at Milestone II. Each DoD Component may develop and implement additional metrics for Milestone II or for subsequent portions of the life cycle to aid in program monitoring or to support other needs of the DoD Component. One metric that should be selected at Milestone II for use during the development phase is "fault profile," which is comprised of the total number of faults over time (identified and corrected) and the severity of these faults categorized as Priority 1, 2, 3 and 4 versus set periods of time that the faults are open (e.g., 0-15 days, 15-30 days, 30-60 days, etc.). Additional metrics are:

a. Cost. A cost metric shall be developed which will provide insight into how well the cost of software development is controlled. The cost metric should address software development costs as well as the life-cycle cost impacts of the software development;

b. Schedule. A schedule metric shall be developed which will indicate changes and adherence to the planned schedules for major system development milestones, activities and key software deliverables; and

c. Requirements Traceability. A requirements traceability metric shall be developed which will measure the adherence of the software products (including design and code) to their requirements at the system level.

Department of the Army Comments

Final Report
Reference

DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF OF STAFF
WASHINGTON, DC 20310-0200

22 JUL 1994

REPLY TO
ATTENTION OF

DACS-TE

MEMORANDUM THRU 7/22/94

DEPUTY UNDER SECRETARY OF THE ARMY (OPERATIONS RESEARCH)

FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE (AUDITING)

SUBJECT Draft Audit Report on Software Testing During Post Deployment Software Support of Weapon Systems (Project No. 4RE-0007)

1. This memorandum is in response to your request (14 June 1994, Subject as Above) to review and comment on the subject draft audit report Although the audit was discontinued and the draft report contains no findings or recommendations, the Army is forwarding the following comments

2 Page 4, **Discussion**, 1st paragraph This problem has also been identified in the General Accounting Office Final Report GAO NSIAD-93-198, "TEST AND EVALUATION: DoD has been Slow in Improving Testing of Software-Intensive Systems". As a result of this report, DoD has developed a core set of metrics consisting of cost, schedule, and requirements traceability These metrics were patterned after the Army's existing metrics identified in DA Pam 73-1, Part Seven (Draft), 30 September 1992

3 Page 5, **PDSS Activity Universe**, 2nd paragraph, last two sentences, **...some Army components did not consider PDSS to begin until after production of a weapon system was completed.** : We are not aware of any specific Army programs that delayed planning PDSS until after production was completed Please note that regarding conduct of PDSS, guidance in Chapter 11 of DA Pam 73-1, Part Seven (Draft), 30 September 1992, states that post-deployment software support (PDSS) consists of modifications and maintenance of software in *fielded systems or systems to be fielded after MSIII decision.* Page 4

4 Page 6, **Software Testing Policy**, last paragraph, **...the Military Departments also have not developed comprehensive software testing policy applicable to post-deployment support.** The Army disagrees with this statement. The Army clearly delineates its comprehensive software testing policy of its PDSS in paragraphs 3-2, 3-7, 4-4, 4-5 and 4-6 of AR 73-1.

5 Page 6, **Management of Software Testing**, 1st sentence, **...The DoD has not adopted a core set of software metrics...** Please refer to comments in paragraph 2 of this letter.

ENCLOSURE 5
(Page 1 of 2)

Department of the Army Comments

Final Report Reference

DACS-TE
SUBJECT: Draft Audit Report on Software Testing During Post Deployment Software Support of Weapon Systems (Project No 4RE-0007)

6 Page 6, **Management of Software Testing**, 2nd sentence,...**Lacking a common quantifiable basis for measuring the elements of the software development process, the Military Departments based testing management and practices primarily on the experiences of individual managers.** This assessment is not valid for the Army The Army has clearly identified a set of 12 metrics in Chapter 17 of DA Pam 73-1, Part Seven (Draft), 30 September 1992 The Army also established procedures for software testing of PDSS in chapters 11, 12, 13, 14, and 15 of the same pamphlet

Page 6

7 Page 7, **Software Testing Tools** Since several tools were identified, we feel that it is significant to note the Army has developed and fielded a database, commonly referred to as the Software Metrics Management Information System (SMMIS), which uses a core set of software metrics to judge the maturity and readiness of software. The SMMIS has been distributed to over 870 program offices for use on software embedded weapon systems and automated information systems

Pages 7,8

8 Pages 8 & 9, **Better Software Practices** We agree these are good examples of effective software practices

Pages 8,9

9 Pages 9&10, **DoD Software Test and Evaluation Task Force**: The Army was actively involved in the DoD Task Force on Improved Software Test and Evaluation

Page 9

10. Page 10, **Software Test and Evaluation Procedures**, second sentence, **...the test and evaluation function did not usually participate during the requirements**: The Army concurs with this statement The current Army initiatives in software T&E evolved from findings and recommendations of the Army's Software Test and Evaluation Panel (STEP) As a result of this STEP effort, guidance and training is supplied to Army T&E managers to participate early in the software acquisition process, to include requirements generation It is also recommended that a *positive mechanism* be established at the DOD level to ensure that PMs of all services get the T&E community involved as early as possible

11 POC for this action is Mr. James P. Finfera, DSN 225-8995, COM 703-695-8995, FAX 225-9127 or 703-695-9127, e-mail james.p.finfera@pentagon-1dms18.army.mil

for John B. Foulkes
John F Gehrig
Director, Test and Evaluation
Management Agency

Department of the Air Force Comments

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE

24 JUN 1994

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING
OFFICE OF THE INSPECTOR GENERAL
DEPARTMENT OF DEFENSE

FROM: AF/TE
1650 Air Force Pentagon
Washington, DC 20330-1650

SUBJECT: DoDIG Draft Audit Report, "Software Testing During Post-Deployment Software Support of Weapon Systems," 10 Jun 94, Project No. 4RE-0007

This is in reply to your memorandum requesting the Assistant Secretary of the Air Force (Financial Management and Comptroller) provide Air Force comments on the subject report.

We appreciate the opportunity to review the subject document and provide the following comments:

a. We are concerned the auditors reviewed the wrong DoD and Services' policy documents. The auditors confused software development with software testing. Software test policy and management are defined in the Services' T&E instructions and manuals. The auditors reviewed software development, software quality, software reuse, and software support documents, which, as the auditors found, do not address software testing procedures. Enclosure 3 shows the auditors visited the Army and Navy operational test agencies (OTAs), but not the Air Force OTA which is HQ AFOTEC. If the auditors had visited AFOTEC, they would have learned how the Air Force tests software during OT&E (Atch 1) by reviewing the appropriate documents. Suggest the DoDIG delete all non-software testing discussions from the subject report (such as software development practices, cleanroom software engineering, software quality programs, software reuse programs, Software Engineering Institute Capability Maturity Model, and how a program manager funds a given project).

b. The subject report incorrectly states the DoD does not have a standard set of software metrics (Atch 2).

c. The subject report fails to point out the advantages of providing the post-deployment software support activities the flexibility to select whatever software tools best fit their needs, which allows for easy technology insertion in this fast-moving area. Additionally, it is highly unlikely many software testing tools would be applicable across all applications which were developed using a variety of software languages and design methodologies running on different hardware and operating systems/run-time environments.

d. We are concerned with the DoDIG "estimate" of $21 billion a year for post-deployment software support of weapon systems is based on an unsubstantiated DSMC "estimate" of $31 billion annual total software cost and an old early 1980s 70 percent rule of thumb for software life cycle maintenance cost. The DoDIG analysis showing the $483 million reported by the military departments seems to be more factual given the small number of lines of code required to support major weapon systems (like the referenced 230,000 lines of code to support the F-16C). The DoDIG should not base their "estimates" on others' "estimates" without fully understanding the assumptions made in the original research. Suggest the DoDIG not make "estimates" without the data to back them up. In the future, the Services should be better able to track software costs for individual systems given software has been added to the work breakdown structure.

Point of contact is Maj Sonnemann, voice DSN 225-0900 or (703) 695-0900; fax DSN 225-0803 or (703) 695-0803.

HOWARD W. LEAF
Lt Gen, USAF (Ret)
Director, Test and Evaluation

Attachments:
1. Excerpts from AFOTECP 800-2
2. OUSD(A&T) Memo, 23 May 94

cc:
SAF/FMB

Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
Comptroller of the Department of Defense
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Assistant to the Secretary of Defense (Public Affairs)

Department of the Army

Secretary of the Army
Auditor General, Department of the Army

Department of the Navy

Secretary of the Navy
Auditor General, Department of the Navy

Department of the Air Force

Secretary of the Air Force
Auditor General, Department of the Air Force

Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Logistics Agency
Director, National Security Agency
Inspector General, Central Imagery Office
Inspector General, Defense Intelligence Agency
Inspector General, National Security Agency
Director, Defense Logistics Studies Information Exchange

Non-Defense Federal Organizations

Office of Management and Budget
Technical Information Center, National Security and International Affairs Division, General Accounting Office

Non-Defense Federal Organizations (cont'd)

Chairman and Ranking Minority Member of Each of the Following Congressional Committees and Subcommittees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Subcommittee on Readiness, Committee on Armed Services
House Committee on Government Operations
House Subcommittee on Legislation and National Security, Committee on Government Operations

Audit Team Members

This report was prepared by the Readiness and Operational Support Directorate, Office of the Assistant Inspector General for Auditing, Department of Defense.

Thomas F. Gimble
Mary Lu Ugone
James W. Hutchinson
Karim Malek
JoAnn Henderson
Haskell I. Lynn
Judith A. Curry
Philip T. Davis
Suzette L. Luecke
Charlene K. Grondine
Darwin L. Webster
Nancy C. Cipolla

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Software Testing During Post-Deployment Support of Weapon Systems

B. DATE Report Downloaded From the Internet: 03/16/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 03/16/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.