

*E*valuation



*R*eport

INFORMATION ASSURANCE AT CENTRAL DESIGN ACTIVITIES

Report No. D-2001-046

February 7, 2001

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, visit the Inspector General, DoD Home Page at: www.dodig.osd.mil or contact the Secondary Reports Distribution Unit of the Audit Followup 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 Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

| | |
|---------|-----------------------------------------------------------------------------|
| AIS | Automated Information System |
| CDA | Central Design Activity |
| DAA | Designated Approving Authority |
| DITSCAP | DoD Information Technology Security Certification and Accreditation Process |
| DISA | Defense Information Systems Agency |
| IT | Information Technology |
| OMB | Office of Management and Budget |
| SRR | Security Readiness Review |
| STIG | Security Technical Implementation Guide |



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

February 7, 2001

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND,
CONTROL, COMMUNICATIONS, AND
INTELLIGENCE)
DIRECTOR, DEFENSE INFORMATION SYSTEMS
AGENCY

SUBJECT: Evaluation Report on Information Assurance at Central Design Activities
(Report No. D-2001-046)

We are providing this report for review and comment. This is the first of two reports concerning information assurance at Central Design Activities. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) comments were partially responsive on Recommendations A.1.b. and B. We request that the Assistant Secretary provide additional comments with completion dates for all corrective actions in response to the final report by April 9, 2001.

We appreciate the courtesies extended to the evaluation staff. For additional information on this report, please contact Mr. Kenneth Stavenjord at (703) 604-8952 (DSN 664-8952) (kstavenjord@dodig.osd.mil) or Mr. Dan Convis at (703) 604-8908 (DSN 664-8908) (dconvis@dodig.osd.mil). See Appendix D for the report distribution. The evaluation team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2001-046

(Project No. D2000PT-0121)

(Formerly Project No. OPT-0112)

February 7, 2001

Information Assurance at Central Design Activities

Executive Summary

Introduction. For the purpose of this evaluation, a Central Design Activity is defined as a designated organization (or segment thereof) within a component that, at a minimum, has responsibility for designing, converting, coding, testing, documenting, or subsequently maintaining or modifying computer operating or applications software for use at more than one location. For this evaluation, we visited an Army, a Navy, and an Air Force Central Design Activity.

Central Design Activities use software development environments to develop and maintain the software for which they are responsible. A software development environment is an automated information system that provides an integrated suite of tools to aid the development of software in a particular language or for a particular application.

Information assurance comprises the operations to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. Information assurance includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Objectives. This evaluation had two objectives. The first objective was to determine whether information assurance policies and management controls were working to protect the software development environments and software libraries the Central Design Activities use for DoD software development and maintenance. The second objective was to evaluate whether the controls the Central Design Activities have in place ensure that the DoD systems developed and maintained by the Central Design Activities do not contain malicious code.

Results. The three Central Design Activities we visited had not certified or accredited their software development environments as required by DoD policy. In addition, those Central Design Activities did not participate in the accreditation of software development environments created for them and housed at Defense Information Systems Agency facilities. As a result, there is an increased risk of unauthorized access to and modification of DoD software (finding A).

The management controls were inadequate to detect and remove malicious code from some software products in development at the three Central Design Activities we visited. As a result, those Central Design Activities cannot ensure that software produced by them does not contain malicious code (finding B).

Summary of Recommendations. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) update DoD Instruction 5200.40 to explicitly include software development environments as systems that need to be certified and accredited; establish a program of guidance and oversight to ensure the certification and accreditation of software development environments; establish a performance measure for designated approving authorities to report the accreditation status of software development environments; and hold periodic reviews of that performance measure, with the goal of 100 percent accreditation.

We recommend that the Commander, Defense Information Systems Agency Western Hemisphere, require Defense Enterprise Computing Center Commanders to fully involve Central Design Activity user representatives in the certification and accreditation process for software development environments that the Defense Information Systems Agency provides for Central Design Activities as well as provide Central Design Activity Commanders the details of any vulnerabilities discovered during the accreditation.

We also recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) update DoD policy to require that the development and maintenance of DoD software include a review of each new and changed line of final source code to deter, detect, and remove any malicious code.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) partially concurred with the recommendations and initiated several actions that meet their intent. The Defense Information Systems Agency concurred with the recommendations and directed the Defense Enterprise Computing Centers to involve the Central Design Activities in the Security Readiness Review process and to provide them the results of the reviews. The Assistant Secretary concurred in theory with updating DoD policy to include the review of each new and changed line of code; however, he stated that the implementation would likely exceed the available resources and may require future budgeting before implementation could begin. A discussion of management comments is in the Finding section of the report and the complete text is in the Management Comments section.

Evaluation Response. The comments from the Assistant Secretary were partially responsive. We believe the Assistant Secretary's proposed actions to determine measurements for the management of DoD software development environments and to review certification and accreditation procedures and status of DoD software development environments meet the intent of the recommendation if continued on a cyclic basis. We also believe the formal review of each new and changed line of final source code is practical. The Assistant Secretary needs to establish a time-phased approach to ensure the certification and accreditation of the DoD Component and DoD contractor software development environments, and provide a time-phased approach to updating DoD policy to require that the development and maintenance of DoD software include a review of each new and changed line of final source code. We request that the Assistant Secretary provide additional comments by April 9, 2001.

Table of Contents

| | |
|----------------------------------------------------------------------------------------|----|
| Executive Summary | i |
| Introduction | |
| Background | 1 |
| Objectives | 2 |
| Findings | |
| A. Software Development Environment Security | 3 |
| B. Malicious Code Detection | 9 |
| Appendixes | |
| A. Evaluation Process | |
| Scope and Methodology | 13 |
| Management Control Program | 14 |
| Prior Coverage | 14 |
| B. Military Department Central Design Activities | 16 |
| C. Effective Development Practices | 17 |
| D. Report Distribution | 18 |
| Management Comments | |
| Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) | 21 |
| Defense Information Systems Agency | 24 |
| Department of the Army | 27 |

Background

Central Design Activities. For the purpose of this evaluation, a Central Design Activity (CDA) is defined as a designated organization (or segment thereof) within a component that, at a minimum, has responsibility for designing, converting, coding, testing, documenting, or subsequently maintaining or modifying computer operating or applications software for use at more than one location. The Army, the Navy, and the Air Force have a total of 17 CDAs. A list of those CDAs is provided in Appendix B. For this evaluation, we visited an Army, a Navy, and an Air Force CDA. We visited the Software Development Center Lee (Army), the Fleet Material Support Office (Navy), and the Materiel Systems Group (Air Force). Other DoD agencies have CDAs also. The Marine Corps, the Defense Finance and Accounting Service, the Director for Information and Technology, and the Defense Logistics Agency list CDA organizations.

Software Development Center Lee. The Software Development Center Lee in Fort Lee, Virginia, reports to the Army Information Systems Software Center located at Fort Belvoir, Virginia. As one of the largest centralized software development centers within the Army, the Lee center employs more than 200 civilian and military personnel. The Software Development Center Lee is responsible for the development and maintenance of more than 30 automated information systems (AISs) for the Army. It produces logistics, engineering, procurement, and subsistence systems for the Army Deputy Chief of Staff for Logistics; the Defense Commissary Agency; the Army Procurement, Research and Analysis Office; and other DoD agencies.

Fleet Material Support Office. The Fleet Material Support Office in Mechanicsburg, Pennsylvania, is a major field activity of the Naval Supply Systems Command. The Fleet Material Support Office has more than 900 employees and provides information technology (IT) products and services to the Navy, DoD, and other Federal organizations. Its systems integrate supply, financial, maintenance, procurement, and other logistics functions through networks, telecommunications, and interrelated databases.

Materiel Systems Group. The Materiel Systems Group in Dayton, Ohio, is a direct reporting unit of the Electronic Systems Center, Air Force Materiel Command, Hanscom Air Force Base, Massachusetts. The Materiel Systems Group supports the Air Force information goals through acquiring, developing, maintaining, reengineering, and providing technical services for information systems. The Materiel Systems Group has 576 employees and manages more than 160 of the Air Force Materiel Command's logistics information systems.

Software Development Environments. A software development environment is an AIS that includes the facilities, hardware, software, firmware, procedures, and documentation needed to perform software development. A software development environment includes all networks and systems used for development or maintenance of a project's software. The CDAs use software development environments to develop and maintain the software for which they

are responsible. A software development environment provides an integrated suite of tools to aid the development of software in a particular language or for a particular application. Usually, the tools consist of a compiler and editor and may include a debugger and source code manager. The software development environment may also include computer-aided software engineering (CASE) tools, simulators, documentation tools, database management systems, and operating systems.

Information Assurance. Information assurance comprises the operations to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. Information assurance includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information can be erased or become inaccessible, resulting in loss of availability. When information is modified in unexpected ways, the result is a loss of integrity. A loss of integrity occurs when unauthorized changes are made to information, whether by human error or intentional tampering. To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization. Confidentiality is lost when an unauthorized person is allowed to read or copy classified information. Security is strong when the means of authentication cannot later be refuted, which is known as nonrepudiation.

Objectives

This evaluation had two objectives. The first was to determine whether information assurance policies and management controls were working to protect the software development environments and software libraries the CDAs use for DoD software development and maintenance. The second was to evaluate whether the controls the CDAs have in place ensure that the DoD systems developed and maintained by the CDAs do not contain malicious code. See Appendix A for a discussion of the scope and methodology and prior coverage.

A. Software Development Environment Security

The three CDAs we visited had not certified or accredited their software development environments as required by DoD policy. In addition, the CDAs did not participate in the accreditation of software development environments created for them and housed at Defense Information Systems Agency (DISA) facilities. Those problems occurred because of a lack of management oversight of software development environment security. As a result, there is an increased risk of unauthorized access to and modification of DoD software.

Policy Requirements for Software Development Environment Security

Office of Management and Budget Circular A-130. The Paperwork Reduction Act of 1980, Public Law 96-511, establishes the Office of Management and Budget (OMB) as responsible for developing information security policies and overseeing agency practices. The OMB provided guidance for agencies in OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," February 8, 1996. Since 1985, that circular has directed agencies to implement an adequate level of security for all AISs, ensuring effective and accurate operations as well as continuity of operations for systems that support critical agency functions.

The OMB Circular A-130, Appendix III, also specifies that a management official should authorize in writing the use of each system before beginning or significantly changing the use of the system. By authorizing use of a system, a manager accepts the risks associated with it.

DoD Directive 5200.28. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1998, provides mandatory, minimum AIS security requirements and specifies that more stringent requirements may be necessary for selected systems based on an assessment of acceptable levels of risk. It stresses the importance of a life-cycle management approach to implementing computer security requirements and applies to systems processing unclassified, sensitive-but-unclassified, and classified information. DoD Directive 5200.28 specifies that the accreditation of an AIS be supported by a certification plan, a risk analysis of the AIS in its operational environment, an evaluation of the security safeguards, and a certification report, all approved by the Designated Approving Authority (DAA). DoD Directive 5200.28 states that the AIS developer is responsible for ensuring the early and continuous involvement of the users, information system security officers, data owners, and DAAs in defining and implementing security requirements of the AIS. The directive also requires an evaluation plan for the AIS that shows progress toward meeting full compliance with stated security requirements and safeguards.

DoD Instruction 5200.40. DoD Instruction 5200.40, “DoD Information Technology Security Certification and Accreditation Process (DITSCAP),” December 30, 1997, (the DITSCAP) establishes a DoD standard infrastructure-centric approach that protects and secures the Defense Information Infrastructure. The activities presented in the DITSCAP standardize the certification and accreditation process. The four-phase process considers the system mission, environment, and architecture while assessing the impact of operation of that system on the Defense Information Infrastructure.

The DITSCAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information. It applies to any IT or information system life cycle, including the development of new IT systems, the development of prototype IT systems, the reconfiguration or upgrade of existing systems, and legacy systems.

The key to the DITSCAP is the agreement between the IT system program manager, the DAA, the Certifying Authority, and the user representative. Those managers resolve critical schedule, budget, security, functionality, and performance issues. Resolution of those issues is documented in the System Security Authorization Agreement that is used to guide and document the results of the certification and accreditation process. The objective is to use the System Security Authorization Agreement to establish a binding agreement on the level of security required before system development begins or before changes to a system are made.

Phase 3 of the process, the Validation phase, includes activities to evaluate the fully integrated system operating in a specified computing environment with an acceptable level of residual risk.

Accreditation of CDA-Housed Software Development Environments

None of the three CDAs we visited, Army Software Development Center Lee, Navy Fleet Material Support Office, and Air Force Materiel Systems Group, had developed System Security Authorization Agreements for their software development environments. Two of the three CDAs, Fleet Material Support Office and Materiel Systems Group, had not accredited their software development environments, and the third, Software Development Center Lee, had an expired accreditation letter. The Fleet Material Support Office DAA had signed an Interim Authority to Operate on December 2, 1999, that was not based on any formal process or risk assessment. Only one of the three CDAs, Software Development Center Lee, conducted periodic security exercises or vulnerability assessments to determine the adequacy of security measures and to identify security deficiencies. In summary, none of the three CDAs had accredited their software development environments nor could they provide the System Security Authorization Agreements, which document the certification and accreditation process results required by DITSCAP, for their software development environments.

Accreditation of DISA-Housed Software Development Environments

The Navy Fleet Material Support Office and the Air Force Materiel Systems Group used software development environments that were housed at DISA facilities.

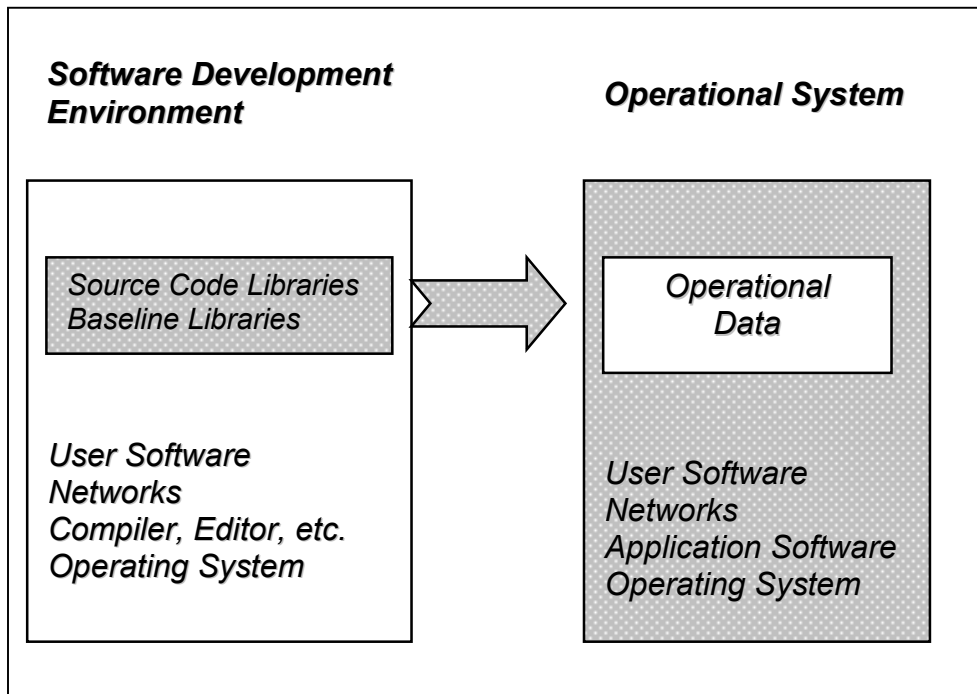
The Navy Fleet Material Support Office Interim Authority to Operate did not include the DISA housed mainframe software development environments. The Navy CDA considered the operation of the mainframe to be a DISA responsibility.

The Air Force Materiel Systems Group's software development environments housed in DISA facilities were covered by a DISA site accreditation, but that accreditation process did not include user representatives from the CDA, as required by the DITSCAP. DISA provided the Air Force CDA with a copy of the site accreditation letters for the DISA facilities, but did not provide information on vulnerabilities discovered during the accreditation process. DISA performed periodic vulnerability assessments using its Security Technical Implementation Guides (STIGs) and documented the results in a Security Readiness Review (SRR). DISA provided a summary of the results to the DISA DAA and a copy of the SRR to the DISA facility commander. DISA did not provide a copy of the SRR to the CDA and did not inform the CDA of the results of the SRR or any potential risks to the software development environments. The inclusion of the CDA user representative in the accreditation process could lead to identifying additional potential security vulnerabilities of the software development environments.

Consequences of Not Certifying and Accrediting Software Development Environments

The consequence of not conducting certification and accreditation on each software development environment is that the unique risks involved in operating each software development environment were not fully assessed. Without a comprehensive risk assessment and adjudication of those risks by the DAA, there is no balance of risk versus operational need and the system has the potential of operating at an unacceptable level of risk. That could lead to a number of problems, including unauthorized access to the software development environment, alteration or destruction of the software libraries, and use of the software development environment to exploit vulnerabilities of the network or of other systems connected to the network.

Importance of Software Development Environment Security



The figure illustrates that the software development environment is the system that supports development, builds the release materials used to deploy the new operational system, and protects the operational system while in development or maintenance. Just as the operational data depends on the security of the operational system, the confidentiality and integrity of the operational system software depends on the security of the software development environment.

Recommendations, Management Comments, and Evaluation Response

A.1. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence):

a. Update DoD Instruction 5200.40 to explicitly include software development environments as systems that need to be certified and accredited.

b. Establish a program of guidance and oversight to ensure the certification and accreditation of DoD Component and DoD contractor software development environments.

c. Establish a performance measure for designated approving authorities to report the certification and accreditation status of DoD Component and DoD contractor software development environments.

d. Hold periodic reviews of that performance measure, with the goal of 100 percent accreditation.

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) stated that the Software Management Office and the Defense-Wide Information Assurance Program are working in a coordinated effort to review all appropriate policies and, where necessary, will update those policies to address information assurance. The review will also include the possible insertion of software development environment certification and accreditation language. The Assistant Secretary agreed that a program of guidance and oversight to ensure the certification and accreditation of DoD Component and DoD contractor software development environments should exist. However, the DoD Chief Information Office does not have the resources nor the consent of the DoD Components for the operation of such a program. The DoD Chief Information Office will examine the feasibility and resources needed for a software development environment accreditation effort within the Software Management Office. The Software Management Office established a Software Metrics Integrated Product Team to determine what measurements are necessary for the adequate management of DoD software development environments. The Integrated Product Team will assign designated approving authorities to report the certification and accreditation status of DoD Component and DoD contractor software development environments as a part of the team's overall effort to improve software management. The Software Management Office, in cooperation with the Defense-Wide Information Assurance Program, will review certification and accreditation procedures and status of DoD Component and DoD contractor software development environments with a goal of 100 percent accreditation.

Evaluation Response. The Assistant Secretary's proposed actions meet the intent of Recommendations A.1.a., A.1.c., and A.1.d. The DoD Chief Information Office's examination of the feasibility and resources needed for a software development environment accreditation effort does not fully meet the intent of recommendation A.1.b. However, we believe that the proposed actions of assigning designated approving authorities to report the certification and accreditation status and the cooperative efforts of the Software Management Office and the Defense-Wide Information Assurance Program to review and maintain reports on the certification and accreditation status of DoD Component and DoD contractor software development environments would meet the intent of recommendation A.1.b. if continued on a cyclic basis.

In response to the final report, we request that the Assistant Secretary provide the estimated date those policies will be updated with software development environment certification and accreditation language; the estimated date the Software Metrics Integrated Product Team will assign designated approving authorities to report the certification and accreditation status of DoD Component and DoD contractor software development environments; the estimated

completion date for the certification and accreditation procedures and status review; and the estimated completion dates for a time-phased approach to ensure the certification and accreditation of the DoD Component and DoD contractor software development environments.

Army Comments. Although not required to comment, the Army Materiel Command nonconcurred with the recommendation to require accreditation of Central Design Activities because the Central Design Activities do not have fixed hardware and software configurations.

Evaluation Response. The recommendation was intended for the certification and accreditation of the systems used by the Central Design Activities for development and maintenance of DoD software, not for the Central Design Activities as a whole.

A.2. We recommend that the Commander, Defense Information Systems Agency Western Hemisphere, require Defense Enterprise Computing Center Commanders to:

a. Fully involve Central Design Activity user representatives in the certification and accreditation process for software development environments that the Defense Information Systems Agency provides for Central Design Activities.

b. Provide Central Design Activity Commanders the details of any vulnerabilities discovered during the accreditation of software development environments that the Defense Information Systems Agency provides for Central Design Activity customers.

Defense Information Systems Agency Comments. The Defense Information Systems Agency concurred, stating that a memorandum from the Chief, Operations Division, will be issued to the Defense Enterprise Computing Centers and Detachments, directing that the Central Design Activities be involved in the Security Readiness Review process and that the results obtained from the reviews be provided to the Central Design Activities and other customers of the platforms.

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments. The Assistant Secretary stated that the DoD Chief Information Office will request quarterly progress and status reports be sent from DISA to the Software Management Office and that the two offices will continue to work closely with each other.

B. Malicious Code Detection

The management controls were inadequate to detect and remove malicious code from some software products in development at the three CDAs we visited. Controls were inadequate because the development teams did not review final source code for malicious code and because DoD policy does not address malicious code detection and removal. As a result, the CDAs cannot ensure that software produced by them does not contain malicious code.

Malicious Code

Source Code. A programmer writes a program in a particular programming language. This form of the program is called the source program or, more generically, source code. Source code is the only format that is readable by humans. When you purchase programs, you usually receive them in their machine-language format. That means you can execute the programs directly, but you cannot read or modify them.

Malicious Code. The National Information Systems Security (INFOSEC) Glossary defines malicious code as software or firmware capable of performing an unauthorized function on an information system. Malicious code includes viruses, worms, Trojan horses, logic bombs, and other “uninvited” software.

Risk of Malicious Code. In the world of personal computers, “Easter eggs” are the name given creative gimmicks that programmers have hidden inside some popular desktop applications and hardware. They are called Easter eggs after the U.S. tradition of parents hiding eggs for their children to find. As programmers’ work is often uncredited, they may sneak their names into the programs with Easter eggs.

By definition, Easter eggs are not damaging; however, Trojan horses, logic bombs, worms, and other malicious code can be hidden just as easily and later activated to cause damage to the system or to data. It is just as simple to put in a backdoor to a computer system, allowing unauthorized access at a later date for anything from stealing funds to spying. Once installed, malicious code is extremely hard to find because it can be small and hidden in the application. Detection methods require access to the source code, tools, experience with the programming language, and system knowledge.

Malicious Code Policy

We could find no DoD policy reference to “Malicious Code.” However, asset protection and data integrity are frequently referenced. DoD Directive 5010.38, “Management Control (MC) Program,” August 26, 1996, requires each DoD component to implement a comprehensive system of management controls that

provides reasonable assurance that assets are safeguarded against waste, loss, unauthorized use, and misappropriation. DoD Directive 5200.28 requires safeguards to be in place to detect and minimize inadvertent modification or destruction of data and to detect and prevent malicious destruction or modification of data. The CDA software libraries are DoD assets and the source code they contain are data.

Controls for Detecting and Removing Malicious Code

The three CDAs we visited had weak physical access controls to the programmer work areas. There were good procedures for adding and removing software development environment users, but no process that verified that the access list was correct and that the access activity was as expected. We evaluated projects where team passwords could be captured and used by someone else, tools were not used to highlight code changes, and code reviews checked only selected modules for correct function. In summary, the management controls on those projects were inadequate to deter, detect, and remove malicious code.

Effective Detection Practices. A software development organization with a repeatable and defined development process uses commercial tools, documented processes, and trained teams to consistently produce quality software. It uses separation of duties and development practices to limit the opportunities for malicious code to be inserted without detection. The following development practices help deter and detect malicious code.

- Configuration management tools and procedures.
- Formal peer reviews.
- Coding standards checking.
- New and changed code reviews.
- Software quality assurance monitoring.

See Appendix C for details on those development practices.

An Example of a Good Process. We interviewed one project team with very good management control processes, though they were project specific and not consistent throughout the CDA. There was open access to the programmer work areas, but the servers with the software libraries were in locked rooms. At the start of each maintenance cycle, the last version of the system is used to create a test environment. When the code required an update, a design document was created with a description of the changes to be made to the code. After approval of the design document, the code to be changed was copied from the test environment to a floppy disk for the programmer. The code on the floppy is the only code that the programmer can change, though the programmer has read-only access to the entire test environment.

The programmer then completes the necessary changes and returns the floppy with the new code to the lead programmer. The new code is then compared to the original code using a text compare tool that highlights the changes. The lead programmer checks that the changes described in the design document were made and that no additional changes took place. The lead programmer uploads the new code to the test environment where it is tested for operation errors. After the new version is tested, the test environment is uploaded to the baseline library and the new baseline saved to compact disk. Access to the baseline library is limited to the lead programmer and an assistant. Virus detection runs every 2 hours on the test environment and the baseline. A security log is kept to track hacking attempts.

Using a floppy to provide the programmers the code that they update effectively limits programmers' access to only their assigned modules and compensates for the lack of physical access controls. The current lead programmer had been working on that project's system for many years and had reviewed nearly all of the system's code. The lead programmer would detect any malicious code when reviewing the changed code, which is a deterrent to the entry of malicious code.

Summary

Programmer access controls were weak in most cases. Therefore, there was a need for controls over code changes to be robust, but most were not. Even so, code review teams reviewing each new and changed line of the final source code could have detected and removed malicious code. However, this was not done consistently. As a result, the CDAs cannot ensure that their software products do not contain malicious code.

Recommendation, Management Comments, and Evaluation Response

B. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) update DoD policy to require that the development and maintenance of DoD software include a review of each new and changed line of final source code to deter, detect, and remove any malicious code.

Management Comments. The Assistant Secretary concurred with the recommendation in theory. The Assistant Secretary stated that the implementation of this recommendation would likely exceed the resources of the Central Design Activities, the program managers, and the Component Chief Information Offices. The Software Management Office will examine the feasibility of the code inspection tools and applications that can review each new and changed line of final source code for malicious code; however, such tools may not be adequate to the task or may require future budgeting before

implementation could occur. In addition, the Assistant Secretary stated that a formal review of source code in commercial off-the-shelf products is not possible.

Evaluation Response. The Assistant Secretary's comments were not fully responsive. The formal review of each new and changed line of final source code is possible and practical. Some project teams already perform malicious code reviews. Project teams could also include malicious code review in their formal peer reviews, if the reviewed source code was saved and protected. There are configuration management and other inspection tools available that can identify new and changed lines of source code by comparison of current versions to saved versions. Only the first code baseline would need a complete review. We agree that commercial off-the-shelf software products cannot be reviewed in the same way; however, known commercial off-the-shelf vulnerabilities are currently tracked and reported by the Computer Emergency Response Teams and the National Institute of Standards and Technology. In response to the final report, we request that the Assistant Secretary reconsider his comments and provide a time-phased approach to implementing the recommendation.

Appendix A. Evaluation Process

Scope and Methodology

Work Performed. We reviewed and evaluated information assurance controls for software development environments at three CDAs. At the selected CDAs, we evaluated the implemented policy and general controls that protect software development environments and software libraries used to develop and maintain DoD systems. We also evaluated the controls that the CDAs had in place to identify and remove malicious code. We developed a questionnaire to help collect information and documentation from the CDAs. We also selected two active projects at each CDA and met with the project teams. We used the questionnaire responses and discussions with officials from the CDAs to evaluate their controls for protecting their software development environments and software libraries. We used the discussions with the project teams to evaluate the controls in place to identify and remove malicious code.

DoD-Wide Corporate Level Government Performance and Results Act (GPRA) Coverage. In response to the GPRA, the Secretary of Defense annually establishes DoD-wide corporate level goals, subordinate performance goals, and performance measures. This report pertains to achievement of the following goal:

FY 2000 DoD Corporate Level Goal 2: Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineer the Department to achieve a 21st century infrastructure. **(00-DoD-2)**

DoD Functional Area Reform Goals. Most DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objectives and goals:

- **Information Technology Management Area. Objective:** Ensure DoD's vital information resources are secure and protected.
Goal: Build information assurance framework. **(ITM-4.1)**
- **Information Technology Management Area. Objective:** Ensure DoD's vital information resources are secure and protected.
Goal: Build information assurance architecture and supporting services. **(ITM-4.2)**
- **Information Technology Management Area. Objective:** Ensure DoD's vital information resources are secure and protected.
Goal: Improve acquisition processes and regulations. **(ITM-4.3)**

-
- **Information Technology Management Area. Objective:** Ensure DoD's vital information resources are secure and protected.
Goal: Assess information assurance posture of DoD operational systems. (ITM-4.4)

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the DoD. This report provides coverage of the Information Management and Technology high-risk area.

Use of Computer-Processed Data. We did not use computer-processed data to perform this evaluation.

Evaluation Type, Dates, and Standards. We performed this economy and efficiency evaluation from November 1999 through July 2000 in accordance with standards implemented by the Inspector General, DoD.

Contacts During the Evaluation. We visited or contacted individuals and organizations within DoD. Further details are available on request.

Management Control Program

DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, requires DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of Review of Management Controls. We did not review the management control program related to the overall evaluation objectives because DoD recognized Information Assurance as a material management control weakness area in the FY 1999 Annual Statement of Assurance. However, we did review the adequacy of management controls for protecting software development environments used by the CDAs to develop and maintain DoD software (see the Finding section).

Prior Coverage

No prior coverage directly related to our evaluation objectives has been conducted during the last 5 years. However, there have been numerous reports related to information assurance in general. Two Inspector General, DoD, reports summarize all of the General Accounting Office and DoD audit reports issued on information assurance from January 1, 1995, through March 31, 2000. Unrestricted Inspector General, DoD, reports can be accessed over the Internet at <http://www.dodig.osd.mil/audit/reports>.

Inspector General, DoD

Inspector General, DoD, Report No. D-2000-124, "Information Assurance Challenges—A Summary of Audit Results Reported December 1, 1998, through March 31, 2000," May 15, 2000.

Inspector General, DoD, Report No. 99-069, "Summary of Audit Results—DoD Information Assurance Challenges," January 22, 1999.

Appendix B. Military Department Central Design Activities

Central Design Activities

For the purpose of this evaluation, a CDA is defined as a designated organization (or segment thereof) within a component that, at a minimum, has responsibility for designing, converting, coding, testing, documenting, or subsequently maintaining or modifying computer operating or applications software for use at more than one location.

While each Military Department's definition of a CDA may vary slightly from the definition above, they each identified their CDAs (see table below) and noted that they had other software development groups that were not CDAs. Those other software development groups are not considered CDAs because they support software only for the business area organization they belong to, as opposed to more than one location as our definition of CDAs requires.

Military Department Central Design Activities

Army

- Logistics Systems Support Center
- Industrial Logistics Systems Center
- Software Development Center Washington
- Software Development Center Lee
- Army Total Personnel Command

Navy

- Bureau of Naval Personnel
- Fleet Material Support Office
- Naval Aviation Depot Operations Center
- Naval Computer and Telecommunications Area Master Station, Atlantic
- Naval Computer and Telecommunications Station, Jacksonville
- Naval Computer and Telecommunications Station, Pensacola
- Naval Computer and Telecommunications Station, Washington
- Naval Education and Training Professional Development and Technology Center
- Naval Reserve Information Systems Office

Air Force

- Materiel Systems Group
- Standard Systems Group

Appendix C. Effective Development Practices

A software development organization with a repeatable and defined development process uses commercial tools, documented processes, and trained teams to ensure it produces quality software. It uses separation of duties and development practices to limit the opportunities for malicious code to be inserted without detection. The following are some of the development practices used to guard against the insertion of malicious code.

Configuration Management Tools and Procedures. Configuration management is the means by which the content, change, or status of shared information within a project is managed and controlled. The purpose of configuration management is to establish and maintain the integrity and control of software products. No new code can be written without a change authorization. Configuration management tools also limit access to final versions of code.

Formal Peer Reviews. Configuration management and formal peer review are software development best practices identified by the DoD Software Acquisition Best Practices Initiative. Formal peer reviews use a trained team approach to ensure that the program design is correctly implemented. Technical documentation and code are inspected. Formal peer reviews can eliminate approximately 80 percent of all software defects.

Coding Standards Checking. Depending on the computer language, there are software tools that can analyze source code to check that programming standards have been followed, that all variables are used, and that there is no dead (inaccessible) code. Use of standards checking tools can quickly identify code that does not follow organizational coding standards.

New and Changed Code Reviews. The change management features of a configuration management tool or a separate text compare tool can highlight the changes in an updated module by comparing it to the original baseline module. Changes can then be reviewed for code defects, standards violations, and malicious code.

Software Quality Assurance Monitoring. Software quality assurance consists of an independent team of people that monitors changes to the baseline throughout the development process. Software quality assurance involves regular reviews throughout the development process to ensure that any defects built into the code are detected as early as possible. The software quality assurance team works to verify the implementation of standards and processes that would help detect malicious code.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller)
 Deputy Chief Financial Officer
 Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
 Deputy Assistant Secretary of Defense, Deputy Chief Information Officer
 Deputy Assistant Secretary of Defense, Security and Information Operations
 Director, Infrastructure and Information Assurance
 Director, Policy Integration and Operations

Joint Staff

Director, Joint Staff
 Director, Operations
 Director, Command, Control, Communications, and Computers

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Commanding General, Army Communications and Electronics Command
 Commander, Software Development Center Lee
Auditor General, Department of the Army

Department of the Navy

Commander, Naval Supply Systems Command
 Commanding Officer, Fleet Material Support Office
Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Commander, Air Force Materiel Command
 Executive Director, Materiel Systems Group
Inspector General, Department of the Air Force
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
 Commander, Defense Information Systems Agency Western Hemisphere
Director, Defense Logistics Agency
Director, National Security Agency
 Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency

Non-Defense Federal Organizations

Office of Management and Budget
 Office of the Information and Regulatory Affairs
General Accounting Office
 Director, Defense Information and Financial Management Systems, Accounting and
 Information Management Division

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

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 Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology,
 Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International
 Relations, Committee on Government Reform

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments



COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

NOV 30 2000

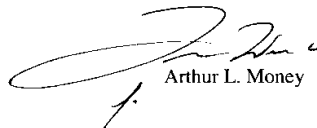


MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Proposed Inspector General Report "Information Assurance at
Central Design Activities," Project No. D2000PT-0121, August 21, 2000

Thank you for the opportunity to review the Office of the Inspector General (OIG) report titled: "Information Assurance at Central Design Activities," Project No. D2000PT-0121. The Department of Defense Chief Information Officer is pleased with the OIG efforts in bringing the information assurance risks associated with the Central Design Activities to our attention. Our past and continued cooperative relationship is vital to the continued improvement and advancement of information technologies in a manner which continues to provide our warfighters with the information superiority they need, while ensuring the safety and reliability of the information systems upon which they rely.

We concur with the OIG's assessments and particularly appreciate your raising the issue of information assurance and software code. The draft report has recommendations that we would like to take the opportunity to address individually. The attachment provides our comments on each of the recommendations.


Arthur L. Money

Attachment



ATTACHEMENT

Recommendation

A.1 "We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence):

- a. Update DoD Instruction 5200.40 to explicitly include software development environments as systems that need to be certified and accredited.
- b. Establish a program of guidance and oversight to ensure the certification and accreditation of DoD Component and DoD contractor software development environments.
- c. Establish a performance measure for designated approving authorities to report the certification and accreditation status of DoD Component and DoD contractor software development environments.
- d. Hold periodic reviews of that performance measure, with the goal of 100 percent accreditation."

Response: One of the highest priorities of the Software Management Office is the review of all applicable DoD Directives and Instructions in the 5000 and 8000 series for applicability to software development, process improvement, and management. The Software Management Office will be working closely with the Defense-Wide Information Assurance Program (DIAP) in a coordinated effort, to see that all the appropriate policies are reviewed and where necessary, updated to address information assurance. Part of the review will be the possible insertion of software development environment certification and accreditation language. We agree that ideally, a program of guidance and oversight to ensure the certification and accreditation of DoD Component and DoD contractor software development environments should exist. However, currently the CIO does not have the resources nor the consent of the DoD Components for the operation of such a program. The CIO will examine the feasibility and resources needed for a software development environment accreditation effort within the Software Management Office.

It is the position of the CIO that performance measures are key for proper management of all aspects of software development. The Software Management Office has established a Software Metrics Integrated Product Team (IPT) which is chartered to determine what measurements are necessary for the adequate management of DoD's software environments. Part of the IPT's effort will be to examine what measures are needed to ensure information assurance in our software. The IPT will assign designated approving authorities to report the certification and accreditation status of DoD Component and DoD contractor software development environments as a part of their overall effort to improve software management.

The Software Management Office, in cooperation with the DIAP, will review certification and accreditation procedures and status of DoD Component and DoD contractor software development environments and will strive for a goal of 100 percent accreditation despite the increasing amount of commercial-off-the-shelf (COTS) software being used in the Department. The Software Management Office has as its highest priority an overall examination of security

and information assurance, for both internally developed software and COTS products used in DoD.

Recommendation

A.2 “We recommend that the Commander, Defense Information Systems Agency (DISA) Western Hemisphere, require Defense Enterprise Computing Center Commanders to:

- a. Fully involve Central Design Activities user representatives in the certification and accreditation process for software development environments that the DISA provides for Central Design Activities.
- b. Provide Central Design Activity Commanders the details of any vulnerabilities discovered during the accreditation of software development environments that DISA provides for Central Design Activity customers.

Response: The DoD CIO fully concurs with these recommendations and will request quarterly progress and status reports be sent from DISA to the DoD CIO Software Management Office and that the two offices will continue to work closely with each other in the future.

Recommendation

B. “We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) update DoD policy to require that the development and maintenance of DoD software include a review of each new and changed line of final source code to deter, detect, and remove any malicious code.”

Response: The DoD CIO concurs with this recommendation in theory. However, the implementation of this effort would likely exceed the resources and capabilities of the Central Design Activities, the program managers and the Component CIOs. The Software Management Office will be examining the feasibility of the code inspection tools and applications that can review each new and changed line of final source code to deter, detect, and remove any malicious code. However, such tools--should they be adequate to the task--are expensive and may require future budgeting and insertion in the POM cycle before implementation could occur.

A formal review of each new and changed line of final source code to deter, detect, and remove any malicious code in COTS products is not possible. Alternative means to deter, detect, and remove any malicious code in COTS products will need to be examined.

Defense Information Systems Agency Comments



IN REPLY
REFER TO:

Inspector General (IG)

8 November 2000

DEFENSE INFORMATION SYSTEMS AGENCY


701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
(ATTN: AUDIT FOLLOWUP AND TECHNICAL SUPPORT
DIRECTORATE)

SUBJECT: Response to DoD IG Draft Report, "Information
Assurance at Central Design Activities," August 21,
2000 (DoD IG Project D2000PT-0121, formerly project
OPT-0112)

1. The attached enclosure provides general comments from the
Defense Information Systems Agency on the above referenced DoD
IG Draft Report.

2. If you have any questions, please call Jason Bakker, at
(703) 607-6607.


RICHARD T. RACE
Inspector General

Enclosure a/s

Quality Information for a Strong Defense

INTEROFFICE MEMORANDUM

TO: INSPECTOR GENERAL (IG)
FROM: Business Management Division (WE05)
DATE: 8 November 2000
SUBJECT: DOD IG Draft Report, Information Assurance at
Central Design Activities (Project D2000PT-0121,
formerly project OPT-0112)
Preparer: S. Burns/WE03/(703) 681-2286/sb

1. The subject audit was conducted by the DOD Inspector General's office to determine whether information assurance policies and management controls were working to protect the software development environments and software libraries that the Central Design Activities (CDAs) use for DOD systems development and maintenance.

There were two WESTHEM findings, Recommendations A.2a and A.2b, that the DOD IG has requested DISA to comment on.

A.2.a Fully involve Central Design Activity user representatives in the certification and accreditation process for software development environments that the Defense Information Systems Agency provides for Central Design Activities.

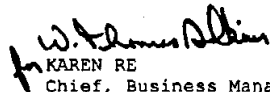
DISA WESTHEM distinguishes between the CDA responsibility and the WESTHEM responsibility for the certification and accreditation of a software development environment. The CDA is responsible for the certification and accreditation of the application. WESTHEM is responsible for the certification and accreditation of the hardware and facilities. WESTHEM conducts Security Readiness Reviews (SRRs) on all platforms. WESTHEM concurs with the inclusion of CDAs in the SRR process. A memorandum from the Chief, Operations Division will be issued to the Defense Enterprise Computing Centers (DECCs) and Detachments by 17 November 2000 directing that the CDAs be involved in the SSR process and get a copy of the results.

SUBJECT: DOD IG Draft Report, Information Assurance at
Central Design Activities (Project D2000PT-0121, formerly
project OPT-0112)

A.2.b. Provide Design Activity Commanders the details
of any vulnerabilities discovered during the accreditation
of the software development environments that the Defense
Information Systems Agency provides for Central Design
Activity customers.

WESTHEM concurs and the results obtained from the SRRs will
be provided to the CDAs and other customers of the
platforms. The memorandum to the DECCs and Detachments
will have an effective date of 1 December 2000.

2. Our point of contact for this audit is Ms. Sandy Burns,
WE03, (703)681-2286.


for KAREN RE
Chief, Business Management
Division

Copy to:
FSO

Department of the Army Comments



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MATERIEL COMMAND
5001 EISENHOWER AVENUE, ALEXANDRIA, VA 22333 - 0001

4 - DEC 2000

AMCIO-F (380-19a)

MEMORANDUM FOR THE OFFICE OF THE INSPECTOR GENERAL,
DEPARTMENT OF DEFENSE, ATTN: OASIG-AUD,
400 ARMY NAVY DRIVE (ROOM 801), ARLINGTON,
VA 22202-2885

SUBJECT: U.S. Army Materiel Command Comments on the Draft
of a Proposed Evaluation Report - Information Assurance at
Central Designed Activities (CDA)

1. Reference, Draft of a Proposed Evaluation Report
Information Assurance at Central Design Activities (CDA),
21 Aug 00, prepared by the Office of the Inspector General,
Department of Defense.

2. The referenced document has been reviewed and the
comments listed below are provided for your consideration.
The document is currently being staffed through the Software
Engineering Center (SEC) at CECOM to the CDAs.
As a result, additional comments may be provided.

a. In order to accredit the CDAs under the DITSCAP,
they would need to have a fixed hardware and software
configuration. As a result, we non-concur with the
recommendation to require accreditation of CDAs. The
development environment does not lend itself to the
accreditation process.

b. The DITSCAP requires re-accreditation when
significant changes are made to the existing environment.
In a CDA environment hardware and software configurations
are changed frequently. This enables testing of software
under various conditions for the many environments under
which it will need to operate. This capability is necessary
to ensure that the software will function properly when
released.

AMCIO-F

SUBJECT: U.S. Army Materiel Command Comments on the Draft of a Proposed Evaluation Report - Information Assurance at Central Designed Activities

c. While there are valid observations regarding Information Assurance at the CDAs in the referenced document, we believe that alternative measures can be taken to address the situation, such as a DOD level policy directing the security measures that must be implemented at CDAs.

d. Page 2, 3rd paragraph states "Confidentiality is lost when an unauthorized person is allowed to read or copy classified information". Suggest this sentence be changed as follows: "Confidentiality is lost when an unauthorized person is allowed to read or copy information no matter what the classification of the data."

e. Page 4, 1st paragraph states the date of DoD Instruction 5200.40 is "30 December 1997". There is an updated copy and it was officially signed off on 10 Feb 98.

f. Page 14, Table - Military Department Central Design Activities. The Army Materiel Command - Headquarters is not an Army CDA. The Logisitcs, Systems Support Center, Industrial Logistics Systems Center, Software Development Center Washington, and Software Development Center Lee are the designated organizations within a component (which is Headquarters AMC) that are CDA. Suggest you use Army Materiel Command - Headquarters as a heading and place the CDA's mentioned under us.

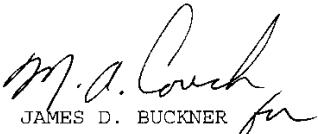
AMCIO-F

SUBJECT: U.S. Army Materiel Command Comments on the Draft
of a Proposed Evaluation Report - Information Assurance at
Central Designed Activities

3. Point of contact for this action is Lucille Newman,
DSN 767-3310, commercial (703) 617-3310, ncwmanl@hqamc.army.mil

4. AMC --Army Readiness Command...Supporting Every Soldier Every Day.

FOR THE COMMANDER:


JAMES D. BUCKNER *for*
Chief Information Officer

Evaluation Team Members

The Audit Followup and Technical Support Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector, DoD, who contributed to the report are listed below.

David A. Brinkman
Kenneth H. Stavenjord
Dan B. Convis
Michael D. Walker
Benzad B. Akavan
James B. Mitchell
Kevin W. Klein