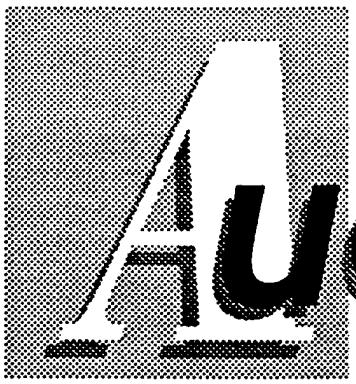

OFFICE OF THE INSPECTOR GENERAL

FOLLOWUP AUDIT OF CONTROLS OVER OPERATING SYSTEM AND SECURITY SOFTWARE ON COMPUTER SYSTEMS AT DEFENSE MEGACENTER, MECHANICSBURG, PENNSYLVANIA

Report No. 96-179 June 27, 1996

19991126 041

Department of Defense

AQI 00-02-0549

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Analysis, 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 of the Analysis, 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:

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

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 the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

AFAA	Air Force Audit Agency
DLA	Defense Logistics Agency
DFAS	Defense Finance and Accounting Service
DIPC	Defense Information Processing Center
DISA	Defense Information Systems Agency
DMC	Defense Megacenter
IBM	International Business Machines Corporation
IG	Inspector General
CA-IDMS	Computer Associates, Inc., Integrated Data Management System
NAVICP	Naval Inventory Control Point
SVC	Supervisor Call
WESTHEM	Western Hemisphere

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

June 27, 1996

MEMORANDUM FOR ASSISTANT SECRETARY OF THE NAVY (FINANCIAL MANAGEMENT AND COMPTROLLER)
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Audit Report on Followup Audit of Controls Over Operating System and Security Software on Computer Systems at Defense Megacenter, Mechanicsburg, Pennsylvania (Report No. 96-179)

We are providing this report for information and use. We considered management comments on a draft of this report in preparing the final report.

Comments on a draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to our audit staff. Questions about the audit should be directed to Mr. David C. Funk, Audit Program Director, at (303) 676-7445 (DSN 926-7445), or Mr. W. Andy Cooley, Audit Project Manager, at (303) 676-7393 (DSN 926-7393). See Appendix E for the report distribution. The audit 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. 96-179 **June 27, 1996**
(Project No. 5FD-2030)

Followup Audit of Controls Over Operating System and Security Software on Computer Systems at Defense Megacenter, Mechanicsburg, Pennsylvania

Executive Summary

Introduction. This audit was made to evaluate actions taken by the Defense Information Systems Agency and Naval Supply Systems Command in response to prior audits of computer security and other general controls. The audit was performed at the Defense Megacenter and the Naval Inventory Control Point in Mechanicsburg, Pennsylvania. The audit focused on the security software, operating system, and the database management system supporting the Navy PX06 Inventory Accounting and Billing application.

Audit Objective. Our objective was to determine whether corrective actions taken or planned by the Defense Megacenter and Naval Inventory Control Point to improve general controls adequately responded to the 11 recommendations made in Inspector General, DoD, Report No. 95-066, "Controls Over Application Software Supporting the Navy's Inventories Held For Sale (Net)," December 30, 1994.

Audit Results. The Defense Megacenter and the Naval Inventory Control Point had fully implemented 7 of the 11 recommendations. However, additional corrective actions were required on 4 recommendations to improve general controls over the operating system and database management system. Specifically, weaknesses existed in the controls over supervisor calls, sensitive utilities, and the database management system on the test and production systems supporting the PX06 application at the Defense Megacenter and Naval Inventory Control Point. Inadequate general controls made it possible for knowledgeable users to improperly access, modify, or destroy computer data and programs without detection. The inadequate controls over supervisor calls were a material weakness. The results of this audit are detailed in Part I of the report.

Because of their sensitive nature, the deficiencies discussed in this report are presented in general terms only; specific details of the findings were separately provided to management.

Summary of Recommendations, Management Comments, and Audit Response. We recommend that controls over supervisor calls be improved, that sensitive utilities be defined to the security software, and that access be limited to the database management system supporting the PX06 Inventory Accounting and Billing application software. Implementing the recommendations made in this report will complete the corrective actions required in response to the prior recommendations. The Navy and Defense Information Systems Agency concurred with the recommendations. The planned correctives actions were fully responsive, so no additional comments are required on this report. See Part III for the complete text of management's comments.

Table of Contents

Part I - Audit Results

Audit Background

Computer Security. During FYs 1990 through 1994, the Inspector General (IG), DoD, and the Air Force Audit Agency (AFAA) performed a series of five audits to evaluate the controls over operating system and security software and other general controls for computer systems supporting the Defense Finance and Accounting Service (DFAS). As detailed in Appendix B, the audits determined that financial computer systems critical to DoD were exposed to fraud and other risks. Knowledgeable users could exploit weaknesses in the operating system controls to improperly access, add, modify, or destroy sensitive computer data, programs, and other resources (accidentally or intentionally) without risk of detection.

Congressional and DoD Oversight. Heightened concern over DoD computer security surfaced during FY 1994. As a result, the IG, DoD, was asked to follow up on prior computer security audits. In April 1994, the Deputy IG, DoD, testified on Defense Financial management issues before the Senate Governmental Affairs Committee. The Deputy IG advised the committee that inadequate controls over computer security were among several high-risk problems requiring the immediate attention of DoD. In May 1994, the Committee Chairmen requested that the IG, DoD, closely monitor DoD efforts to correct weaknesses in computer security and other financial management problems.

Also in April 1994, the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) requested a briefing on computer security from the IG, DoD. As a result of that briefing and directions from the Assistant Secretary, the Defense Information Systems Agency (DISA) created a task force on information security to improve information systems security at all Defense megacenters, including the computer centers that were being consolidated into those Defense megacenters. One of the DISA task force objectives was reviewing and implementing prior audit recommendations related to computer security at those sites.

In June 1994, the Senior Financial Management Oversight Council, chaired by the Deputy Secretary of Defense, was briefed on the computer security of DoD financial management systems. Among other actions, the Deputy Secretary of Defense directed DISA to ensure that problems on computer security were corrected. The Deputy Secretary of Defense also stated that the IG, DoD, needed to provide oversight to ensure that computer security was improved.

Audit Request. On July 12, 1994, in response to directions from the Deputy Secretary of Defense, the Under Secretary of Defense (Comptroller) and the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) requested that the IG, DoD, confirm that DFAS and DISA had corrected the previously reported problems with computer security. The IG, DoD, expanded the audit scope to include evaluating corrective actions taken by

the Defense Logistics Agency (DLA) in response to those prior IG, DoD, reports and by DISA in response to a prior report issued by the AFAA.

Followup Completed. In response to the audit request, we issued three reports on the followup completed at DFAS, DISA, and DLA:

o Report No. 95-263, "Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service," June 29, 1995,

o Report No. 95-270, "Corrective Actions on System and Software Security Deficiencies," June 30, 1995, and

o Report No. 96-053, "Followup Audit of Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service, January 3, 1996."

Current Followup. Shortly after the audit request, the IG, DoD, issued Report No. 95-066, "Controls Over Application Software Supporting the Navy's Inventories Held For Sale (Net)," December 30, 1994. Followup on that report was delayed to allow management an opportunity to implement the audit recommendations. The current report summarizes the audit of corrective actions by the Defense Megacenter (DMC)-Mechanicsburg and the Naval Inventory Control Point (NAVICP)* at Mechanicsburg, Pennsylvania, in response to 11 recommendations made in Report No. 95-066. The prior audit identified opportunities for improving the computer security over the Navy PX06 Inventory Accounting and Billing application. This application was installed on the PX06 Production-Only System (the Production System) and the Development and Test Guest System (the Test System). The prior audit determined that general controls needed to be improved over the:

o Resource Access Control Facility (the Security Software) used to control access to the operating systems,

o Multiple Virtual Storage/Extended Architecture operating system software (the Operating System) used to control the execution of the computer programs, and

o Computer Associates, Inc., Integrated Data Management System (CA-IDMS), which was the database management system used to support the Production and Test Systems.

Technical Terms. See Appendix C, "Glossary," for definitions of the technical terms used in this report.

*In Oct 1995, the Navy Ships Parts Control Center was renamed the Naval Inventory Control Point.

Audit Objective

The objective of our audit was to determine whether corrective actions taken or planned by DMC-Mechanicsburg and NAVICP to improve computer security adequately responded to the recommendations made in IG, DoD, Report No. 95-066.

See Appendix A for a discussion of the scope and methodology and Appendix B for a discussion of prior audit coverage.

General Controls

The DMC-Mechanicsburg and NAVICP fully implemented 7 of 11 prior recommendations made to improve the general controls over the Security Software, Operating System, and the CA-IDMS data base supporting the PX06 Production and Test Systems. However, additional corrective actions were needed to fully implement four recommendations.

o At the DMC-Mechanicsburg, the integrity of one, locally developed supervisor call (SVC) had not been verified, two other supervisor calls with integrity exposures were still in use, and sensitive utilities were not adequately protected.

o At NAVICP, database administrators had not fully implemented access controls over CA-IDMS data bases.

These weaknesses in the Security Software, Operating System, and CA-IDMS database management system resulted because managers at DMC-Mechanicsburg and NAVICP assigned a higher priority to other work requirements and were not aware of the sensitivity of certain programs. As a result, PX06 application programs and inventory data could be added, modified, or deleted without detection, and the integrity of systems was not ensured. The inadequate control over supervisor calls on the Operating System was a material weakness in management controls.

Supervisor Calls

Use and Control. A supervisor call is a computer instruction that interrupts a program being executed and passes control so that a specific function can be performed in the Operating System. Such functions can be sensitive and must be controlled. For example, an SVC may without detection open a file for read or write access. SVCs may be controlled by requiring the vendor supplying the SVC (or other independent sources for locally written SVCs) to provide written assurance to the integrity of the SVC and by using Security Software to limit access to individual SVCs.

Corrective Actions. Prior to the audit, system programmers deleted or properly installed 8 of the 17 SVCs previously reported as presenting significant exposure risks to system integrity. During the audit, DMC-Mechanicsburg properly installed 3 more of those 17 SVCs. A new SVC exposure identified during the audit was also eliminated. However, additional corrective actions were needed.

System and Application Integrity. Six user/vendor SVCs (three each on two systems) installed on the Test and Production Systems at DMC-Mechanicsburg could compromise the integrity of the Operating System and application data.

o One SVC with an integrity exposure on both the Test and Production Systems was rewritten; however, there was no review of that SVC by an independent source vouching for the integrity of the SVC. No independent integrity review was conducted because DISA-WESTHEM standards did not require that such reviews be conducted on locally developed SVCs.

o A second SVC on both systems was not correctly installed. System programmers delayed reinstallation while they evaluated whether the SVC should be deleted or reinstalled.

o A third SVC had been identified in the prior audit as an exposure on the Test and Production Systems. However, the SVC was still in use despite the fact that the vendor no longer supported that version of the SVC on the Operating System used by the two systems. DMC-Mechanicsburg personnel said the Operating Systems would be upgraded later this year, allowing them to install an SVC with no integrity exposure. Management personnel indicated that their migration work load prevented upgrading the current Operating System.

The lack of an integrity review of the SVC and the integrity exposures could allow a knowledgeable user to bypass normal controls on the Operating System and Security Software. Thus, the user could add, modify, or delete system data.

Sensitive Utilities

Use and Control. Sensitive utility programs provide general support for computer processes, such as creating test data or copying data from one storage device to another. The utilities become sensitive when they can bypass the computer system's security software or internal controls and, thereby, could destroy data if not used properly.

Security Status. Three sensitive utilities (two on the Test System and one on the Production System) were not adequately controlled, as discussed below.

o The DMC-Mechanicsburg used the Security Software to limit access to some sensitive utilities on both the Production and Test Systems but did not secure the one previously reported on the Test System. During the audit, DMC-Mechanicsburg secured this sensitive utility.

o Access was not adequately limited to another sensitive utility installed on both the Production and Test Systems. This utility was not adequately secured because it was not one of the programs identified as requiring control by the "DISA WESTHEM MVS Security Technical Implementation Standards," September 1995. However, the utility had similar functions to the other sensitive programs identified as sensitive by these standards.

We alerted the Director, DMC-Mechanicsburg, to these security weaknesses in our memorandum, Subject: "Technical Information on Draft Audit Report, 'Application Controls Over Application Software Supporting the Navy's Inventories Held for Sale (Net)' (Project No. 3FD-2025)," September 21, 1994. Because sensitive utilities can be used to add, delete, or change programs and accounting data, they must be adequately controlled.

Database Access Controls

Database Management System. The CA-IDMS database management system used by NAVICP to support the Production System controls and organizes all data used by the PX06 application. The CA-IDMS software must be properly installed to adequately limit user access to the PX06 Production System and data base.

Access Controls. Access to CA-IDMS database libraries was not adequately controlled on the Production System, as detailed below.

o Since our prior audit, a new version of CA-IDMS had been installed featuring a new sign-on security option. The security option eliminated over 3,800 batch users that could update the data base. However, there were still too many user IDs (over 850) with the batch and CA-IDMS sign-on capabilities on the Production System. Although of low risk, with their read access to certain CA-IDMS libraries, those 850 user IDs could make unauthorized changes to the data base.

o In addition, excessive access was given to the database libraries because over 140 user IDs could update them. Database administrators at NAVICP were not aware of the magnitude of user access to the data bases and agreed that access should be limited. During the audit, NAVICP personnel developed Security Software modifications to limit access to specific CA-IDMS libraries. When implemented, the modifications should adequately limit read and update access to data and database datasets.

If read and update access is not adequately controlled, users could make unauthorized changes to CA-IDMS data, program, and utilities.

Summary

To ensure the integrity of the financial information derived from the PX06 application, adequate general controls must exist over the Production and Test Systems. Opportunities exist to improve the controls over SVCs, sensitive utility programs, and CA-IDMS access controls.

Recommendations for Corrective Action

1. We recommend that the Chiefs of Technical Support Division and System Support Division, Defense Megacenter, Mechanicsburg, Pennsylvania:

a. Obtain an integrity review of the new code for the locally developed supervisor call on the Production and Test Systems from the Deputy Chief of Staff for Security, Defense Information Systems Agency, Western Hemisphere.

b. Remove the other two supervisor calls on the Production and Test Systems and replace them with correctly installed versions or planned upgrades.

2. We recommend that the Chief, Automated Data Processing Security, Defense Megacenter, Mechanicsburg, Pennsylvania, examine the two unsecured sensitive utilities and restrict their use in accordance with "DISA WESTHEM MVS Security Technical Implementation Standards," revised in accordance with Recommendation 3.b.

3. We recommend that the Deputy Chief of Staff for Security, Defense Information Systems Agency, Western Hemisphere:

a. Develop procedures that require the Defense megacenters to submit locally developed supervisor calls to him for an integrity review and include the new procedures in a revision to the "DISA WESTHEM MVS Security Technical Implementation Standards."

b. Include the unsecured sensitive utility on the Production and Test Systems in the list of programs that should be protected in the next revision of the "DISA WESTHEM MVS Security Technical Implementation Standards."

4. We recommend that the Commander, Naval Supply Systems Command, direct the Commander, Naval Inventory Control Point, Mechanicsburg, Pennsylvania, to limit read and update access to the Computer Associates, Incorporated, Integrated Data Management System libraries to those users having a valid need.

Management Comments

The DISA concurred with Recommendations 1.a. and b. stating that an integrity review of the locally developed supervisor call would be obtained in May 1996, and the integrity exposures caused by the supervisor calls would be eliminated by July 1997. DISA verbally confirmed that the integrity review, though not completed, was in process. Management also concurred with Recommendation 2. stating that the sensitive utilities were restricted as of March 1996. In addition, they concurred with Recommendations 3.a. and b., stating that the requirements for integrity reviews for DMC locally developed supervisor calls

and protection of the sensitive utilities will be included in the next edition (July 1996) of the "DISA WESTHEM MVS Security Technical Implementation Standards."

The Navy concurred with Recommendation 4. stating that action was taken to limit access to data base libraries.

THIS PAGE INTENTIONALLY LEFT BLANK

Part II - Additional Information

Appendix A. Scope and Methodology

Scope Limitations. The audit was limited to following up on prior audit recommendations. Therefore, we did not evaluate the management control programs at DMC-Mechanicsburg or NAVICP.

Methodology. We examined general controls that could affect the integrity of the PX06 application. Specifically, controls over library access, supervisor calls, and sensitive utilities; implementation of the Security Software's access protection; and CA-IDMS controls over integrated data dictionaries, access to the PX06 application, CA-IDMS libraries, and utility programs.

Use of Statistical Sampling Procedures and Computer-Processed Data. To achieve the audit objectives, we did not rely on statistical sampling procedures. However, we did rely on computer-processed data in the Operating System and Security Software libraries that support the Production and Test Systems at DMC-Mechanicsburg. The audit used Computer Associates, Incorporated, EXAMINE auditing software to extract data directly from computer memory and the Operating System libraries. EXAMINE is a software program that audits the Operating System. We used automated and manual techniques to analyze system data. The audit also used Computer Associates, Incorporated, CULPRIT report writer and on-line display options to extract data directly from the CA-IDMS production data base and the integrated data dictionary. All system testing was done in a controlled environment with management's approval. Based on those tests and assessments, we concluded that the data were sufficiently reliable to be used in meeting the audit objectives.

Organizations Visited, Audit Period, and Standards. We performed audit work at DMC-Mechanicsburg and NAVICP. This program audit was performed from September 7, 1995, through March 20, 1996. The audit was made in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the IG, DoD, and accordingly included such tests of management controls as were considered necessary. During the audit, we visited or contacted the organizations shown in Appendix D.

Appendix B. Summary of Prior Audits and Other Reviews

Computer Security Audits

Prior IG, DoD, and AFAA audits determined that financial computer systems critical to DoD were exposed to fraud and other risks. Knowledgeable users could exploit weaknesses in the operating system and security software and other general controls to improperly access, add, modify, or destroy sensitive computer data, programs, and other resources (accidentally or intentionally) without risk of detection. Management generally concurred in the recommendations made to improve computer security. The reports issued on these prior audits and the audit followup made in this and other IG, DoD, audits are discussed below.

AFAA Report, "Data Processing Center (DPC) Operations and Security at the Air Force Accounting and Finance Center (AFAFC) (Project No. 0195410)," August 5, 1991. The report identified weaknesses in the controls over operating system and security software at the finance center. IG, DoD, Report No. 95-263, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," June 29, 1995, was issued on the followup made on the prior recommendations, which were intended to improve the security of the computer center (now DMC-Denver) of the Air Force Accounting and Finance Center (now DFAS Denver Center).

IG, DoD, Report No. 93-002, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," October 2, 1992. The report identified weaknesses in the controls over the operating system and security software at two DISA organizations: Defense Information Processing Center (DIPC)-Cleveland and DIPC-Indianapolis. IG, DoD, Report No. 95-263 was issued on the followup at DIPC-Cleveland. Followup results at DMC-Denver on the recommendations made to DIPC-Indianapolis were made in Report No. 96-053. Repeat findings at DMC-Denver were reported on sensitive features of the operating system and on the tape management system, the production scheduling system, and the master catalog.

IG, DoD, Report No. 93-133, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," June 30, 1993. The report identified weaknesses at DIPC-Dayton, DIPC-Columbus (now DMC-Columbus), and the DLA Defense Systems Automation Center (now DLA Defense Systems Design Center) over operating system and security software. The DIPC-Dayton no longer exists because its

work load migrated to DMC-Columbus during FY 1994. IG, DoD, Report No. 95-263 was issued on the followup at DLA Defense Systems Design Center and DMC-Columbus.

IG, DoD, Report No. 94-060, "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization," March 18, 1994. The report identified weaknesses at one DFAS and three DISA organizations in controls over abnormal endings to computer operations; maintenance and security oversight of automatic data processing equipment; access to sensitive computer assets; and potential environmental hazards. Weaknesses in change control procedures at the DFAS Financial Systems Activity-Denver were also identified. See IG, DoD, Report No. 95-270, "Corrective Actions on System and Software Security Deficiencies," June 30, 1995, for followup at DFAS Financial Systems Activity-Denver. See IG, DoD, Report No. 95-263 for followup at the Defense Information Services Organization (now DISA WESTHEM), DIPC-Columbus (now DMC-Columbus), and DIPC-Denver (now DMC-Denver). We determined that followup was no longer viable on recommendations to DIPC-Indianapolis to make structural improvements or revise operating procedures. Such recommendations were made obsolete when the DIPC-Indianapolis computer system migrated to DMC-Denver.

IG, DoD, Report No. 94-065, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," March 24, 1994. The report identified weaknesses in the controls over operating system and security software at DFAS Financial Systems Activity-Pensacola (now DIPC-Pensacola), DIPC-Kansas City, and the Marine Corps Computer and Telecommunications Activity, including the latter's Worldwide Support Division. See IG, DoD, Report No. 95-270 for followup at DIPC-Pensacola. The computer systems previously audited at DIPC-Kansas City and both Marine Corps organizations migrated to DMC-St. Louis during FY 1995. See IG, DoD, Report No. 96-053 for followup at DMC-St. Louis on the recommendations made to DIPC-Kansas City and the two Marine Corps organizations.

IG, DoD, Report No. 95-066, "Controls Over Application Software Supporting the Navy's Inventories Held for Sale (Net)," December 30, 1994. The report identified weaknesses in the controls over operating system and security software, and in the integrated data management system at DMC-Mechanicsburg (Pennsylvania) and the Naval Supply Systems Command, Ships Parts Control Center, Mechanicsburg, Pennsylvania. Followup on the 11 recommendations is discussed in Part I of this report.

Audit Followup

Followup was conducted on the prior audits under the present followup audit and three other followup audits: IG, DoD, Reports No. 95-263, 95-270, and 96-053.

The earlier followup audits determined that DFAS, DISA, and DLA made commendable efforts to implement prior audit recommendations. However, the 3 Defense agencies had not adequately implemented 23 of 112 prior audit recommendations. The reports identified weaknesses in the controls over operating system and security software, environmental hazards, system recertification reviews, change controls, and other operating procedures. Certain weaknesses in the operating system were considered material. Improvements were recommended in operating system and security software, environmental controls, and management controls.

Appendix C. Glossary

Access control is a general term used to describe a number of techniques that restrict users of a computer system from gaining unauthorized access to the system or other users' data programs. When applied to software, access control usually refers to a specialized software security package, such as Resource Access Control Facility.

Batch processing is the execution of a program or set of programs on the basis of a single initiating action.

Computer Associates, Incorporated, CULPRIT is a report writer that can extract data directly from a CA-IDMS data base and the integrated data dictionary.

Computer Associates, Incorporated, Integrated Data Management System provides utilities to control and organize all data used, while allowing the data to be rearranged to suit different applications. All data records are stored in a data base, which is a central repository for each application. A dictionary-driven database management system, CA-IDMS uses an active data dictionary that contains information used to control the execution of the database management's components.

Data base is a collection of interrelated data that are stored together.

Database management system is a software system that facilitates the creation and maintenance of a data base and the execution of computer programs using the data base. Computer Associates, Incorporated, Integrated Data Management System is one of many types of database management systems available commercially.

Disk is a data storage device that allows data to be accessed randomly or sequentially without passing through unwanted data.

File is a collection of related data records stored on an external storage medium, usually a disk or tape.

Integrated data dictionary controls and directs outputs and actively documents the source and use of all data; definitions need not be duplicated, and all database management system and data communication components can use integrated data dictionary definitions.

Job is a basic unit of work on an IBM computer. A job consists of one or more steps or program executions.

Library is a collection of related data files or programs.

Multiple Virtual Storage/Extended Architecture operating system is one of two major operating systems that run on large IBM mainframe computers. The other major IBM operating system is known as the Virtual Machine operating system.

Operating system is the major component of any computer system. It is an integrated collection of computer programs, service routines, and supervising applications (that is, scheduling jobs, loading programs, allocating computer memory, managing files, and controlling input/output operations). Operating systems also isolate and protect individual user programs from one another.

Read access is a security feature that allows a user to only read, execute, or copy a file.

Sensitive utilities are computer programs that provide general support for computerized processes (such as diagnostic programs or programs designed to create test data or copy data from one storage device to another). The utilities become sensitive when they can bypass the system's security software or internal controls and thereby destroy data if not used properly.

Software is a generic term used to define all programming on a computer system, whether supplied by vendors or developed by in-house programmers. System software includes the operating system and accompanying utility programs that enable users to control, configure, and maintain the computer system.

Supervisor call is an assembler language instruction that causes a hardware interruption when executed. The operating system then passes control to the supervisor call to inform the operating system of the service (open a file for read or write access, close a file, etc.) that is being requested.

Supervisor calls are divided into two categories. One category is available to all programs, while the second is restricted to those programs authorized by the authorized program facility. Validity checking is the control technique that limits the execution of sensitive, unrestricted supervisor calls. The first 200 supervisor calls are provided by IBM or other software vendors. The remaining 56 supervisor calls can be added by a computer center's in-house programmers to meet its unique requirements or a vendor's software requirements.

Update access is a security system feature that allows write access to a file.

User ID is a method by which users sign on to a computer system and are identified.

Utility programs are computer programs or routines that perform general data- and system-related functions (such as copying, sorting, and merging files) required by other application software, the operating system, or users.

Validity checking is an integrity control used in a Multiple Virtual Storage/Extended Architecture operating system environment. It detects and disallows invalid user operations and system requests that could compromise security controls. In an application environment, validity checking refers to testing the validity of codes, such as account numbers, transaction numbers, or vendor numbers.

Appendix D. Organizations Visited or Contacted

Department of the Navy

Naval Supply Systems Command, Arlington, VA
  Naval Inventory Control Point, Mechanicsburg, PA

Defense Organizations

Western Hemisphere, Defense Information Systems Agency, Fort Ritchie, MD
Defense Megacenter, Mechanicsburg, PA
Inspector General, Defense Information Systems Agency, Arlington, VA

Appendix E. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
    Director, Chief Financial Officer Support Office
      Chief, Internal Management Control Division
      Internal Control Officer
    Director, Management Improvement
  Deputy Comptroller (Program/Budget)
Assistant to the Secretary of Defense (Public Affairs)
Director, Defense Logistics Studies Information Exchange

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
  Internal Control Officer
Auditor General, Department of the Navy
Commander, Naval Supply Systems Command
  Commander, Naval Inventory Control Point
Superintendent, Dudley Knox Library, Naval Postgraduate School

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Information Systems Agency
  Commander, Center for Information System Security
  Commander, Western Hemisphere
    Director, Defense Megacenter-Mechanicsburg
  Inspector General
  Internal Control Officer, Office of the Comptroller
Policy Liaison Division; Office of the Assistant Director, Policy and Plans; Defense Contract Audit Agency
Chief, Internal Review Group, Defense Logistics Agency
Inspector General, National Security Agency
Audit and Internal Management Control Liaison, National Security Agency

Non-Defense Federal Organizations and Individuals

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

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 National Security, Committee on Appropriations
  House Committee on Government Reform and Oversight
  House Subcommittee on National Security, International Affairs and Criminal Justice, Committee on Government Reform and Oversight
  House Committee on National Security

THIS PAGE INTENTIONALLY LEFT BLANK

Part III - Management Comments

Department of the Navy Comments

DEPARTMENT OF THE NAVY
OFFICE OF THE ASSISTANT SECRETARY
RESEARCH, DEVELOPMENT AND ACQUISITION
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

JUN 6 1996

MEMORANDUM FOR THE DEPARTMENT OF DEFENSE ASSISTANT INSPECTOR GENERAL FOR AUDITING

Subj: DODIG DRAFT AUDIT REPORT ON FOLLOW-UP AUDIT ON CONTROLS OVER OPERATING SYSTEM AND SECURITY ON COMPUTER SYSTEMS AT DEFENSE MEGACENTER, MECHANICSBURG, PA (PROJECT NO. 5FD-2030)

Ref: (a) DODIG memo of 3 Apr 96

Encl: (1) Department of the Navy Comments

We have reviewed the finding and recommendations provided by reference (a). We concur with the finding and recommendation 4, directed to the Naval Inventory Control Point, Mechanicsburg, to limit read and update access to data base libraries to those users having a valid need. Naval Inventory Control Point, Mechanicsburg already has taken action to reduce access to data base libraries.

Detailed comments are in enclosure (1).

J. P. DAVIDSON
Principal Assistant for
Information Resources Management

Copy to:
FMO-31
NAVINSGEN

DEPARTMENT OF THE NAVY COMMENTS
ON
DODIG DRAFT AUDIT FOLLOWUP REPORT
ON
CONTROLS OVER OPERATING SYSTEM AND SECURITY SOFTWARE ON COMPUTER SYSTEMS AT DEFENSE MEGACENTER, MECHANICSBURG, PENNSYLVANIA
(PROJECT NO. 5FD-2030)

Finding. General Controls

The DMC-Mechanicsburg and NAVICP fully implemented seven of 11 prior recommendations made to improve the general controls over the Security Software, Operating System, and the CA-IDMS data base supporting the PX06 Production and Test Systems. However, additional corrective actions were needed to fully implement four recommendations.

- At the DMC-Mechanicsburg, the integrity of one, locally developed supervisor call (SVC) had not been verified, two other supervisor calls with integrity exposures were still in use, and sensitive utilities were not adequately protected.

- At NAVICP, database administrators had not fully implemented excess controls over CA-IDMS data bases.

These weaknesses in the Security Software, Operating System, and CA-IDMS database management system resulted because managers at DMC-Mechanicsburg and NAVICP assigned a higher priority to other work requirements and were not aware of the sensitivity of certain programs. As a result, PX06 application programs and inventory data could be added, modified, or deleted without detection, and the integrity of systems was not ensured. The inadequate control over supervisor calls on the Operating System was a material weakness in management controls.

DON Comment

Concur.

Recommendations for Corrective Action

1. We recommend that the Chiefs of Technical Support Division and System Support Division, Defense Megacenter, Mechanicsburg, PA:

a. Obtain an integrity review of the new code for the locally developed supervisor call on the Production and Test Systems from the Deputy Chief of Staff for Security, Defense Information Systems Agency, Western Hemisphere.

b. Remove the other two supervisory calls on the Production and Test Systems and replace them with correctly installed versions or planned upgrades.

Enclosure (1)

DON Comment

Defer comment to the Defense Megacenter.

2. We recommend that the Chief, Automated Data Processing Security, Defense Megacenter, Mechanicsburg, PA, examine the two unsecured sensitive utilities and restrict their use in accordance with "DISA WESTHEM MVS Security Technical Implementation Standards," revised in accordance with recommendation 3.b.

DON Comment

Defer comment to the Defense Megacenter.

3. We recommend that the Deputy Chief of Staff for Security, Defense Information Systems Agency, Western Hemisphere:

a. Develop procedures that require the Defense Megacenters to submit locally developed supervisor calls to him for an integrity review and include the new procedures in a revision to the "DISA WESTHEM MVS Security Technical Implementation Standards."

b. Include the unsecured sensitive utility on the Production and Test Systems in the list of programs that should be protected in the next revision of the "DISA WESTHEM MVS Security Technical Implementation Standards."

DON Comment

Defer comment to the Defense Megacenter.

4. We recommend that the Commander, Naval Supply Systems Command direct the Commander, Naval Inventory Control Point, Mechanicsburg, PA, to limit read and update access to the Computer Associates, Incorporated, Integrated Data Management System libraries to those users having a valid need.

DON Comment

Concur. NAVICP-Mechanicsburg Data Base Administrators (DBAs) have made adjustments to the security profiles of the data base which houses NAVICP corporate data required for the execution of Application PX06. The changes that were incorporated reduced access to the analyst and DBA personnel required to maintain and execute the system. These modifications limit the access to and, in the opinion of Navy, provide more than adequate protection of NAVICP-Mechanicsburg corporate business data. The NAVICP-Mechanicsburg DBA staff continue to monitor the data base in question for unauthorized access attempts and will make necessary adjustments to the security access controls as required.

Defense Information Systems Agency Comments

DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

IN REPLY REFER TO: Inspector General

31 May 96

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ATTN: Tom Hare

SUBJECT: Additional Agency Comments, DODIG Draft Report, "Followup Audit of Controls Over Operating System and Security Software on Computer Systems at Defense Megacenter Mechanicsburg, PA (Project No. 5FD-2030)

As requested, we are providing additional management comments that directly address recommendation 1.b of the subject report.

The point of contact is Ms. Barbara Nichols on (703) 607-6607.

1 Enclosure a/s

PHILIP D. LAVIETES
Assistant Inspector General
For Audits

Quality Information for a Strong Defense

Additional Agency Comments, DODIG Report,"Followup Audit of Controls Over Operating System and Security Software on Computer Systems at Defense Megacenter Mechanicsburg, PA (Project No 5FD-2030)

Recommendation 1b:

"The second SVC is employed by a non-supported version of the Database Management System (DBMS). An SVC (with PROTECT KEY 10) was created on another image and sent to the ICPM16 image to resolve this issue. However, this SVC module was unacceptable due to its creation on a different version of the operating system, which could cause problems due to possible different controls blocks in the operating system. The Technical Support Division, DMC Mechanicsburg, is now involved with the creation of this SVC module in the resident operating environment. After a short testing/verification process, the SVC with PROTECT KEY 10 will be placed into service. The previous SVC will be removed. The original plan was to resolve this problem by 31 December 1996, when the NAVICP-M RAM application would be converted to run under IDMS version 12.0 or later. It will be corrected in IDMS 10.2. The estimated completion date is now projected for 15 July 1996."

DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

IN REPLY REFER TO:

Inspector General

10 May 1996

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ATTN: Director, Finance and Accounting

SUBJECT: Draft Audit Report on Followup Audit of Controls Over Operating System and Security Software on Computer Systems at Defense Megacenter, Mechanicsburg, PA (Project No. 5FD-2030)

Reference: DODIG Report, subject as above, 3 Apr 96

1. We have reviewed the subject draft report and concur with the recommendations. Our management comments which describe corrective actions currently underway or planned are contained at the enclosure.

2. The point of contact for this action is Ms. Sandra J. Leicht, Audit Liaison, on commercial (703) 607-6316.

FOR THE DIRECTOR:

1 Enclosure a/s

RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense

MANAGEMENT COMMENTS TO
FOLLOWUP AUDIT OF CONTROLS OVER OPERATING SYSTEMS AND SECURITY SOFTWARE ON COMPUTER SYSTEMS AT DEFENSE MEGACENTER, MECHANICSBURG, PENNSYLVANIA
(PROJECT NO. 5FD-2030)

1. **Recommendation 1.a:** Recommend that the Chief of Technical Support Division and System Support Division, DMC-Mechanicsburg, obtain an integrity review of the new code for the locally developed supervisor call on the Production and Test Systems from the Deputy Chief of Staff for Security, DISA WESTHEM.

Comment: Concur. DMC-Mechanicsburg submitted a request for integrity review of the new code for the locally developed supervisor call on the Production and Test Systems to the Deputy Chief of Staff for Security (WE5) on 15 April 1996. WE5 will review the request to ensure there are no potential security vulnerabilities. The estimated completion date for review and approval of the integrity review by WE5 is 31 May 1996.

2. **Recommendation 1.b:** Recommend that the Chief of Technical Support Division and System Support Division, DMC-Mechanicsburg, remove the other two supervisor calls on the Production and Test Systems and replace them with correctly installed versions or planned upgrades.

Comment: Concur. The two supervisor calls (SVC) require different corrective actions as described below:

a. SVC 1. The first SVC will not be provided by the vendor for the version of the product that is running at DMC Mechanicsburg under the MVS/XA operating system. The latest release of the product corrects the SVC integrity exposure; however, the latest release of the product will run only under an MVS/ESA environment. Removal of the SVC from the existing systems will result in loss of functionality for our customers. DMC Mechanicsburg's implementation of MVS/ESA will include an upgrade of this product with the new SVC. Projected dates for MVS/ESA implementation based on software availability to be provided by the DISA Deputy Director for Engineering and Interoperability (D6) are January 1997 for the Test System and July 1997 for the Production System.

b. SVC 2. The second SVC is employed by a non-supported version of database management system (DBMS). A letter has been sent to the DMC customer for that application requesting a timeframe for their conversion. Removal of the SVC from the existing system without conversion by the customer will result in a loss of application availability for the DMC's customers. The DMC has requested the customer, Navy Inventory Control Point, to convert the URAM application to run under IDMS version 12.0 or later, not later than 31 December 1996. After conversion of the application, DMC Mechanicsburg will remove the SVC. Estimated completion date is projected for 31 December 1996. Copy of the memo to the DMC customer requesting conversion of the URAM application is attached as Enclosure 1.

3. **Recommendation 2:** Recommend that the Chief, Automated Data Processing Security, DMC Mechanicsburg, examine the two unsecured sensitive utilities and restrict their use in accordance with "DISA WESTHEM MVS Security Technical Implementation Standards," revised in accordance with Recommendation 3.b.

Comment: Concur. DMC Mechanicsburg has examined the two unsecured sensitive utilities in accordance with the DISA WESTHEM MVS STIS. Corrective actions have been accomplished as of 5 March 1996, and the utilities have been restricted. Completion dates for the two unsecured utilities were as follows:

a. SHOPMAPF on system ICPM02, 5 December 1995 and on system ICPM16, 24 January 1994.

b. PDS84EX w/REPLACE on system ICPM02, 29 February 1996 and on system ICPM16, 5 March 1996.

The action recommended by the audit has been met; therefore, request this action be closed.

4. **Recommendation 3.a:** Recommend the Deputy Chief of Staff for Security (WE5), DISA WESTHEM, develop procedures that will require the DMCs to submit locally developed supervisor calls to WE5 for an integrity review and include the new procedures in a revision to the "DISA WESTHEM MVS Security Technical Implementation Standards."

2

Comment: Concur. The Deputy Chief of Staff for Security (WE5) prepared and distributed a memorandum to all DMCs as well as related Central Design Agencies (CDA) requesting the submission of developed authorized code. Copy of memo is attached as Enclosure 2. This requirement will be incorporated into the next edition of the DISA WESTHEM MVS Security Technical Implementation Standards, currently scheduled for release by 31 July 1996. Although WE5 currently lacks the resources to examine all SVCS/utilities, WE5 will begin to analyze the ones included in this audit report (reference Recommendation 1.a). WE5 will incorporate a task into their Statement of Work for contractor support for next fiscal year to accomplish this task for all DMCs.

5. **Recommendation 3.b:** Recommend the Deputy Chief of Staff for Security (WE5), DISA WESTHEM, include the unsecured sensitive utility on the Production and Test Systems in the list of programs that should be protected in the next revision of the "DISA WESTHEM MVS Security Technical Implementation Standards."

Comment: Concur. The utility that has the capability of modifying the Authorized Program Facility (APF) list will be secured by adding it to the list of protected programs. The general use utility with the sensitive function requires additional analysis. The Deputy Chief of Staff for Security concurs that the sensitive function within the shareware utility must be secured, but the methodology by which the function is to be secured is unknown at this time. Methods of securing this function will be researched and incorporated into the next edition of the DISA WESTHEM MVS Security Technical Implementation Standards, currently scheduled for release by 31 July 1996.

3

DEFENSE INFORMATION SYSTEMS AGENCY
DISC MECHANICSBURG
5450 CARLISLE PIKE
P O BOX 2020
MECHANICSBURG PA 17055-0975

IN REPLY REFER TO WEP1/058

23 APR 1996

Commanding Officer
Naval Inventory Control Point
Attn: Code M04
5450 Carlisle Pike
P.O. Box 2020
Mechanicsburg, PA 17055-0788

Subject: Conversion of URAM Application to IDMS 12.0

1. During a recent DoDIG Audit of Controls Over Operating System and Security Software on Computer Systems at Defense Megacenter, Mechanicsburg, Pennsylvania (Project 5FD-2025), an operating system integrity exposure was discovered that is related to IDMS version 10.2. Currently, on the ICPM16 system, only the URAM application still uses this version of IDMS. Due to the integrity exposure to the entire system, it is imperative that the URAM application be converted to run under IDMS version 12.0 (or later). It is requested that this conversion be accomplished no later than December 1996.

2. If there are any questions or comments contact either Terry Farley, WEP4, at extension 3637 or John Szwast, WEP3, at extension 2298.

M. D. HUDOCK
Captain, SC, USN
Commanding Officer

INTEROFFICE MEMORANDUM

TO: Distribution

FROM: Deputy Chief of Staff for Security (WE5)

DATE: 2 [illegible] 1996

SUBJECT: Request for Source Code and/or Integrity Statements for User Developed Exits and Supervisor Calls

Reference: DISA WESTHEM Security MVS Security Technical Implementation Standards, Version 2, Release 1, January 1996

Preparer: C. Adams/WE5/DSN 277-4974

1. Many of the MVS-related findings were based on missing source code and integrity statements. Consequently, source code and/or integrity statements for user developed exits and supervisor calls will now be maintained by DISA WESTHEM Security, WE5.

2. IAW Paragraph 2.1.2.6 of reference, source code and/or integrity statements for user developed exits used in the operating system (i.e. SMF and JES) are to be reviewed for their potential exposures. Request agencies responsible for such exits, review them and provide the DMC and WE5 with source code and/or integrity statements by 31 May 1996.

3. IAW Paragraph 2.1.2.7 of reference, user developed External Security Manager (ESM) exits and Supervisor Calls (SVCs) are to be maintained by WE5. Request source code for all user developed ESM exits (i.e. password exits) and SVCs, be forwarded in electronic format, to WE5 by 30 April 1996. Upon receipt, WE5 will review the exits for vulnerabilities and approve/disapprove the exit for use on the system.

4. Enclosure 1 lists the vendor integrity statements, already acquired by WE5, for COTS products. Please review the list to determine if additional statements are needed. If you have any vendor integrity statements not on the list, please send a copy to WE5 for inclusion in the technical library.

DISA WESTHEM IM, WE5, Request for Source Code and/or Integrity Statements for User Developed Exits and Supervisor Calls,

2 C MAR 1996

5. Points of contact for this action are, Bill Keely, DSN 277-5574, commercial (301) 878-5574, E-Mail address: bill.keely@ritchie.disa.mil and Ed McBride, DSN 277-4459, commercial (301) 878-4459, E-Mail address: ed.mcbride@ritchie.disa.mil.

Enclosure a/s

DAVID B. HUGHES
Deputy Chief of Staff
for Security

Distribution:
WEA, WEB, WEC, WED, WEE, WEG, WEH, WEJ, WEK, WEL, WEM, WEP, WER, WES, WET, WEW, DFAS-FSO, DFAS-DAO Cleveland, DFAS-FSADE, DLA SDC, DSSOAS, ISSC, JEXIM(WE3324), JEXIT(WE3322), JLS, LOGSA, MSG-KELLY AFB, MSG WRIGHT-PATTERSON AFB, MSG-TINKER AFB, USAMC SIMA, IPC BUPERS, NAVMASSO, NFMSO, NRPC, AFPC/DPDS HQ, USMC CTA, MIIC

Copy To:
WE, WE01, WE03, WE1, WE2, WE3, WE4, WE5, WE31 Fort Ritchie RCC, WE31 Scott AFB RCC, WE31 Columbus AFB RCC, WE31 C4I Denver, WE34, WE35, WE36, WE51, WE52, WE53, WE54, WEY, D1, D2, D3, D5, D7, D16, D34, CISS, DISA IG, DLA HQ, DOD IG, IRMD, JIEO, USAMC CIO, NCTS-WASHINGTON, NCTS-PENSACOLA, NCTS-JACKSONVILLE, NCTS-SAN DIEGO, CA, IBM

2

Audit Team Members

This report was prepared by the Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, DoD.

F. Jay Lane
David C. Funk
W. Andy Cooley
Thomas G. Hare

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Followup Audit of Controls Over Operating System and Security Software on Computer Systems at Defense Megacenter, Mechanicsburg, Pennsylvania

B. DATE Report Downloaded From the Internet: 11/24/99

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 11/24/99**

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.