



EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503

Executive Registry

88-4703X

M-89-06

November 29, 1988

1079



## MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Joseph R. Wright, Jr.  
Director

SUBJECT: Review of General Controls in Federal  
Computer Systems Conducted by the  
President's Council on Integrity and  
Efficiency (PCIE)

The attached report is the second in a series of products of the President's Council on Integrity and Efficiency (PCIE) Computer Systems Integrity Project. In a review of ten major Federal computer centers, the PCIE study team found serious control deficiencies in system software, as well as opportunities to recover inefficiently used disk storage.


The findings in the report are both alarming and important. They suggest actions that agencies should take immediately, such as developing effective policies and procedures for operating system security for their computer centers and making greater use of commercially available diagnostic tools to guide operating system maintenance. I urge you to examine the report carefully and take immediate action to address the deficiencies identified both in the specific systems reviewed in the report as well as in other systems in your agency with similar system software. In particular:

- o If your agency is one of the agencies identified in the report, I ask that you determine which of the weaknesses reported for your agency are material, as described in our August 15, 1988 guidance (M-88-29), and report them in this year's annual report to the President under the Office of Management and Budget's (OMB) Circular No. A-123.
- o In accordance with the Computer Security Act of 1987 (Public Law 100-235), your agency is developing computer security plans for each of its computer systems that contain sensitive information. Control of system software is to be included as part of those plans (see OMB Bulletin 88-16). Given the potential risk represented by the weakness found, I ask that you make sure that where security plans concern systems that utilize the system software discussed in this report, extra attention be paid to that portion of the security plan.

DD/A REGISTRY

FILE: 0102-36

-2-



I am also asking the Directors of the National Institute of Standards and Technology and the National Security Agency and the Administrator of the General Services Administration to act on the recommendations addressed to those agencies.

Reports of this sort, which identify potential vulnerabilities and offer constructive advice for addressing them, are critical to our continuing efforts to improve the integrity of Federal systems consistent with the Computer Security Act of 1987, the Federal Manager's Financial Integrity Act of 1982 (Public Law 97-255), and just plain good management practice. I commend the PCIE for its efforts.

Attachment



**PRESIDENT'S COUNCIL  
ON INTEGRITY AND  
EFFICIENCY**

**REVIEW  
of  
GENERAL CONTROLS  
in  
FEDERAL COMPUTER  
SYSTEMS**

**OCTOBER 1988**



## PRESIDENT'S COUNCIL on INTEGRITY & EFFICIENCY

October 12, 1988

MEMORANDUM FOR: The Honorable Joseph R. Wright, Jr.  
Chairman, President's Council on  
Integrity and Efficiency

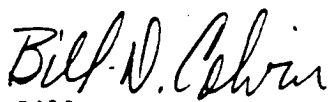
Members, President's Council on  
Integrity and Efficiency

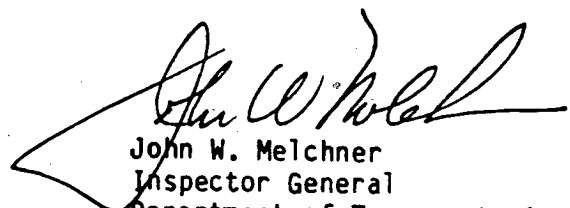
FROM: Project Co-Leaders  
PCIE Computer Committee  
Computer Systems Integrity Project

SUBJECT: Review of General Controls in  
Federal Computer Systems

The enclosed final audit report presents the consolidated results of Task 2A of the President's Council on Integrity and Efficiency (PCIE) sponsored Computer Systems Integrity Project. Task 2A covered the Review of General Controls in Federal Computer Systems. The report's Executive Summary succinctly describes the overall condition identified by the Inspectors General, including (1) the existence of serious operating system and security software control deficiencies at all agency computer centers reviewed and (2) opportunities to recover an estimated \$17 million in inefficiently used disk storage at these centers.

The report makes several Governmentwide recommendations for strengthening information systems management of operating system and security software, and disk and tape storage at Federal computer centers. Implementing these recommendations will require actions by the Office of Management and Budget, the National Institute of Standards and Technology, the National Security Agency, and the General Services Administration. We provided copies of the draft version of this report to all four organizations for comment. We obtained informal comments from Office of Management and Budget officials after receiving formal written comments from the other three organizations (included in their entirety in Appendix F). These comments indicate general agreement with the report and its recommendations, and have been incorporated as appropriate into this final version of the report.

  
Bill D. Colvin  
Inspector General  
National Aeronautics and  
Space Administration

  
John W. Melchner  
Inspector General  
Department of Transportation

Enclosure

THE PRESIDENT'S COUNCIL ON  
INTEGRITY AND EFFICIENCY'S REVIEW OF  
GENERAL CONTROLS IN FEDERAL COMPUTER SYSTEMS

EXECUTIVE SUMMARY

In September 1986, the President's Council on Integrity and Efficiency (PCIE) initiated the Computer Systems Integrity Project. The project is a multi-task effort focusing on controls, security, and other integrity issues related to the entire data processing systems life cycle. The objectives of the overall project are to assess the integrity of Federal computer systems and develop recommendations for Governmentwide improvements in standards, procedures, documentation, and operations affecting computer systems integrity.

The first task, Survey of Agency Implementation of Computer Systems Integrity Requirements, focused on the compliance of eight agencies with mandated policies and other requirements for computer security and controls. It assessed the general level of implementation of those requirements for Federal agency computer systems unrelated to national security. It resulted in a separate product by each of the eight participating Offices of Inspectors General discussing survey results at their particular agency. In addition, a consolidated report by the PCIE which summarized overall survey results was issued on June 2, 1988. The report identified five common obstacles which limited the effectiveness of agency compliance activities, and made recommendations to the Office of Management and Budget (OMB) for overcoming those obstacles and strengthening agencies' compliance capabilities Governmentwide.

This second task, General Controls Review, is one of two project tasks aimed at reviewing operational systems. Initiated in July 1987, the task was aimed at assessing management controls over system software--i.e., operating system software and access (security) software--at 10 Federal computer centers. In addition, disk and tape storage management were analyzed as a byproduct of using the computer assisted audit techniques employed to assess system software controls. The Inspectors General offices at the ten Federal agencies shown in Appendix A participated in this task. They used a combination of both automated and manual audit techniques as described in Appendices B and C. Of the 10 major mission-support/administrative computer centers reviewed (Appendix A also profiles each center), 6 disburse an estimated \$273 billion to American citizens and businesses annually, and 8 support large-scale financial systems that controlled funds which totalled over \$1.4 trillion for FY 1987. Each participating Inspector General issued one or more reports describing the system software internal control weaknesses and disk and tape storage management deficiencies found at each of their respective agencies. These reports are listed in Appendix D.

We concluded that all of the agency computer systems reviewed had serious operating system and security software control deficiencies (see Appendix E). The operating system integrity exposures would allow a knowledgeable perpetrator to access, modify, and/or destroy an agency's computer data, programs, and other resources without leaving an audit trail. These exposures resulted from (a) inadequate controls over enhancements to operating systems, (b) inadequate administration of the authorized program

facility (an important system protection mechanism), (c) improper maintenance of operating system software, and (d) a lack of policies standards, and procedures pertaining to system software management. In addition, improper technical implementation of security software features and inadequate administrative controls over security software further increased the risks to operational continuity and integrity of critical applications which support agency missions.

Using terminals just like those used by regular users to access the systems, we demonstrated to agency information systems managers the seriousness of these collective internal control weaknesses. For example, in the presence of agency information systems managers, we disabled security checking for file accesses and converted our "standard" terminal into the functional equivalent of a "master operator's console." This gave us the capability to take total control over the agency's computer system and access, modify, and/or destroy sensitive data and disrupt the continuity of information processing activities. We convinced agency managers that we, or any knowledgeable user, could have performed any of these adverse acts without being detected. In general, agency information systems managers were not fully equipped to deal with the technically complex interrelationships between system software controls and computer systems integrity. We believe that additional guidance for agency information systems managers is needed to better focus attention on, and to strengthen, operating system and security software controls. Part II of the report discusses these issues in more depth, and includes comprehensive Governmentwide recommendations.

Our computerized analyses of combined disk storage resources showed that significant opportunities existed to improve disk storage management at all ten agency computer centers reviewed. In total, an estimated \$17 million in inefficiently used disk storage could be recovered and made available for reuse through the application of generally accepted disk storage management techniques--thereby reducing the need for future additional disk storage procurements. Similarly, our computerized analyses of magnetic tape storage showed that tape processing efficiency could also be significantly improved. Additional guidance on the use of generally accepted disk and tape storage management techniques is needed for agency information systems managers to better focus attention on, and to strengthen controls over, disk and tape storage resources. Part III of the report discusses this issue in more depth, and contains pertinent Governmentwide recommendations.

Comments of organizations affected by the Governmentwide recommendations have been incorporated into the report as appropriate, and their formal replies are contained in their entirety in Appendix F. OMB staff generally agreed with the recommendations presented in this report for strengthening information systems management of operating system and security software, and disk and tape storage at Federal computer centers. The actions prescribed for the responsible oversight agencies, together with the agency-specific actions recommended by the respective Inspectors General, should substantially strengthen computer systems integrity Governmentwide.

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY . . . . .	i
I. <u>INTRODUCTION</u> . . . . .	1
Background . . . . .	1
Overview of Governmentwide Requirements . . . . .	3
Scope of Evaluation . . . . .	4
II. <u>STRENGTHENING CONTROLS OVER OPERATING SYSTEM AND ENVIRONMENTAL SECURITY SOFTWARE</u> . . . . .	6
Need to Strengthen Operating System Software Controls . . . . .	6
Operating System Extension . . . . .	7
Operating System Protection . . . . .	7
Operating System Maintenance . . . . .	8
Operating System Software Management Policies, Standards, and Procedures . . . . .	12
Need to Strengthen Security Software Controls . . . . .	12
Technical Security Software Controls . . . . .	13
Administrative Security Controls . . . . .	14
Recommendations . . . . .	15
III. <u>IMPROVING MANAGEMENT OF DISK AND MAGNETIC TAPE STORAGE RESOURCES</u> . . . . .	16
Need to Strengthen Disk Storage Management . . . . .	16
Need to Improve Tape Storage Management . . . . .	17
Recommendations . . . . .	18
IV. APPENDICES	
Appendix A. Profile of Agency Missions, Computer Centers Reviewed, and Potential Adverse Impact on Missions. . . . .	19
Appendix B. Audit Methodology and Guidelines. . . . .	26

TABLE OF CONTENTS (Continued)

	Page
Appendix C. Definition of System Software Problem Analysis Management Areas and Severity Levels. . . . .	32
Appendix D. Individual Agency Reports Issued under Task 2A. . .	36
Appendix E. Assessment of System Software Controls at 10 Federal Computer Centers. . . . .	38
Appendix F. Comments of Organizations Affected by Governmentwide Recommendations . . . . .	39
Appendix G. List of Acronyms. . . . .	45



## I. INTRODUCTION

### Background

Federal agencies have significant information technology inventories, and the trend is toward the use of more information technology, especially in the hands of end users. For example, agencies currently have about 18,000 large- and medium-scale computers and, according to estimates by the General Services Administration (GSA), have almost one-half million microcomputers costing about \$1.7 billion in use. Information generated from these systems has become critical to managers for long-range planning as well as day-to-day operations. The increased dependence on computer systems to carry out departments' and agencies' missions requires that the integrity of computer systems is maintained. This involves assuring that cost-effective internal controls are in place to manage and secure the processing of sensitive automated information critical to Government operations.

The information technology explosion has greatly increased opportunities for fraud, waste, and abuse in Federal programs, making effective computer security more important than ever before. The Computer Committee of the PCIE has issued three reports since June 1983 addressing computer-related fraud issues. The first report, entitled "Computer-Related Fraud and Abuse in Government Agencies" (June 1983), discussed 172 computer-related fraud cases and provided data on perpetrator characteristics, losses, methods of perpetration, detection, and controls. The second report, entitled "Computer-Related Fraud in Government Agencies: Perpetrator Interviews" (May 1985), discussed the results of interviews conducted with 46 perpetrators of computer-related fraud involving seven Federal agencies. It provided insight into how, why, and by whom computer crimes are committed, and addressed generic weaknesses in Government computer systems. The third report, entitled "Computers: Crimes, Clues and Controls" (March 1986), discussed the prevention of unauthorized access, disclosure, delay, alteration, destruction, and other misuse of unclassified but sensitive automated data. In response to the growing threat of computer crime, Congress passed the Computer Fraud and Abuse Act of 1986, which made it easier for agencies to prosecute fraudulent and other illegal acts involving Federal computer systems.

From this perspective, in September 1986, the PCIE Computer Committee initiated the Computer Systems Integrity Project. The project is a multi-task effort focusing on controls, security, and other integrity issues related to the entire data processing systems' life cycle. The objectives of the overall project are to assess the integrity of Federal computer systems and develop recommendations for Governmentwide improvements in standards, procedures, documentation, and operations affecting computer systems integrity. Portions of the project are being performed in conjunction with the President's Council on Management Improvement.

The first task, Survey of Agency Implementation of Computer Systems Integrity Requirements, was aimed at providing an overview of the implementation of policies and other requirements pertaining to the establishment of general controls, generic application controls, and other integrity issues for Federal agency computer systems unrelated to national security. The work focused on the compliance of eight agencies with mandated requirements for computer security and controls in order to assess the general level of implementation of those requirements within the agencies. It resulted in nine products--a separate product by each of the eight participating Offices of Inspectors General (issued between April 1987 and May 1988) discussing survey results at their particular agency, and a June 2, 1988 consolidated report by the PCIE summarizing overall survey results.

In general, the survey found that by issuing policies and procedures, assigning responsibilities, putting monitoring activities in place, and conducting some training, Federal agencies complied with many of the computer systems integrity requirements stipulated in OMB Circulars A-123 "Internal Control Systems", A-127 "Financial Management Systems", and A-130 "Management of Federal Information Resources". However, agencies varied widely in the emphasis they placed on implementing each set of requirements, and the specificity of requirements within the circulars appeared to determine which functions were most actively being addressed within the agencies. The PCIE summary report identified five common obstacles which limited the effectiveness of agency implementation activities. The report made recommendations to OMB for overcoming those obstacles and strengthening agencies' implementation capabilities Governmentwide. Officials from OMB, GSA, the Office of Personnel Management (OPM), and the Department of Commerce's National Institute of Standards and Technology (NIST) generally concurred with the report findings and recommendations.

This second task, General Controls Review, is one of two project tasks aimed at reviewing operational systems. It was initiated in July 1987 to assess management controls over system software at selected Federal computer centers. (System software refers to the computer programs that manage the processing workload and control user access to the various resources of the computer system.) Work on this task focused on two key system software controls subareas: (a) operating system software controls and (b) access (security) software controls. In addition, disk and tape storage management were analyzed as a byproduct of using the computer assisted audit techniques employed to assess system software controls.

System software controls is one of six types of general information system controls (the other five are organization controls; system design, development, and modification controls; data center operations controls; data center protection controls; and hardware controls). We concentrated our general controls review on this area because the Inspector General community has traditionally given little or no attention to system software controls--even though the degree of their effectiveness has a major impact on overall computer systems integrity.

### Overview of Governmentwide Requirements

Governmentwide policies and requirements for system software controls and disk and tape storage management have been prescribed in general terms by a variety of Federal sources, including OMB and the Congress. Although system software controls are not specifically mentioned, Circulars A-123 and A-130, in conjunction with the Computer Security Act of 1987, contain the requirements for agencies to establish and implement computer security and control activities. Similarly, OMB Circular A-130, in conjunction with the Paperwork Reduction Reauthorization Act of 1986, requires agencies to establish and implement information resources management controls to ensure the efficient, effective, and economical use of information resources such as disk and tape storage resources. These requirements and their sources are further discussed below.

In providing for implementation of the Federal Managers' Financial Integrity Act of 1982, OMB Circular A-123 requires agencies to establish and maintain cost-effective systems of internal controls to provide management with reasonable assurance that assets are safeguarded against waste, loss, and unauthorized use. Included in its provisions are requirements that agencies (a) conduct risk assessments to identify potential risks in their operations, (b) make internal control evaluations to determine whether their internal control systems are effective, and (c) report annually to the President and Congress on the state of their internal control systems.

OMB Circular A-130 provides for implementing the Paperwork Reduction Act of 1980 and other public laws and Executive orders. The 1980 Act established a broad mandate for agencies to perform their information activities in an efficient, effective, and economical manner. It specifically provided authority to OMB to develop and implement uniform and consistent information resources management policies; oversee the development and use of information management principles, standards, and guidelines; evaluate agency information management practices; and determine compliance of such practices with established policies, principles, and guidelines. In response to its provisions, GSA issued regulations requiring all executive agencies to review their Information Resources Management policies and activities on a triennial cycle. OMB Circular A-130 establishes requirements for general information policy, records management, privacy, and Federal Automatic Data Processing (ADP) and telecommunications. In addition, Appendix III of the circular (entitled "Security of Federal Automated Information Systems") requires agencies to ensure an adequate level of security for all automated information systems so that they operate effectively and accurately, contain appropriate safeguards, and continuously operate in support of critical agency functions.

In 1986, the Congress enacted the Paperwork Reduction Reauthorization Act, which amended the 1980 Paperwork Reduction Act. The 1986 Act prescribed two requirements which further addressed computer systems integrity. The 1986 Act first made agencies responsible for implementing applicable Governmentwide and agency information policies, principles, standards, and guidelines; and second, tasked them with periodically evaluating and improving, as needed, the accuracy,

completeness, and reliability of data and records contained in Federal information systems. (OMB has not yet incorporated these new requirements into Circular A-130.) In addition, the 1986 Act addressed information resources management by requiring that the Federal Government ensure that ADP, telecommunications, and other information technologies are acquired and used in an economical, efficient, and effective manner.

The January 8, 1988 enactment of the Computer Security Act of 1987 (P.L. 100-235) recognized the need for improving the security and privacy of sensitive information in Federal computer systems and created the means for establishing minimum acceptable security practices for such systems. In particular, it assigned NIST responsibility for developing standards and guidelines for the cost-effective security and privacy of information in Federal computer systems, required the establishment of security plans by all operators of Federal computer systems, and required mandatory periodic training for all persons involved in Federal computer systems.

#### Scope of Evaluation

Ten Inspectors General Offices participated in this task (Departments of Agriculture, Energy, Health and Human Services, Housing and Urban Development, Transportation, Treasury; Government Printing Office; National Aeronautics and Space Administration (NASA); OPM; and Veterans Administration). The Inspectors General reviewed system software controls and disk and tape storage resource utilization at a major mission-support/administrative computer center within each of their agencies. These agencies use automated systems to track their operating budget outlays, which are estimated to total about \$746 billion for FY 1988. Of the 10 computer centers reviewed, 6 disburse an estimated \$273 billion to American citizens and businesses annually. Further, eight of the computer centers support large-scale financial systems that controlled FY 1987 funds totaling over \$1.4 trillion.

All but one of the computer centers reviewed operated large-scale International Business Machines (IBM) Corporation computer systems (or compatible brands) using IBM's Multiple Virtual Storage (MVS) operating system. (The review work performed at the one non-MVS equipped computer center did not include an assessment of operating system software controls.) As shown by this task, MVS is the dominant operating system supporting the Federal Government's entitlement, payroll, financial management, accounting, grants management, and general administrative applications. A majority of the centers also used one of several commercially available environmental security software packages. A profile of the missions of each agency and computer center reviewed during this task is included in Appendix A. The Appendix also highlights the mission impairments that can result from inadequately controlled system software.

The Department of Transportation (DOT) and NASA Inspectors General Offices had overall responsibility for coordinating this task. A detailed Task Audit Guide and customized audit software were developed by DOT's Inspector General staff and used by the participants in performing this audit work. In addition, DOT's Inspector General staff provided extensive technical assistance to the participants, primarily in the area of operating system software controls. In performing this task, the participants used industry guidelines on system software management and security software implementation to supplement the Federal computer systems integrity and information resources management requirements. A combination of automated and manual audit techniques described in Appendices B and C was used to review each agency's computer systems. The reviews, which were conducted in accordance with the U.S. General Accounting Office's "Standards for Audit of Governmental Organizations, Programs, Activities, and Functions," were designed to answer the following three questions:

- Were operating system features which control the ability to perform sensitive tasks, such as bypassing system security, properly administered and controlled?
- Were environmental security software mechanisms which control user access to information and other computer resources properly administered and controlled?
- Were disk and magnetic tape storage resources economically, efficiently, and effectively used?

Where available, the participants used past reports and ongoing audits to fulfill specific task requirements. The field work was conducted between August 1987 and March 1988. Based on the information developed, individual agency reports were prepared and issued (see Appendix D). This report consolidates the findings of the individual agency assessments and presents recommendations addressing Governmentwide issues.

## II. STRENGTHENING CONTROLS OVER OPERATING SYSTEM AND ENVIRONMENTAL SECURITY SOFTWARE

All of the agency computer systems reviewed had significant operating system and security software control deficiencies (See Appendix E). The operating system integrity exposures would allow a knowledgeable perpetrator to access, modify, and/or destroy an agency's computer data, programs, and other resources--without leaving an audit trail. The security software control deficiencies further increased the risks to the operational continuity and integrity of critical applications supporting the missions of the agencies. Using terminals just like those used by regular users to access the systems, we demonstrated to agency information systems managers the seriousness of these collective internal control weaknesses. For example, we disabled security checking for file accesses and converted our "standard" terminal into the functional equivalent of a "master operator's console." This gave us the capability to take total control over the agency's computer system and access, modify, and/or destroy sensitive data and disrupt the continuity of information processing activities. Although we did not further exercise any of these powerful security and control privileges to perform any adverse acts, we convinced agency managers that we, or any knowledgeable user, could have performed any of the adverse acts noted above without being detected.

While operating system and security software functions are, in many respects, separate, computer systems integrity cannot be accomplished without having effective internal controls in place simultaneously over both. For example, when operating system integrity has been compromised, even a sophisticated and properly implemented security software package cannot be relied upon to prevent unauthorized access, modification, or destruction of sensitive information or other computer resources. Similarly, weak security software controls threaten operating system integrity by not sufficiently restricting user access to sensitive operating system resources and not ensuring separation of duties within sensitive information systems functional areas. Agency information systems managers were not adequately familiar with the technically complex interrelationships between system software controls and computer systems integrity. Additional guidance for agency information systems management is needed to better focus attention on, and to strengthen, operating system and security software controls.

### Need to Strengthen Operating System Software Controls

An operating system provides a collection of service routines (i.e., special programs) to supervise the sequence and processing of applications by a computer. The operating system also plays a key role in assuring computer systems integrity by isolating and protecting all individual tasks (i.e., applications) from one another in the system. As discussed below, the operating system integrity exposures and vulnerabilities identified by our work resulted from (a) inadequate controls over operating system extension, (b) inadequate administration of an important system protection mechanism, (c) improper maintenance of operating system software, and (d) a lack of policies, standards, and procedures pertaining to system software management.

### Operating System Extension

The standard functional capabilities of the MVS operating system can be extended through the addition of one or more special Supervisor Calls (SVC). SVCs are special machine instructions within an operating system which programs use to communicate with the operating system. For example, a "calling" program uses the SVC mechanism to request that the operating system perform a desired system service routine, such as opening a data file for modification. The vendor provides a standard set of SVCs when a computer center acquires the MVS operating system. In addition, other SVCs can be obtained from system software vendors and public domain software exchange services, and may even be developed inhouse by a computer center's own systems programming staff. Installing such additional SVCs has been a common practice at MVS computer centers.

Proper SVC design and implementation is a key element of operating system integrity and security. SVCs employ specialized and powerful processing capabilities to perform sensitive but crucial processing functions. The MVS vendor has developed rigorous integrity standards for its SVCs to ensure that their use can be highly controlled. SVCs from other sources, however, may not be subjected to similar integrity standards. According to computer security experts, installing such non-MVS vendor tested SVCs creates one of the greatest vulnerabilities for operating systems.

All nine MVS computer centers reviewed had installed non-MVS vendor tested SVCs which compromised system integrity. To demonstrate the seriousness of this type of integrity exposure, our audit tests successfully exploited vulnerable installation-added SVCs at eight of the nine computer centers. In doing so, we were able to bypass security software controls and take full control of the agency computer systems. These tests showed that the added SVCs provided the opportunity for any knowledgeable perpetrator to bypass critical operating system controls and then bypass normal security software controls. Furthermore, all three SVC sources--commercial system software vendors, public domain software exchange services, and local systems programming staff--contributed exposures at the computer centers reviewed. Before any SVC is installed, information systems management should thoroughly review its characteristics to guard against compromising operating system integrity and exposing an agency's computer system to potential penetration by unauthorized individuals.

### Operating System Protection

A key MVS operating system protection mechanism under the administrative control of computer center management is the authorized program facility (APF). Programs which have been placed in specially designated APF libraries become, in effect, part of the operating system and can generally gain the ability to circumvent or disable any security mechanism, alter any audit trail, and/or modify any application's data in the computer, regardless of the presence of access control software. Noncompliance with the MVS vendor's guidelines for APF administration can introduce integrity exposures to

the operating system environment and, at a minimum, seriously jeopardizes information systems management control over system software. For example, one IBM guideline cautions computer center management to avoid assigning the same name to more than one active APF-authorized program because the existence of duplicate names could result in a mixup of program flow and possibly introduce an integrity exposure.

By performing a computer-assisted analysis of the APF libraries at each of the nine MVS computer centers, we determined that all but one had significant numbers of duplicate-named programs. The eight centers averaged over 2,500 sets of duplicate-named programs (out of an average of 15,900 programs per center), and the center with the most duplicates had about 5,900 sets out of a total of about 51,000 programs. Information systems management should ensure that APF libraries and their contents are strictly controlled in accordance with MVS vendor guidelines to protect the operating system, as well as all applications, from accidental and/or deliberate acts to access, modify, or destroy information, programs, or other sensitive computer resources.

#### Operating System Maintenance

In sophisticated and complex operating system environments such as MVS, proper performance of routine and special maintenance tasks--a crucial area of system software management--is essential. Improperly applied changes can result in system modifications where the audit trail is insufficient to verify what changes were actually made. Industry experts strongly recommend that all maintenance to MVS be performed under the control of the vendor's System Modification Program (SMP). SMP provides facilities to manage a computer installation's software inventory by providing extensive records of additions and modifications in a historical control file. For all nine computer centers reviewed, modifications were made to operating system components outside the controls of SMP. Information systems management needs to adequately control operating system software maintenance--using recommended SMP facilities exclusively--to avoid unintentionally compromising the integrity of the system.

Because managing MVS operating system maintenance is complex, information systems management should also consider using commercially available diagnostic software tools as a preventive maintenance catalyst to supplement the traditional system software management process. We used such a commercially available diagnostic software package to analyze a key MVS maintenance dimension--unresolved problems--for the MVS computer systems reviewed. This package, which uses the SMP historical control file and a vendor-developed data base of MVS problems, compares the current MVS operating system software environment with this data base and provides comprehensive information on unresolved problems by severity level in various functional management areas. The summary tables and charts that follow show the range of significant, unresolved problems across the nine MVS computer systems analyzed--indicating that preventive maintenance should be a major concern at these Federal agencies.

Our diagnostic software package identified 4,915 instances of unresolved operating system problems at the nine MVS computer centers reviewed. Appendix C contains a description of each management area.



<u>NUMBER OF PROBLEM INSTANCES BY SYSTEMS MANAGEMENT AREA</u>										
<u>MVS COMPUTER CENTER</u>										
<u>MANAGEMENT AREA</u>	1	2	3	4	5	6	7	8	9	<u>TOTAL</u>
A Performance and capacity	183	129	85	81	90	65	61	56	30	780
B Security	56	22	6	26	16	17	17	8	10	178
C Measurement and accounting	67	35	22	32	27	10	12	9	10	224
D Workload control	5	2	0	2	8	2	2	2	2	25
E Operation and execution	132	124	91	50	57	45	43	36	39	617
F Internal reliability	446	318	298	144	160	130	101	114	76	1787
G External reliability	209	135	63	124	92	61	66	66	42	858
H Unassigned	74	95	18	71	43	31	45	41	28	446
Total	1172	860	583	530	493	361	347	332	237	4915

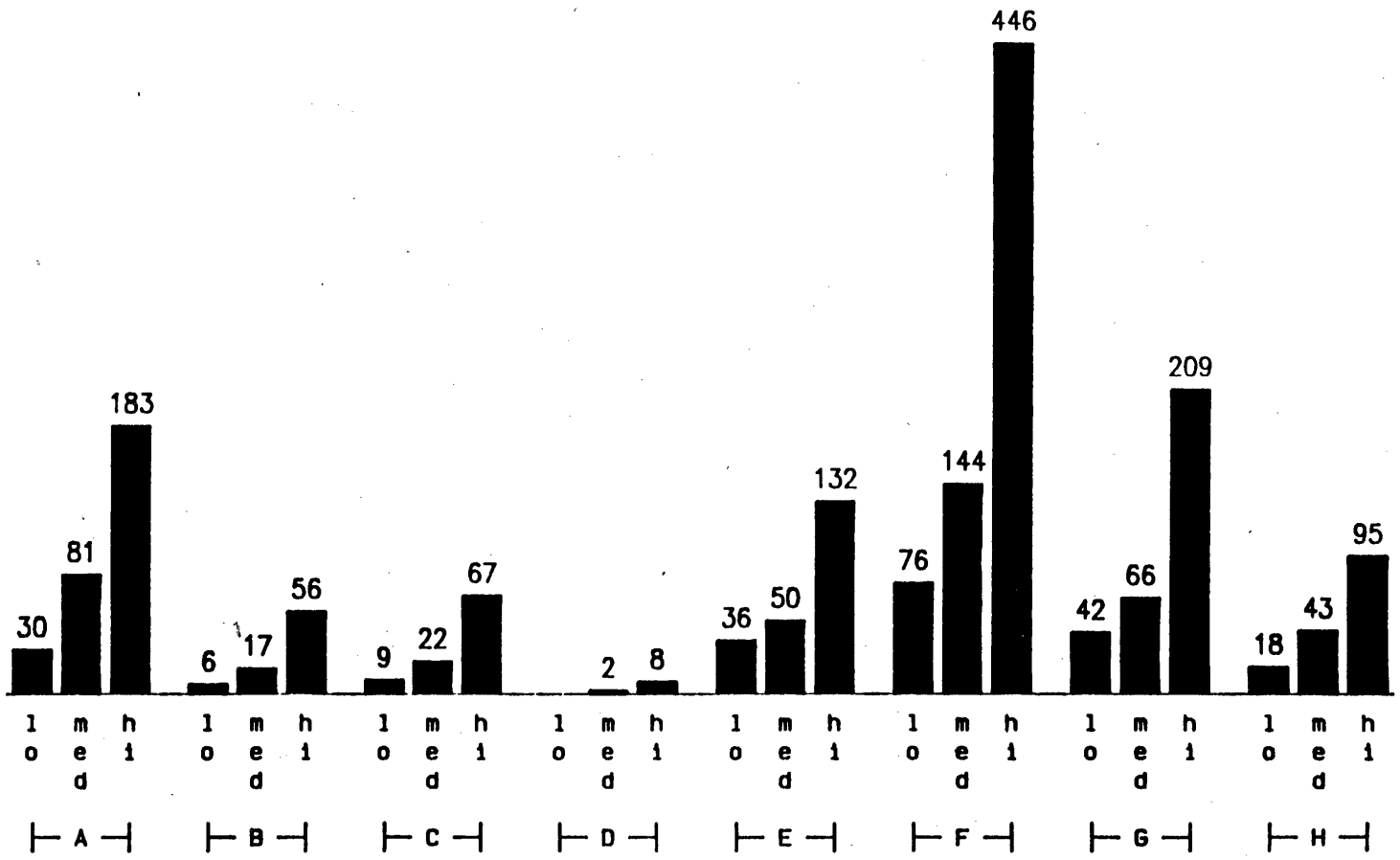
The package's vendor identified three severity levels for problems. The "critical" level is the most serious and can cause the entire computer system to fail (or some similarly catastrophic condition to occur); the "impacting" level is less serious than "critical" but includes integrity problems; and the "limited" level is the least serious but by no means trivial. (Appendix C expands on the vendor's criteria for categorizing problem severity.) Of the 4,915 problem instances identified, 340 were categorized as critical; 1,848 as impacting; and 2,727 as limited.

<u>NUMBER OF PROBLEM INSTANCES BY SEVERITY LEVEL</u>										
<u>MVS COMPUTER CENTER</u>										
<u>SEVERITY LEVEL</u>	1	2	3	4	5	6	7	8	9	<u>TOTAL</u>
Critical	80	65	32	37	31	26	26	18	25	340
Impacting	485	347	257	158	172	127	111	119	72	1848
Limited	607	448	294	335	290	208	210	195	140	2727
Total	1172	860	583	530	493	361	347	332	237	4915

Graphic summaries of the above tables follow.

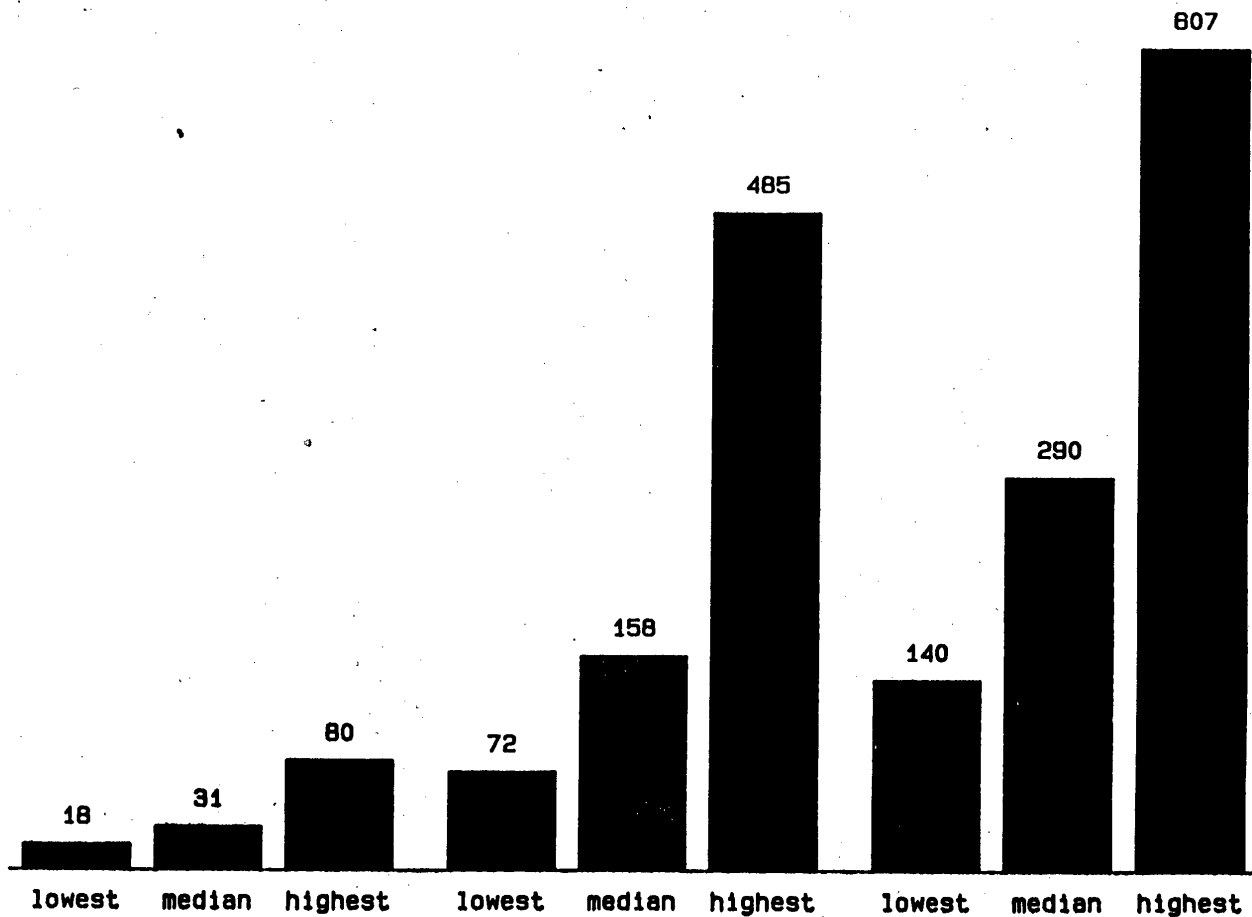
**SUMMARY OF PROBLEMS BY SYSTEMS MANAGEMENT AREA  
ACROSS MVS COMPUTER SYSTEMS REVIEWED**

10



A PERFORMANCE/CAPACITY  
B SECURITY  
C MEASUREMENT/ACCOUNTING  
D WORKLOAD/CONTROL  
E OPERATION/EXECUTION  
F INTERNAL RELIABILITY  
G EXTERNAL RELIABILITY  
H UNASSIGNED

***SUMMARY OF PROBLEMS BY SEVERITY LEVEL  
ACROSS MVS COMPUTER SYSTEMS REVIEWED***



11

Some of the unresolved problems had the potential to adversely affect computer systems integrity. For example, one critical problem identified by the diagnostic software pertained to specialized system software for disk storage management. The problem description provided by the package stated "if an audit, list, or report command uses the ODS parameter specifying a name which is a catalog alias, the catalog will be destroyed." (A catalog is a critical, systemwide data control file; an alias refers to an alternate name.) Since data files and program libraries are normally located by using a catalog, a destroyed catalog can have catastrophic effects on an agency's critical applications. Similarly, the computer-generated description for another critical problem we encountered stated "VTOC index space map can become corrupted for a 3350 or 3380 model E." (A VTOC, or volume table of contents, index space map is a critical data control file for disk storage devices, such as disk device models 3350 and 3380.) A corrupted VTOC can render the data on the entire device essentially unusable and can have severely disrupting effects on an agency's critical applications. Clearly, unresolved problems like these are a serious concern because they threaten the integrity of agency computer systems. Information systems management should take advantage of commercially available diagnostic software tools to guide preventive maintenance activities, thereby strengthening the overall system software management process.

#### Operating System Software Management Policies, Standards, and Procedures

Despite the importance and technical complexity of system software management, none of the nine MVS computer centers reviewed had adequate written policies, standards, or procedures pertaining to this crucial topic. Without such guidance, information systems management cannot be assured that operating system software (which controls agency computer systems) will be installed and maintained in a cost-effective manner that avoids introducing computer systems integrity exposures and vulnerabilities. In our opinion, had proper written guidance pertaining to operating system controls been issued and followed at the computer centers reviewed, many of the problems found--particularly the integrity exposures--probably would not have occurred. By providing quality, documented management guidance, agencies can minimize or even eliminate integrity exposures resulting from errors, omissions, or lack of adequate controls over operating system software.

#### Need to Strengthen Security Software Controls

Effective security requires the segregation of user duties so that no single user can circumvent the computer system's internal controls over the management and use of computer resources. An environmental security software package (in conjunction with an operating system that has its integrity intact) can achieve such segregation of duties by providing reasonable assurance that a computer system's hardware and software resources are being protected from accidental or deliberate modification or unauthorized use. In addition, security software provides the means to restrict and contain accidental or deliberate actions which could otherwise disrupt computer operations or cause errors and improper modification of valid information.

However, state-of-the-art security software packages are only as effective as the quality of their implementation and administration. From this perspective, Federal agencies have been unsuccessful in achieving computer systems integrity--as evidenced by the fact that all agency computer centers we reviewed had significant control deficiencies in security software implementation and administration. As shown below, these deficiencies included (a) improper technical implementation of security software features and (b) inadequate administrative controls. As a result, computer center operations are exposed to significant security risks which threaten the overall missions and goals of the Federal agencies.

---

PROFILE OF SECURITY SOFTWARE CONTROLS  
AT AGENCY COMPUTER CENTERS REVIEWED

	CONTROLS IMPLEMENTED? (NUMBER OF CENTERS)		
	YES	NO	UNK*
<b>TECHNICAL SECURITY SOFTWARE CONTROLS</b>			
Operational parameters/options:			
Critical system files adequately protected	2	6	2
Sensitive utility programs adequately controlled	0	7	3
Tape bypass label processing adequately restricted	2	6	2
Special security exposure interfaces installed	1	5	4
"Super users" adequately restricted	1	9	0
<b>ADMINISTRATIVE SECURITY CONTROLS</b>			
Security administered by independent staff	1	8	1
Adequate policies, standards, and procedures	0	8	2
Security violation reports effectively reviewed	1	8	1

---

\*UNK Unknown. In certain cases, the control dimension either could not be assessed or the results of the assessment did not fall clearly into either the "yes" or "no" category.

---

Technical Security Software Controls

The deficiencies we identified in the various agencies' compliance with generally accepted security practices when implementing security software centered around the (a) selection of parameters and other security-related options, and (b) assignment of user privileges. Only two centers had adequately protected all critical system files (e.g., APF libraries) from unauthorized access. In addition, none of the centers used security software to control sensitive system utility programs (e.g., "superzap," which can copy, modify, and destroy user and critical system data), users generally were not restricted from bypassing label security checks (referred to as bypass label processing) when accessing data residing on magnetic tapes, and special security exposure interfaces (required by certain powerful

software packages to bring them under the control of security software) generally were not installed. Further, the number of users assigned powerful security privileges (i.e., "super users") exceeded generally recommended limits. Collectively, these deficiencies made it virtually impossible for security software to enforce separation of duties between the various users of the computer systems reviewed. To ensure adequate protection of critical agency applications and other computer resources through software-enforced separation of duties, information systems management needs to improve its selection of operational parameters and assignment of user privileges when implementing environmental security software.

#### Administrative Security Controls

Eight of the ten agency computer centers did not have an independent group assigned to administer security software. In general, technical administration of computer security had been assigned to systems programmers, who also had numerous other important system software-related technical responsibilities (e.g., system software maintenance, computer performance monitoring and tuning, etc.). This arrangement violates the generally accepted data processing control practice of not assigning systems programmers to administer a computer center's security function. Because systems programmers at the majority of centers we visited controlled both security software and the operating system software supporting that security software, organizational separation of duties--where the activities of one employee act as a check on those of another--was not achieved. As a result, the controls provided by security software could not be fully relied upon. Information systems management must ensure independent system security administration and control by assigning this important function to a separate group.

Of the ten agency computer centers reviewed, eight lacked adequate computer security policies, standards, and procedures pertaining to the crucial area of security software use, and/or were not following such guidance. (Reviewing this topic at the other two agencies was impractical because of unique conditions affecting their security environments.) Without such guidance, information systems management cannot be assured that security software protecting agency computer systems will be implemented and administered in a cost-effective manner that minimizes security exposures and vulnerabilities. In our opinion, had proper written guidance pertaining to security software controls been issued and followed at the computer centers reviewed, many of the problems found probably would not have occurred. For example, at the eight agency computer centers where this issue was reviewed, no one was effectively reviewing security violation reports--a routine administrative task normally required by formal security policies, standards, and procedures. By providing quality, documented management guidance, agencies can minimize or even eliminate security software control weaknesses resulting from errors, omissions, or lack of adequate controls over security software.

Recommendations

We recommend that:

- OMB encourage Federal agencies to:
  - o develop effective policies, standards, and procedures for operating system software management and security software use;
  - o take advantage of commercially available diagnostic software tools to guide operating system preventive maintenance;
  - o carefully evaluate, and where appropriate adhere to, vendor guidelines in the management and use of operating system and security software; and
  - o use the reporting provisions of OMB Circular A-123 to identify operating system and/or security software weaknesses, where appropriate, as material internal control weaknesses.
- NIST, with technical advice and assistance from National Security Agency (NSA), develop and issue information systems management guidelines which cover both operating system and security software controls, specifically addressing operating system extension, protection, and maintenance and security software implementation and administration.
- NIST appropriately emphasize operating system and security software controls improvements in the computer security plans that are now being prepared in accordance with the Computer Security Act of 1987.
- NIST, with technical advice and assistance from NSA and GSA, develop training guidelines to ensure that Federal information systems managers are aware of the integrity and security risks posed by system software, such as certain commercially available products and public domain programs.
- GSA specify system software management as a Governmentwide priority area for review by Federal agencies under the Information Resources Management review process mandated by the Paperwork Reduction Act of 1980.

### III. IMPROVING MANAGEMENT OF DISK AND MAGNETIC TAPE STORAGE RESOURCES

OMB Circular A-130 and the Paperwork Reduction Reauthorization Act of 1986 require Federal agencies to use their information resources (which include disk and magnetic tape storage resources) in an efficient, effective, and economical manner. However, as shown by our computerized analyses of combined disk storage resources (methodology described in Appendix B) valued in excess of \$83.8 million, significant opportunities existed to improve disk storage management at all agency computer centers reviewed. In total, an estimated \$17 million in inefficiently used disk storage (\$16 million at the nine centers with IBM equipment, and \$1 million at the one center without IBM equipment) could be recovered and made available for reuse through the application of generally accepted disk storage management techniques--thereby reducing the need for future additional disk storage procurements. Similarly, as shown by our computerized analyses of magnetic tape storage (methodology described in Appendix B) at seven of the nine centers equipped with IBM computers, tape processing efficiency could also be significantly improved. In our opinion, the lack of formal storage management plans (addressing both disk and tape use) at 7 of the 10 agency computer centers contributed to the widespread inefficient use of disk and tape storage resources. Additional guidance is needed for agency information systems management to better focus attention on, and to strengthen controls over, disk and tape storage resources.

#### Need to Strengthen Disk Storage Management

Although the unit cost of disk storage technology has fallen dramatically since the 1970's, agencies continue to experience storage shortages and must endure lengthy procurement processes to acquire additional storage. Information systems managers have a vested interest in developing storage management plans and implementing generally accepted disk storage management techniques so that their agencies can achieve the best possible utilization of this resource. These techniques involve migrating (i.e., moving) inactive files from costly online disk storage devices to substantially cheaper offline magnetic tape storage, recovering unused disk space that has been allocated in excess of actual needs, and ensuring that disk space allocation is maximized according to the type of disk device in use. For example, \$17 million worth of disk storage<sup>1</sup> could be recovered for reallocation at the 10 computer centers we visited if agency information systems management (a) migrated to tape those disk files which have been inactive for 30 or more days, (b) released

---

<sup>1</sup> Because of the various ways (e.g., lease, rental, purchase, etc.) in which the nine agencies with IBM (or compatible) equipment procured their disk storage and the different points in time when it was acquired, we computed a standard cost for assigning a value to their combined disk storage resources. This standard cost was based on GSA schedule prices for purchasing IBM disk devices and associated control units, plus 5 years of maintenance. It excluded other significant cost components, such as floor space, electricity, and cooling costs, because figures for these items were not readily available.



unused space which has been overallocated, and (c) reorganized files to use at least 90 percent of disk device track capacity. Each of these techniques is easily accomplished using commercially available disk storage management software.

Need to Improve Tape Storage Management

Agencies can similarly save computer resources when processing magnetic tape files by ensuring that the files are created using efficient blocking techniques. (Blocking refers to the process of grouping logical records together and then writing them onto tape as one physical record, or block.) Performance studies have consistently shown that computer processing efficiency improves significantly when large blocks of data (referred to as large blocking factors) are specified for sequential files such as magnetic tape files. However, over three-fourths of the more than 730,000 magnetic tape files we analyzed at seven of the nine IBM computer centers were blocked for less than maximum efficiency (i.e.; using a blocking factor less than 90 percent of the largest blocking factor possible). Agency information systems management should encourage more efficient blocking of tape files to economically utilize computer processing resources.

Recommendations

We recommend that:

- OMB encourage Federal agencies, in carrying out their information resources management responsibilities, to develop and implement formal storage management plans that:
  - o provide for the use of generally accepted disk and tape storage management techniques such as those discussed in this report, and
  - o ensure the validity of disk storage requirements prior to procuring additional disk storage resources.
- NIST and GSA develop and issue information systems management guidelines for the efficient, effective, and economical use of disk and magnetic tape storage resources.
- GSA specify disk and magnetic tape storage management as a Governmentwide priority area for review by Federal agencies under the Information Resources Management review process mandated by the Paperwork Reduction Act of 1980.

PROFILE OF AGENCY MISSIONS, COMPUTER CENTERS  
REVIEWED, AND POTENTIAL ADVERSE IMPACT ON MISSIONS

Operating system exposures and security software control weaknesses like those discussed in this report pose significant risks to Federal agency information systems, thereby threatening agency missions. These weaknesses can be exploited by a knowledgeable perpetrator to gain unauthorized access to agency computer systems and misuse or destroy mission-critical information resources. When such a perpetrator takes advantage of system software vulnerabilities, the opportunity exists for a damaging event to result that may cause significant harm--such as monetary loss to the Government, reduced services to the public, financial hardship on recipients of Federal entitlement programs, adverse economic impact on the Nation, or unauthorized disclosure of sensitive information. Unless proper controls over system software are implemented, information systems managers are not sufficiently protected against such damaging events. In addition to providing a profile of agency missions and computer centers reviewed, this appendix describes the potential harm to agency missions (and to American taxpayers) from inadequate controls over operating system and security software at the centers we reviewed.

1. Department of Agriculture (USDA)

The USDA was established in 1862 to improve and maintain the agricultural environment and U.S. agricultural production capacity. Further, USDA helps to curb hunger and malnutrition, and ensures standards of quality in the daily food supply through inspection and grading services. In addition, the Department's research findings benefit all Americans either directly or indirectly. Its estimated budget outlay for FY 1988 is \$50.7 billion.

The USDA computer center reviewed is the Department's largest, and it supports critical data processing applications for all USDA agencies. These applications support USDA missions related to agricultural price support, loan, and crop insurance programs. The center's primary workload is supporting financial accounting systems which track over \$100 billion of obligations and expenditures. In addition, the center annually creates loan and direct payment authorization records totaling over \$10 billion. The center's two large-scale IBM computer systems both use the MVS operating system and CA-ACF2 environmental security software. Over 4,500 registered users access the facility through a nationwide telecommunications network, which includes both dedicated high-speed communications lines and public telephone system dialup support. The center, a Government-owned and Government-operated (GOGO) facility, has an operating budget of about \$41 million for FY 1988.

Inadequate controls over system software can result in unauthorized and/or inaccurate disbursements of the more than \$10 billion paid annually to 1.5 million participants under the Agricultural Price Support Program, Agriculture Loan Program, and Federal Crop Insurance

## APPENDIX A

Program. Further, accidental or intentional modifications of data made possible by such internal control weaknesses can lead to erroneous management decisions which in turn could adversely impact Federal agricultural programs in such areas as agricultural product pricing and production capacity.

2. Department of Energy (DOE)

The establishment of DOE in 1977 consolidated major Federal energy functions under one Cabinet-level Department. DOE serves as the framework for a comprehensive and balanced national energy plan through the coordination and administration of the Federal Government's energy functions. With an estimated budget outlay of \$10.5 billion for FY 1988, the Department is responsible for energy technology research and development; the marketing of Federal power; energy conservation; the nuclear weapons program; energy regulatory programs; and a central energy data collection and analysis program.

The DOE computer center reviewed provides sensitive data processing support for critical DOE programs. These critical programs include materials production, defense waste management, and naval nuclear propulsion. With an operating budget of about \$10 million for FY 1988, the center operates three large-scale IBM computer systems. One system is dedicated to classified data processing while the other two support unclassified data processing. All three systems use IBM's MVS operating system and security software developed inhouse. Further, one system uses the IBM Virtual Machine operating system in addition to MVS. Over 3,900 registered users access the facility through a local area network. The center, a Government-owned and Contractor-operated (GOCO) facility, has a small staff of Federal employees who provide general operational oversight on a day-to-day basis.

Inadequate controls over system software can adversely impact the Department's efforts to effectively and efficiently produce defense materials, control nuclear waste, and conduct research and development in energy technology. If critical mission-related data is accidentally or intentionally modified, DOE could experience erroneous management decisions, disruption to operations, compromise of proprietary data, and/or excessive program costs.

3. Department of Health and Human Services (HHS)

HHS is the largest Federal civilian agency. With an estimated budget outlay of \$375.1 billion for FY 1988, the Department administers such programs as retirement income and health insurance, research and treatment of disease, and regulation of the purity of foods and drugs sold in America. The Department's recordkeeping activities cover everyone issued a social security number as well as the thousands of employers who report the earnings of these individuals. It is also the oversight agency for the following five major operating administrations: Health Care Financing Administration, Social Security Administration, the Public Health Service, Family Support Administration, and Office of Human Development Services.

## APPENDIX A

The HHS computer center reviewed processes retirement income and health insurance program-related applications affecting most American citizens, currently paying out over \$200 billion in benefits annually to 40 million people. The computer center operates 14 large-scale computer systems, including Amdahl, NAS, IBM, and UNISYS computer systems. All systems except one, the UNISYS system, use IBM's MVS operating system, in conjunction with CA-TOP SECRET environmental security software. Over 44,100 registered users access the facility through a nationwide network of dedicated lines. The center is a GOGO facility.

The Nation's retirement income and health insurance programs, which disburse more than \$200 billion in annual benefit payments, affect almost every American citizen. Inadequate controls over system software can lead to unauthorized, inaccurate, and/or misdirected disbursements which could result in fraud or financial hardship to millions of program recipients. Further, accidental or intentional modifications of data made possible by such internal control weaknesses could reduce the level of quality of services to the public.

4. Department of Housing and Urban Development (HUD)

HUD, established in 1965, administers programs for mortgage insurance, rental subsidy, fair housing, construction and rehabilitation of rental units, and community and neighborhood development and preservation. Its budget outlay for FY 1988 is estimated at \$18.6 billion.

The HUD computer center reviewed supports the Department's critical housing-related grants and subsidy applications and application development requirements. With an operating budget of over \$1 million for FY 1988, the center operates three large-scale UNISYS computer systems. The center also uses Honeywell minicomputers for front-end processing. The Honeywell MENU System software provides security and allows over 7,000 registered users to perform data entry and/or remote batch or interactive processing with a choice of application systems and functions. Users access the facility from various sites through a nationwide telecommunications network, which includes both dedicated high-speed communications lines and public telephone system dialup support. The center, a GOCO facility, has a small staff of Federal employees who provide general operational oversight.

Strong system software controls are essential for HUD to efficiently and effectively meet its mission responsibilities related to fair housing and rental subsidy. Accidental or intentional modification of data, made possible by system software control weaknesses, can lead to the compromise of proprietary data and erroneous payments resulting in financial hardship to housing recipients and loss of Government funds. During FY 1987, the Department disbursed over \$13 billion for housing-related grants and subsidies.

5. Department of Transportation (DOT)

The founding of DOT in 1967 brought together some 30 Federal transportation bureaus and offices. The mission of DOT is to better foster and promote the various modes of transportation and to regulate

## APPENDIX A

them for the public's safety. With an estimated FY 1988 budget outlay of \$26.3 billion, the Department administers various transportation programs related to highways (Federal Highway Administration, National Highway Traffic Safety Administration); air traffic (Federal Aviation Administration); maritime (U.S. Coast Guard, Maritime Administration, and St. Lawrence Seaway Development Corporation); railroads (Federal Railroad Administration); and mass transit (Urban Mass Transportation Administration).

The DOT computer center reviewed is a major supplier of timesharing services to over 3,000 registered users. This center supports the processing of sensitive automated applications that are critical to the mission of the Department, involving transportation grants management, highway trust fund control, coastal search and rescue operations, and military payroll. The center operates a large-scale Amdahl computer system using IBM's MVS operating system and CA-ACF2 environmental security software. Users access the facility through a nationwide telecommunications network, which includes both dedicated high-speed communications lines and public telephone system dialup support. The center, a GOCO facility, has a small staff of Federal employees who provide general operational oversight. Its operating budget for FY 1988 is about \$20 million.

Strong system software controls are vital to protecting the integrity of DOT's mission-essential applications. With estimated disbursements totaling \$19 billion during FY 1987, inaccurate automated information could result in erroneous payments to vendors, grantees, and employees, and/or misuse of Federal funds. In addition, accidental or intentional modifications of data, made possible by system software control weaknesses, can undermine efforts to foster and promote the various modes of transportation and regulate public transportation safety--thereby resulting in reduced program effectiveness and/or excessive program costs. Further, the compromise of critical mission applications could indirectly lead to accidents involving loss of life, personal injury, and/or property damage.

#### 6. Department of the Treasury

The Department of Treasury was created in 1789 as the official fiscal agency of the Government. The Department had an estimated budget outlay of \$198.9 billion for FY 1988. In addition to tracking the Federal Government's annual budget deficits and total debt, the Department's functions include collection and protection of revenues, administration of import duties and regulations, printing of currency and coins, accounting for public debt securities, and collection of income and other taxes. Among the operating administrations performing these functions are the Financial Management Service, Internal Revenue Service, U.S. Mint, Bureau of Engraving and Printing, Bureau of the Public Debt, U.S. Customs Service, and the U.S. Secret Service.

The Treasury computer center reviewed operates one medium-scale and one large-scale IBM computer system, both running IBM's MVS operating system in conjunction with the CA-TOP SECRET environmental security package. This center supports 16 mission-critical financial

## APPENDIX A

applications of which the Check Payment and Reconciliation System was the major application during FY 1987--processing transactions representing aggregate payments exceeding \$1 trillion. Over 1,800 registered users access the facility through a nationwide telecommunications network. The center, a GOGO facility, has an operating budget of about \$10.2 million for FY 1988.

The data processing support provided by the computer center reviewed is vital to Treasury's mission responsibilities for tracking the Federal Government's annual budget deficits and protecting the Government's revenues. System software control weaknesses could thus undermine agency efforts to track and reconcile Government funds in excess of \$1 trillion. Further, such weaknesses can disrupt or obstruct check reclamation efforts, which in turn can result in financial losses to the Government due to duplicate, fraudulent, and/or erroneous payments.

7. Government Printing Office (GPO)

The GPO was established in 1860 to fill printing and binding orders placed by Congress and the various Federal agencies. GPO prepares catalogs and distributes and sells Government publications. It also furnishes blank paper, inks, and similar supplies on order. GPO's FY 1988 budget outlay is estimated at \$940 million.

The computer center operates two large-scale IBM computer systems using the MVS operating system and CA-TOP SECRET environmental security software. The center's 1,200 registered users access the facility through a telecommunications network which includes both dedicated communications lines and dialup telephone lines. The center, a GOGO facility, has an FY 1988 operating budget of about \$14 million.

Strong system software controls are essential for GPO to efficiently and effectively fill the printing and binding orders placed by the Congress and Federal agencies. For example, billing information is crucial to sustaining printing operations and the continued production of related goods and services. Inadequate system software controls could lead to erroneous or inaccurate tracking of billing and other automated financial information--which in turn could result in significant loss to the Government's printing operations and its customers.

8. National Aeronautics and Space Administration (NASA)

NASA was established in 1958 to plan, direct, and conduct aeronautical and space activities for peaceful purposes for the benefit of all mankind. With an estimated budget outlay of \$9.1 billion for FY 1988, NASA administers programs of a research and development nature that are designed to contribute to a number of national goals, including the preeminence of the nation in the science and technology of aeronautics and space.

## APPENDIX A

The NASA computer center reviewed is the major supplier of computer services to agency headquarters and supports sensitive data processing applications that are critical to NASA's mission. Such sensitive applications include financial management, procurement administration, reimbursable costs management, equipment and inventory control, payroll and personnel, and resources management. The center operates two medium-scale IBM computer systems, both running IBM's MVS operating system in conjunction with CA-ACF2 environmental security software. About 850 registered users access the facility through a local area network and remote access dedicated high-speed communications lines. The center, a GOCO facility, has a small staff of federal employees who provide general operational oversight. Its operating budget for FY 1988 is over \$3 million.

System software control weaknesses at the NASA computer center reviewed could lead to unauthorized or inaccurate payments to employees and vendors, resulting in loss of Government funds and interruption of mission-related activities. Moreover, such integrity exposures undermine NASA's efforts to efficiently and effectively plan, direct, and conduct its aeronautical and space activities.

9. Office of Personnel Management (OPM)

OPM, established in 1978 to replace the Civil Service Commission, is tasked with ensuring that the Federal Government provides essential personnel services to applicants and employees. With an estimated budget outlay of \$28.5 billion for FY 1988, the Office administers a merit system for Federal employment which calls for recruiting, examining, training, and promoting people only on the basis of their knowledge, skills, and abilities, regardless of their race, religion, sex, or other nonmerit factors. OPM is also charged with administering benefit programs for Federal employees. In that regard, OPM administers the Civil Service Retirement System (CSRS), a large, automated application which provides monthly pension benefits to Federal Government retirees. This mission-critical application disburses annuities totaling about \$21.6 billion annually to 1.9 million annuitants. In addition to monthly check issuance, OPM oversees all CSRS processing associated with adjudication of new retirement cases and adjustment of existing accounts.

The OPM computer center reviewed provides data processing support for CSRS. With an FY 1988 operating budget of about \$6 million, the center operates one large-scale and one medium-scale IBM computer system. Both computers use the MVS operating system and commercial security software packages which protect only certain online environments. About 350 registered users access the facility through a network of local terminals. The center is a GOGO facility, but has an onsite contractor providing software maintenance support.



## APPENDIX A

Integrity weaknesses in the system software controlling the CSRS can lead to unauthorized and/or inaccurate annuity payments (including the theft of Government funds) and economic hardship for program recipients. Further, accidental or intentional modifications of data made possible by system software control weaknesses can lead to excessive costs of Government operations.

10. Veterans Administration (VA)

The VA was established in 1930 to serve America's veterans and their families by ensuring that they receive quality medical care, appropriate levels of benefits, adequate compensation, decent working conditions, necessary training and education, and equal employment opportunity. It has an estimated FY 1988 budget outlay of \$27.6 billion.

The VA computer center reviewed is a major supplier of timesharing services to over 5,000 registered users. The center supports more than 76 mission-critical applications associated with every major VA program. These critical applications include VA-owned home mortgage loans; VA-owned facility construction, expansion, and upgrading appropriations; civilian payroll and personnel; and financial accounting systems. Collectively, these applications disbursed about \$9.7 billion during FY 1987 for goods, services, and personnel costs. The center operates two large-scale Amdahl computer systems using IBM's MVS operating system in conjunction with CA-TOP SECRET environmental security software. Users access these systems through a nationwide telecommunications network, which includes dedicated communications lines and public telephone system dialup support. The center, a GOGO facility, has an FY 1988 operating budget of about \$50 million.

The majority of VA's programmatic and administrative applications are supported by the computer center reviewed. System software control weaknesses at that center could lead to accidental or deliberate modification of application data--which in turn could cause financial hardship to millions of American veterans and their families. In addition, the disruption of these critical applications could debilitate agency efforts to provide veterans with quality medical care, decent working conditions, adequate training and education, and equal employment opportunity.

AUDIT METHODOLOGY AND GUIDELINESOverview of Audit Methodology

An operating system has integrity if it can (1) prevent one program from interfering with or modifying another program's execution--unless "authorized" to do so, and (2) protect itself against unauthorized access by ensuring that integrity controls cannot be bypassed. This basic definition--embodying the concepts "authorized program" and "authorized user"--guided the formulation of our audit objectives and the development of a methodology for meeting those objectives. MVS integrity controls can ensure that only authorized programs (i.e., those meeting standard MVS authorization conventions) can gain the sensitive powers needed to modify another program's execution. These controls, however, are not intended to ensure that only authorized users can execute sensitive authorized programs. Control of authorized users is provided by environmental security software, which is crucial but optional for MVS environments.

Thus, the primary objectives of our MVS system software controls audit were to determine whether (1) operating system features which control the ability to perform sensitive tasks (i.e., execute authorized programs) were properly administered and controlled, and (2) environmental security software mechanisms which control user access to computer resources were properly administered and controlled. In addition, because the computer assisted audit techniques we employed to assess system software controls also provided the capabilities for assessing disk and tape storage management, we performed such an analysis as a subordinate audit objective. The remainder of this appendix provides brief descriptions of the computer assisted audit techniques we used, the general methodology and audit steps we employed to meet each audit objective, and audit references including industry guidelines on system software management and security software implementation which we used to supplement Federal computer systems integrity and information resources management requirements.

Computer Assisted Audit Techniques Used

The automated tools and techniques used consisted of (1) DOT-developed computer programs (collectively referred to as the "Scrubber" system), (2) a public domain software analysis program (called an object code "disassembler"), (3) specialized MVS utility programs (classified by IBM as service aids), (4) IBM's Interactive Systems Productivity Facility (ISPF) program product, (5) vendor-provided security package reporting programs, and (6) a commercially available MVS-oriented system software diagnostic package known as Problem Alert System (PAS) (described in Appendix C).

The Scrubber system is an integrated set of Basic Assembly Language routines and Dylakor, Inc., (i.e., DYL-260 and DYL-280) data retrieval and analysis software programs which analyzes MVS operating system software. Certain Scrubber routines analyze large, complex sets of APF libraries and critical operating system control tables which are all key control points regarding MVS integrity. Scrubber also analyzes certain aspects of disk

## APPENDIX B

storage usage and, for installations using the CA-1 tape management system package, tape processing efficiency. The public domain disassembler program assists in analyzing certain critical operating system routines (primarily SVCs) for integrity exposures. The IBM service aids, AMBLIST and AMASPZAP, assist in reviewing system software program modifications and control tables, respectively. ISPF was used as the primary timesharing operating environment in which we conducted many of our technical review activities, such as job processing, output retrieval, system software file review, and miscellaneous data management. Finally, utility reporting programs, which are standard components of commercially available environmental security software packages like CA-ACF2 and CA-TOP SECRET, provided critical information regarding an installation's selection of parameters, security-related options, and assignment of security privileges to system users.

### Review of Operating System Software Controls

Operating systems, such as IBM's MVS, generally have very elaborate control mechanisms designed specifically to ensure processing integrity. These control mechanisms isolate and protect numerous simultaneously processing tasks from one another. As indicated above, only authorized programs should have the capability to perform sensitive tasks such as accessing and modifying another program's execution or data areas. The key mechanism in IBM's MVS operating system for controlling such capabilities is APF. That is, MVS will allow programs to perform sensitive tasks only if they have first been identified according to APF conventions. If a program can gain the capability to perform such sensitive tasks outside of normal APF conventions, then MVS' integrity has been compromised, and all applications and data are at risk of unauthorized access, manipulation, destruction, or disclosure. Audit experience has shown that poor APF administration and the improper modification (i.e., corruption) of key operating system components by an installation results in the compromise of system integrity controls.

### Documenting the System Software Environment

This set of audit steps involved developing a basic understanding of the system software environment under review and making a preliminary assessment of nontechnical controls. Organization and staffing of the computer center's technical support function (i.e., primarily the systems programming group) was reviewed to evaluate such control areas as separation of duties, personnel qualifications, and documented procedures for staff management. General management and specific technical direction were also reviewed, addressing such critical control areas as system software management policies, standards, procedures, and change control. In addition, an inventory of computer hardware and software was developed to validate the configuration under review.

### System Generation and Initialization

This set of audit steps focused on two key technical control areas--operating system extension, primarily involving locally added SVCs, and human intervention in the system initialization process. As

## APPENDIX B

discussed in the body of the report, controls over the addition of non-MVS vendor tested SVCs is crucial to preserving MVS integrity. Also highly desirable, is minimizing the role of the computer operator during system startup (also referred to as initial program load (IPL)) to avoid accidental or intentional modifications to critical MVS control parameters (as specified in the MVS library named SYS1.PARMLIB). Initialization parameters for the Job Entry Subsystem (JES), a critical MVS subsystem controlling the entry of work into the system and disposition of job output, were reviewed for controls over user submission of operator commands and JES processing integrity. The Scrubber system, disassembler, and IBM's ISPF file management and display functions were used in performing these audit steps.

APF Administration

This set of audit steps was included to determine whether computer center management had promulgated integrity guidelines, as recommended by the vendor, and was generally complying with the vendor's recommendations for proper APF administration and control. APF works on the assumption that if the first module in a program sequence is authorized, then authorized individuals have determined the flow of control to all subsequent modules in that sequence. MVS considers these modules authorized to use sensitive system functions as long as they come from authorized libraries. As a result, the installation must follow certain critical guidelines when using APF. Specifically, information systems management must:

- Ensure that all programs that will run as authorized programs adhere to the installation's integrity guidelines and to MVS system integrity requirements.
- Control which programs are stored in authorized libraries.
- Protect authorized libraries through environmental security software to ensure that only selected users can store or alter programs in these libraries.
- Ensure that no two load modules with the same name exist across the set of authorized libraries. (Two modules with the same name could lead to accidental or deliberate mixup in module flow, possibly introducing an integrity exposure.)
- Ensure that the SYS1.PARMLIB library does not contain the names and volume serial numbers of data sets that no longer exist. (If it does, a user could assign his/her own data sets with the same names to those volumes and cause his/her own libraries to become authorized.)
- Ensure that volumes specified in SYS1.PARMLIB are mounted at IPL and are permanently resident. (Otherwise, a user could introduce a "counterfeit" APF library by supplying his own disk volume.)

The Scrubber system, IBM's AMASPZAP service aid, and IBM's ISPF file management and display functions were used to review the APF library environment.

## APPENDIX B

System Software Maintenance

This set of audit steps addressed the computer center's system software maintenance activities. MVS maintenance is an important control area because of its impact on system integrity and security, the sheer complexity and magnitude of fixes provided by the vendor to correct operational problems, and its significant burden on the typically severely strained technical support staff. The vendor ships maintenance tapes to MVS customer sites about nine times a year, with each tape containing about 1,500 to 2,000 fixes for the typical MVS installation. Some of the corrections included with each maintenance tape are basic system integrity fixes. MVS maintenance should be performed under the absolute control of the vendor's SMP and software corrections should be made in a preventive maintenance mode (i.e., compensating operational adjustments are made to temporarily circumvent unresolved system software problems, and/or fixes are applied as soon as practicable after they are made available by the vendor.) The Scrubber system and IBM's AMBLIST service aid were used to identify potential instances where maintenance was applied to system software program libraries outside of the controls of SMP. The PAS package (see Appendix C) was used to assess the status of vendor-supplied maintenance actions.

Review of Security Software Controls

IBM's MVS operating system, through the APF mechanism, can control the execution of sensitive tasks, but has no way of detecting and controlling who is executing the sensitive tasks (i.e., determining whether an authorized program was submitted by an authorized user). Effective control of "authorized users" generally requires specialized environmental security software, such as RACF, CA-ACF2, or CA-TOP SECRET. The following audit steps were designed to evaluate both generic and product-specific security software controls. Utility reporting programs, which are standard components of commercially available environmental security software packages, were used where appropriate to obtain critical security profile information.

Documenting the General System Security Environment

This set of audit steps involved developing a basic understanding of the computer center security environment under review. Organization and staffing of the computer center's security function was reviewed to evaluate such control areas as separation of duties, personnel qualifications, and documented procedures for staff management. General management and specific technical direction were also reviewed, addressing such critical control areas as security software management policies, standards, procedures, and user registration change control. In addition, a technical security profile was developed to evaluate the center's selection of parameters, implementation of security-related options, and assignment of security privileges to system users. Regardless of the type of security software used by the installation, the following general areas of concern were reviewed:

- The universe of "super users"--i.e., those with especially powerful security privileges.

## APPENDIX B

- Access profiles for sensitive system files affecting integrity, security, and general operational control.
- Controls over sensitive system utility programs.
- Security software parameters implemented, such as minimum password length, number of access attempts allowed, etc., and the security system's production mode of operation (e.g., abort, warn, etc.).
- Disposition of security logging and reporting facilities.
- Controls over tape bypass label processing.
- System software program products requiring special interface with the installation's security software.

Environmental Security Package Review

For those seven installations using a commercially available environmental security software package, we applied the vendor's audit-related guidance to the extent practicable. Examples of vendor-provided guidance are the RACF Auditors Guide, CA-ACF2 Auditors Guide, and CA-TOP SECRET Auditors Guide.

Review of Disk and Tape Storage Resources

The purpose of this set of audit steps was to assess whether disk and magnetic tape storage resources were being economically, efficiently, and effectively used. Using the Scrubber system, we developed a profile of the disk environment by scanning the VTOCs of all online disk devices and building a data base of all online disk data set names and attributes. From the disk data base, we summarized utilization statistics by disk device type (e.g., 3330, 3350, 3380) for data set activity, blocking efficiency (based on a minimum track utilization of 90 percent), releasable space, and presence of invalid data sets. We also calculated potential storage savings under five alternative policies for migrating inactive disk data sets to tape. These policy alternatives covered disk data sets which have not been accessed for 180, 90, 60, 45, and 30 days, respectively. (By calculating storage savings under alternative migration policies, computer center managers can perform sensitivity analyses on the alternative policies.) A similar analysis was performed, again using the Scrubber system, on tape-based data sets. Through this analysis we identified those data sets most likely to encounter permanent read errors due to media age, and those having blocking factors not conducive to efficient processing.

Audit References

The following audit references include industry guidelines on system software management and security software implementation which we used to supplement Federal computer systems integrity and information resources management requirements.

1. "System Software Controls," Evaluating Internal Controls in Computer-Based Systems, Audit Guide, Section V, Questionnaire 8, Publication AFMD-81-76, U.S. General Accounting Office.

APPENDIX B

2. "Examine/MVS Concepts and Facilities and Usage Guides", Rosemont Development and Support Center, Computer Associates International.
3. "MVS Security," GC28-1400-D, IBM.
4. "Problem Alert System (PAS) User Guide," Morino Associates, Inc.
5. "PAS Systems Software Management Methodology," Morino Associates, Inc.
6. "OS/VS2 Conversion Notebook," GC28-0689-6, IBM.
7. "OS/VS2 MVS System Programming Library: Initialization and Tuning Guide," GC28-1029-4, IBM.
8. "MVS/XA MVS System Programming Library: Initialization and Tuning Guide," GC28-1149, IBM.
9. "Auditing the Technical Support Function," Chester M. Winters, EDPACS, Volume XII, No. 8, February 1985, Automation Training Center.
10. "Auditing an MVS Operating System," Auerbach Information Management Series, EDP Auditing, 75-04-30.
11. "ACF2 Auditor's Guide," Rosemont Development and Support Center, Computer Associates International.
12. "RACF Auditor's Guide," SC28-1342-3, IBM.
13. "CA-TOP SECRET Auditor's Guide," Computer Associates International.
14. "ACF2 Other Products Manual," Publication No. ABP0011-01, Chicago Development and Support Center, Uccel Corporation.
15. "DP Policies and Procedures," Robert E. Umbaugh, The AUERBACH Data Processing Management Library, Volume 1: A Practical Guide to Data Processing Management.
16. "The Auditor's Use and Control of Utility Programs," Michael I. Sobol, The AUERBACH Data Processing Management Library, Volume 7: EDP Auditing.

DEFINITION OF SYSTEM SOFTWARE PROBLEM ANALYSIS  
MANAGEMENT AREAS AND SEVERITY LEVELS

This appendix defines the management areas and severity levels associated with the system software problems reported by the MVS diagnostic software package used during this task to review the status of system software maintenance. This diagnostic software package--Morino Associates, Inc.'s PAS--consists of a software maintenance analyzer, a data base describing thousands of MVS-related system software problems, and a reporting subsystem which produces summary and detail level reports. The purpose of the package is to help MVS installations reduce security and integrity exposures, minimize the risk of disabling service disruptions, and decrease vulnerability to data deletion and/or destruction.

The opportunity for unresolved system software problems exists in virtually all MVS computer systems because of software complexity, interaction between software packages, interaction between hardware and software, and human resource limitations. Timely and thorough preventive maintenance is the key to minimizing these problems and avoiding altogether the problems which can produce catastrophic effects on Federal agency computer systems. As described below, effective use of PAS can help managers of MVS systems assess the adequacy of preventive system software maintenance at their installation.

PAS Management Areas

To facilitate review and prioritization of problems applicable to an installation, PAS classifies MVS system software problems by specific management areas. These logical groupings can be related to specific areas of interest or concern reflecting management objectives and priorities. While not all problems fit exactly and consistently into them, the following defined management areas are used to account for the items in the PAS data base:

**PERFORMANCE AND CAPACITY** - Problems with critical system resources (e.g., central processing unit or CPU, real storage, virtual storage, disk space, etc.) or functions (e.g., paging, swapping, processing delay, etc.) which adversely affect the system's ability to satisfy service level objectives and availability requirements. Examples include (1) the performance of unnecessary CPU instruction processing for a given function, (2) the need for excessive input/output operations or device/controller/channel resources, and (3) unnecessary delay in performing services for a program or function which is ready to execute.

**SECURITY** - Problems involving system integrity and related functional errors which adversely affect security. Examples include (1) MVS system integrity corrections excluding data integrity problems, (2) an erroneous or incomplete security-related function such as failure to protect a data set or failure to update or delete a RACF security



## APPENDIX C

profile, and (3) erroneous or incomplete security-related records or messages on successful and unsuccessful resource access requests.

MEASUREMENT AND ACCOUNTING - Problems with the accuracy and completeness of system resource measurement and task event data. Examples include (1) erroneous or incomplete resource utilization or logging data--principally System Management Facility (SMF) and Resource Measurement Facility, (2) errors associated with SMF exits, and (3) implementation errors which prevent performance of a required operation or cause incorrect or incomplete results.

WORKLOAD CONTROL - Problems with the management, control, and prioritization of jobs which impair the system's ability to get work accomplished. Examples include (1) problems with data management and JES exits commonly used for workload management functions, (2) implementation errors preventing the appropriate controls or priorities from being used, and (3) failure to enforce installation performance-related controls and service objectives.

OPERATION AND EXECUTION - Problems with operator console functions, system services, and device support. Examples include (1) system operator controls or facilities not performing as intended, (2) job control language functions not performing as expected, and (3) inadequate support for new devices or device features.

INTERNAL RELIABILITY - Problems that cause system abnormal ends (ABEND), perpetual wait, and looping conditions. Examples include (1) an unexpected program ABEND due to a programming error or invalid data, (2) an unending wait state created by processing a program containing a request for a resource which is permanently unavailable, and (3) a programming error causing the same instruction or group of instructions to be executed repeatedly (if CPU interrupts are disabled during this loop, all applications may suffer loss of service, and a total system restart may be required).

EXTERNAL RELIABILITY - Problems involving data damage, device error, and incorrect, duplicate, or missing data. Examples include (1) the damaging or destruction of external data (e.g., VTOC, catalog, system, or user data set), (2) a programming error causing an external device to terminate input/output with an ABEND, and (3) erroneous or incomplete critical operating system error recording file information.

UNASSIGNED - Problems which do not fit any of the above classifications.

## APPENDIX C

PAS Severity Levels

In assigning severity levels to MVS problems, PAS attempts to reflect the impact a given system software error is likely to have on an installation. The three possible problem severity levels and the conditions they represent are:

**CRITICAL** - Generally results in substantial adverse impact on performance, security, user or system data sets, measurement data, or system availability. One or more of the following conditions may be present.

- Failure of the entire system (resulting from a disabled loop or hard wait state) or loss of a processor in an attached processor, multiprocessor, or dyadic configuration.
- Unrecoverable error and/or loss of a critical system component or subsystem which either precludes continued system operation or severely limits it.
- Significant performance degradation to entire system (even if it degrades gradually).
- Total exhaustion of a resource, such as the common service area (CSA) and system queue area (SQA) (critical pools of virtual storage), which prevents introduction of new work.
- Loss of an external resource or facility which is critical to continued system operation, such as damaged page, swap, spool, catalog, SMF, RACF, or other critical system data sets.
- System or component errors or damage which cause loss of significant system capability (such as initiator or timesharing logon failures).
- Problems in device error recovery procedures which lead to job failure or incorrect data.
- Errors that cause discontinuance of a significant logging, auditing, or diagnostic capability (such as SMF or system error recording) or the inability to produce a system or stand-alone storage contents listing.
- Errors involving failure to release enqueued resources or MVS locks, which lead to eventual wait state in multiple address spaces.
- Any problems which result in overlay of common storage areas, such as the nucleus, SQA, CSA, and link pack area. The actual results may be unpredictable, depending on the system use of the damaged area.

## APPENDIX C

IMPACTING - Problem impact is less severe than critical or is limited to certain users or applications. One or more of the following conditions may be present.

- Moderate system performance degradation on a global basis, or affecting all users of a common function or program, or applicable to a single component or subsystem.
- Failures resulting from storage overlays or program errors which terminate all user sessions within a restricted subset (such as all ISPF users or all jobs using a particular access method).
- All MVS system integrity corrections.
- Security-related (RACF or password) errors which may impact all users of a common system service such as disk allocation or scratch.
- Partial loss or waste of internal or external resources such as global storage (CSA/SQA) or disk space.
- SMF and other recording data errors which result in significant loss of valuable information or substantial distortion of important values such as resource utilization counts or timings.
- Loss of a single user address space or initiator due to a wait state or loop condition.
- Damage to a nonglobal resource or facility, such as a damaged user volume, VTOC, user catalog, or user data set.

LIMITED - Problem is more limited and/or less severe than the higher severity levels described above, but should not be considered trivial. One or more of the following conditions may be present.

- Failure is limited to those jobs or sessions using an infrequently used system function or optional subfunction.
- All SMF and recording data errors not classified as critical or impacting.
- Moderate performance degradation for a single user, or for all users of a limited-use function or program.
- User data damage resulting from situations with a low probability of occurrence.
- Minor to moderate performance degradation of a facility or device which is not significant to overall system performance.
- Security-related (RACF or password) errors confined to a single user or data set.
- System or component failures which may be significant but which have a low probability of occurrence.

INDIVIDUAL AGENCY REPORTS  
ISSUED UNDER TASK 2A

Agency and Product Title	Type of Report and Number	Date Issued
<u>Department of Agriculture</u>		
PCIE Computer Systems Integrity Project	Interim Report 58099-10-FM	02-12-88
PCIE Computer Systems Integrity Project	Interim Report 58099-10-FM	03-10-88
Office of Information Resources Management PCIE Computer Systems Integrity Project National Computer Center At Kansas City	Final Report 58099-10-FM	09-30-88
<u>Department of Energy</u>		
Audit of Central Computer Systems Integrity at the Savannah River Plant	Final Report ER-0-88-06	07-29-88
<u>Department of Health and Human Services</u>		
Social Security Administration, Systems Software Internal Control Review	Final Report CIN-A13-88-00011	10-11-88
<u>Department of Housing and Urban Development</u>		
General Controls Over Computer Operations	Final Report 85-AA-166-0004	07-25-85
Computer Access Controls	Final Report 88-AA-166-0001	08-22-88
<u>Department of Transportation</u>		
Report on Observations Regarding System Software Control Weaknesses at the Transportation Computer Center	Interim Report * AD-OT-5-004	02-28-85
Report on the Need for Stronger Management Controls Over Disk Storage at the Transportation Computer Center	Final Report AD-OT-5-011	08-16-85
Report on Internal Control Weaknesses in Operating System Software and Major Subsystems at the Transportation Computer Center	Final Report * AD-OT-6-003	03-27-86
Report on Control Weaknesses in the Implementation and Administration of Access Control Software at the Transportation Computer Center	Final Report * AD-OT-7-004	06-02-87

\* Contents Restricted

INDIVIDUAL AGENCY REPORTS  
ISSUED UNDER TASK 2A

Agency and Product Title	Type of Report and Number	Date Issued
<u>Department of the Treasury</u>		
Internal Audit Memorandum - Unauthorized Access Exposure	Interim Report * No Number	12-23-87
Audit Memorandum -- Operating System Software Maintenance	Interim Report * A-FM-88-002	02-23-87
Computer System Integrity at the Financial Management Service	Final Report * OIG 88-078	09-14-88
<u>Government Printing Office</u>		
Management of System Software, Access Security, and Resource Management Can Be Improved	Final Report 88-36	07-29-88
<u>National Aeronautics and Space Administration</u>		
Interim Report on the Computer Systems Integrity Project	Interim Report A-HQ-88-001	10-20-87
Final Report on The PCIE Computer Integrity Task 2A Audit of the NASA Headquarters Computer Center (NHCC)	Final Report A-HQ-88-001	07-22-88
<u>Office of Personnel Management</u>		
Possible Weakness for Director's A-123 Report	Interim Report 88-21(M)	12-09-87
Final Report on PCIE Computer Security Audit of the WDPC	Final Report 88-37	06-03-88
<u>Veterans Administration</u>		
Audit of Austin Data Processing Center Program and Data Security	Final Report * 8AD-G07-121	09-30-88

\* Contents Restricted

ASSESSMENT OF SYSTEM SOFTWARE CONTROLS  
AT 10 FEDERAL COMPUTER CENTERS

<u>CONTROL CATEGORY</u>	<u>NUMBER OF CENTERS</u>			
	<u>STRONG</u>	<u>MARGINAL</u>	<u>INADEQUATE</u>	<u>UNKNOWN</u>
Operating System Software Controls: <sup>1</sup>				
Extension (SVC) controls	0	1	8	0
Protection (APF) controls	0	1	8	0
Maintenance controls	1	1	7	0
Policies, standards, procedures	0	3	6	0
Security Software Controls:				
Technical controls	0	0	7	3
Administrative separation of duties	1	1	8	0
Policies, standards, procedures	0	4	4	2
Security violation report review	1	0	8	1

## Legend:

- Strong - No significant control deficiencies found nor any major integrity or security exposures identified (e.g., for the security violation report review category, center security staff were effectively reviewing and investigating violations reported by security software).
- Marginal - One or more significant control deficiencies found but no resulting major integrity or security exposures confirmed; however, development of such exposures in the future was highly likely (e.g., for the policies, standards, and procedures control category, existing guidance either did not sufficiently cover all system software management areas or was only partially implemented).
- Inadequate - One or more significant control deficiencies found which produced at least one major integrity or security exposure (e.g., for the technical security software controls category, all critical system software files were not adequately protected from unauthorized access).
- Unknown - Not all elements of specified control category evaluated at these centers. Thus, at best, only a partial assessment of overall control effectiveness could be made--producing results not comparable to those at centers where all control elements were evaluated.

<sup>1</sup>The one non-MVS computer center was excluded from this portion of the audit. Thus, evaluations were performed at 9 of the 10 centers reviewed.



**UNITED STATES DEPARTMENT OF COMMERCE**  
**National Institute of Standards and Technology**  
**(formerly National Bureau of Standards)**  
Gaithersburg, Maryland 20899  
OFFICE OF THE DIRECTOR

SEP 23 1988

John W. Melchner  
Inspector General  
Department of Transportation  
Room 9210  
400 Seventh Street, SW  
Washington, DC 20590

Dear Mr. Melchner:

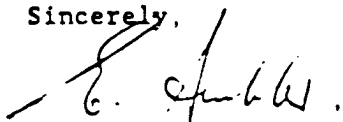
The National Institute of Standards and Technology (NIST) has received and reviewed the draft Summary Report for Task 2A of the PCIE's Computer Systems Integrity Project. We commend the PCIE and the project staff for an outstanding job of assessing management controls over system software and over disk and tape management. We support the conclusions of the report regarding the vulnerabilities caused by inadequate system software controls and the opportunities for improved efficiency in disk and tape management in Federal computer systems.

We are in general agreement with the recommendations of the report and believe that the NIST Computer Security program is already moving in the directions indicated. NIST, as part of its ongoing Computer Security Program and its activities under Public Law 100-235, expects to provide additional guidance in several areas affecting improved privacy and security of Federal computer systems -- including those areas addressed in the report. It is expected that agencies will address systems software controls as one of several areas of controls in their security plans for sensitive systems as required under the law. NIST and others are working to increase the security and integrity features of commercially-available computer systems.

In addition, we believe that emphasis should be placed on the report's recommendation that Federal agencies develop their own policies and procedures for effective systems software management controls, including adherence to vendor guidance and recommendations. This is particularly important, since each agency will have its own, vendor-specific, systems environment for which government-wide guidance will simply be too broad and general in scope. It would be impractical and inappropriate for NIST, GSA, or any other agency to attempt writing guidance directed to specific vendor systems, regardless of how extensive their use in the Federal Government.

Again, we commend the Council and its project staff on a fine job in the Task 2A report. If you have specific questions, please contact Dennis Steinauer, Computer Security Management Group, at (301) 975-3359.

Sincerely,

A handwritten signature in dark ink, appearing to read "E. Ambler", written over a horizontal line.

Ernest Ambler  
Director



# NATIONAL COMPUTER SECURITY CENTER

FORT GEORGE G. MEADE, MARYLAND 20755-6000

Serial: C-306-88  
7 October 1988

John W. Melchner  
Inspector General  
Department of Transportation  
400 7th Street SW  
Washington, DC 20590

Dear Mr. Melchner:

1. We have reviewed the portions of the PCIE Draft Report that are relevant to the National Computer Security Center's (NCSC) mission. We agree with those comments and recommendations.

2. We have two specific comments. First, we believe the phrase "commercially available system software products meet minimum computer system integrity requirements . . ." needs clarification both in terms of what is meant by "integrity" and what is meant by meeting "minimum requirements," i.e., whose requirements? We have already relayed these two comments to Mr. John Lainhart at the Department of Transportation. Mr. Lainhart remarked that the report uses "integrity" in its generic sense, not in the more technical and specific sense we associate with it.

3. We would be pleased to support the recommendation that OMB work with NSA and the National Institute of Standards and Technology in areas that touch the civil and private sectors, as long as it is within the purview of PL 100-235, the Computer Security Act of 1987.

4. The PCIE Draft Report again emphasizes the need for better computer security measures to protect sensitive unclassified data. The NCSC is prepared to assist OMB in any way we can to overcome the current deficiencies in federal computer systems.

Sincerely,

  
PATRICK R. GALLAGHER, JR.  
Director

Serial: C-306-88

Copy Furnished:

June Gibbs Brown  
Inspector General  
Department of Defense  
400 Maryland Avenue SW  
Mail Code W  
Washington, DC 20546



General Services Administration  
Information Resources Management Service  
Washington, DC 20405



SEP 19

MEMORANDUM FOR KAREN SHAFFER  
OFFICE OF THE INSPECTOR GENERAL

FROM: TOM HORAN *T. Horan*  
CHIEF, PROCUREMENT AND MANAGEMENT  
REVIEWS BRANCH

SUBJECT: Comments on PCIE "Draft Report for Computer  
Systems Integrity Project, Task 2A: Review of  
General Controls in Federal Computer Systems

The project team did an outstanding job in its review of general controls. Although security and electronic media storage been identified as important governmentwide priorities by OMB and others, the PCIE team was able to document specific deficiencies that highlight the urgent need for agencies to address these functions immediately. We strongly agree with the recommendations of the PCIE, particularly those that pertain to our Governmentwide review function.

Regarding the recommendation that OMB work with GSA to specify system software controls as a Governmentwide priority area for review by Federal agencies under the Information Resources Management review process mandated by the Paperwork Reduction Act of 1980 on page 15 of the draft report:

Each year, in our annual data call for plans and synopses of agency-conducted IRM reviews, we encourage agency officials to consider the most recent information technology priorities addressed by OMB. In the past, OMB has communicated these areas of emphasis through two publications: "A Five Year Plan for Meeting the ADP and Telecommunications Needs of the Federal Government" and, most recently, "Management of the United States Government."

It should be noted, however, that OMB and GSA are relying upon agency officials to focus review efforts upon those areas which best meet individual agency needs. Establishment of system software controls as a governmentwide priority will not guarantee that agencies focus their efforts on this particular area.

- 2 -

Security has been identified as a priority item ever since passage of the Security Act of 1987 and publication of OMB Circular A-130. However, since system software controls have not been specifically addressed, and in light of the findings of the Computer Systems Integrity Project, software controls could be singled out for executive level attention in future OMB planning documents.

Regarding the recommendation that OMB work with GSA to specify disk and magnetic tape storage management as a Governmentwide priority area for review by Federal agencies under the Information Resources Management review process mandated by the Paperwork Reduction Act of 1980 on page 18 of the draft report:

Electronic recordkeeping has been and will continue to be a governmentwide priority under the Federal IRM Review Program. Since management of electronic storage media falls within the category of electronic recordkeeping, we believe that OMB should address the issue within the context of electronic recordkeeping in its future planning documents. Perhaps the PCIE should make it clear to OMB that efficient management of electronic storage media deserves recognition as a separate priority category.

We also support the establishment of governmentwide guidelines and standards in both of these areas by OMB, NSA, NBS and GSA.

LIST OF ACRONYMS

ABEND	Abnormal End
ADP	Automatic Data Processing
APF	Authorized Program Facility
CA-ACF2	Computer Associates' Access Control Facility 2
CPU	Central Processing Unit
CSA	Common Service Area
CSRS	Civil Service Retirement System
DOE	Department of Energy
DOL	Department of Labor
DOT	Department of Transportation
FY	Fiscal Year
GOCO	Government-owned and Contractor-operated
GOGO	Government-owned and Government-operated
GPO	Government Printing Office
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
IBM	International Business Machines Corporation
IPL	Initial Program Load
ISPF	Interactive Systems Productivity Facility
JES	Job Entry Subsystem
MVS	Multiple Virtual Storage
NAS	National Advanced Systems
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PAS	Problem Alert System
PCIE	President's Council on Integrity and Efficiency
RACF	Resource Access Control Facility
SMF	System Management Facility
SMP	System Modification Program
SQA	System Queue Area
SVC	Supervisor Call
USDA	Department of Agriculture
VA	Veterans Administration
VTOC	Volume Table of Contents