IG-98-009

AUDIT REPORT

NASA DATA CENTER GENERAL CONTROLS

JET PROPULSION LABORATORY

March 24, 1998

WARNING: **This document is a final report of audit issued by the NASA Office of Inspector General (OIG). Contractor information contained herein may be company confidential. The restriction of 18 USC 1905 should be considered before this data is released to the public. Any Freedom of Information Act request for this report should be directed to the NASA Inspector General for processing in accordance with Title 14 Code of Federal Regulations, Part 1206.504.**

National Aeronautics and
Space Administration

OFFICE OF INSPECTOR GENERAL

ADDITIONAL COPIES

To obtain additional copies of this audit report, contact the acting Assistant Inspector General for Auditing at 202-358-1232.

SUGGESTIONS FOR FUTURE AUDITS

To suggest ideas for or to request future audits, contact the Assistant Inspector General for Auditing. Ideas and requests can also be mailed to:

Assistant Inspector General for Auditing
NASA Headquarters
Code W
300 E St., SW
Washington, DC 20546

NASA HOTLINE

To report fraud, waste, abuse, or mismanagement, contact the NASA OIG Hotline by calling 1-800-424-9183; 1-800-535-8134 (TDD); or by writing the NASA Inspector General, P.O. Box 23089, L'Enfant Plaza Station, Washington, DC 20026. The identity of each writer and caller can be kept confidential upon request to the extent permitted by law.

ACRONYMS

AIS	Automated Information Security
CA-7	Computer Associate's job scheduling product
CalTech	California Institute of Technology
CCURE	CCUREsystem 1 Plus Security Management System
FY	Fiscal Year
JPL	Jet Propulsion Laboratory
IBM	International Business Machines
IBS	Institutional Business Systems operation
ICIS	Institutional Computing and Information Services
ID	Identification
IPC	Institutional Processing Center
NHB	NASA Handbook
NMO	NASA Management Office
OIG	Office of Inspector General
OMB	Office of Management and Budget

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

OBSERVATIONS AND RECOMMENDATIONS 3

UPDATE THE AIS IMPLEMENTATION PLAN FOR IBS 3

PERFORM TIMELY AIS AUDITS 4

ENSURE THAT THE IPC'S PHYSICAL ACCESS SECURITY SYSTEM IS . . . . YEAR 2000 COMPLIANT 5

IMPLEMENT PASSWORD REQUIREMENTS FOR AUTOMATED JOB . . . . SCHEDULING 7

STRENGTHEN PHYSICAL SECURITY FOR IBS'S MAIN PRINTER 8

ENHANCE ACCESS CONTROL IN THE IPC COMPUTER OPERATIONS AREA . . . 9

PROVIDE VENDOR TECHNICAL SUPPORT FOR PHYSICAL ACCESS CONTROL SYSTEM 10

REENFORCE AND PERIODICALLY MONITOR VISITOR LOG-IN PROCEDURES 11

ESTABLISH FORMAL PHYSICAL ACCESS POLICIES AND PROCEDURES FOR THE IPC 12

PERIODICALLY INVENTORY TAPE ASSETS 13

STRENGTHEN HARDWARE AND SOFTWARE CHANGE MANAGEMENT PROCESS 14

APPENDIX 1 - OBJECTIVES, SCOPE, AND METHODOLOGY 17

APPENDIX 2 - AUDIT CRITERIA 19

APPENDIX 3 - MANAGEMENT'S RESPONSE 21

APPENDIX 4 - REPORT DISTRIBUTION LIST 29

NASA DATA CENTER GENERAL CONTROLS

JET PROPULSION LABORATORY, CALIFORNIA

EXECUTIVE SUMMARY

INTRODUCTION

The Jet Propulsion Laboratory (JPL) is a Federally Funded Research and Development Center (FFRDC) operated by the California Institute of Technology (CalTech) under NASA Contract NAS7-1260. The Laboratory, staffed with largely CalTech employees, is a Government-owned installation located in Pasadena, California. Its primary NASA mission is to conduct challenging robotic space missions. JPL also operates other NASA facilities in Southern California, at the Goldstone Tracking Station and Talbe Mountain. The NASA Management Office (NMO) at JPL provides NASA management oversight of JPL operations.

The NASA Office of Inspector General has completed an audit of JPL's Institutional Processing Center (IPC). The IPC houses computer systems for three different operations: (1) Institutional Business Systems (IBS), (2) Flight project systems, and (3) Supercomputing. The IPC is also the hub for JPL's high-speed network.

The primary focus of this audit was the IBS operations. Its mainframe computers operate 24 hours a day, 6.5 days a week. The five major JPL financial/administrative functions supported by the IBS are:

- Acquisition;
- finance;
- human resources;
- resource information; and
- services and property.

The operation’s primary goal is to ensure system availability, performance accuracy and adequate response time to meet its service agreements with users. The IBS Manager reports to the JPL Controller.

OBJECTIVES

The objective of this audit was to determine whether JPL has established an adequate internal control structure to provide for a reliable computing environment, including:

- physical and environmental protection; and
- operating procedures associated with general computer operations, library management, data communications, storage management, backup and recovery, and software change management.

RESULTS OF AUDIT

Overall, JPL has established an adequate internal control structure to provide for a reliable computing environment. However, we identified improvement opportunities in the areas of: (1) automated information security planning and audits, (2) physical security, (3) automated job scheduling security, (4) technical support, (5) tape management, and (6) hardware/software change management.

RECOMMENDATIONS

This report provides recommendations which we believe will help improve controls in the areas cited above. In some cases, management initiated immediate actions during audit field work to address our concerns.

OBSERVATIONS AND RECOMMENDATIONS

UPDATE THE AIS IMPLEMENTATION PLAN FOR IBS

IBS management did not fully comply with JPL's automated information security guidelines. The required plan for protective computer measures, known as the AIS Implementation Plan, has not been updated since 1992. This is primarily due to lack of management oversight for these projects. Proper and timely updating of the implementation plan provides adequate information to make informed decisions concerning risk exposures.

JPL Automated Information Security Guidelines for Data Processing Installation Security Managers, JPL D-10396 requires data processing installations to develop an implementation plan which defines the protective measures and their implementation schedule for each computer system. The plan basically addresses data security. It is to be updated when there is any change in the assigned sensitivity level or computer system configuration. The last implementation plan for IBS was dated 1992. While IBS's sensitivity level remains unchanged, many computer changes have occurred since 1992. Therefore, the IBS's implementation plan is outdated.

Physical security is addressed in the contingency planning process. During our field work, we found that the last documented contingency plan for the IBS was dated 1988. In April 1997, during our audit, IBS updated its contingency plan which addressed physical security.

RECOMMENDATION 1

The NMO should require the IBS Manager to fully comply with JPL D-10396, including updating AIS implementation plans.

Management's Response

A plan was originally generated in 1992 but has not been updated. JPL concurs that the plan should be updated because the systems have since been modified. A new plan is being generated for the Oracle Financial system implementation. The Automated Information Security (AIS) plan will be completed prior to the planned Oracle system implementation date of September 20, 1998.

Evaluation of Management's Responses

The NMO's proposed actions are responsive to the OIG recommendation.

PERFORM TIMELY AIS AUDITS

Automated Information Security audit(s) of the IBS have not been performed as required by JPL procedures. This is primarily due to an inadequate number of staff to perform AIS audits and management's failure to monitor the scheduling of the audits. Properly accomplishing the required audits would result in adequate identification of security weaknesses.

NASA Automated Information Security Handbook 2410.9A, June 1993 specifies that compliance reviews be performed by centers at least once every 3 years to ensure that compliance with AIS requirements has not degraded. This requirement was incorporated into CalTech's contract NAS7-1260 with NASA, effective September 1993. Accordingly, JPL established Automated Information Security Audit Procedures, May 1994 (JPL D-11395) to conduct AIS audits which, in substance, are compliance reviews. According to these procedures, the Network and Computer Security group is responsible for performing AIS audits of JPL's sensitive computer systems at least once every 3 years. This group is part of JPL's Institutional Computing and Information Services (ICIS), which is independent of IBS. The purpose of these audits is to obtain an independent assessment of the current AIS status of JPL's sensitive systems and to provide assurance to NASA, the JPL Director, and other applicable parties that JPL's sensitive systems comply with applicable NASA AIS requirements.

Based on the 3 year requirement, ICIS should have completed audits of all JPL critical systems by September 1996. According to its FY 97 Information Technology Security Program Plan, ICIS was scheduled to complete the audit of IBS by January 31, 1997, and the remaining six by the end of FY 1997. However, at the end of our field work, ICIS had completed only one system audit. ICIS management does not monitor the scheduling and completion of these audits.

RECOMMENDATION 2

The NMO should require that ICIS Management fulfill its AIS audit obligations and implement a process to monitor compliance with JPL-D 11395.

Management's Response

Institutional Computing and Information Services (ICIS) Management will ensure that the conducting and monitoring of system audits receives a higher priority of the Network and Computer Security (NCS) Group. The ICIS Computer Security Official and the NCS Supervisor will meet periodically to ensure that appropriate agreed-upon priorities are established and followed. JPL anticipates that seven AIS audits will be completed by the end of Fiscal Year 1998.

Evaluation of Management's Responses

The NMO's proposed actions are responsive to the OIG recommendation.

ENSURE THAT THE IPC'S PHYSICAL ACCESS SECURITY SYSTEM IS YEAR 2000 COMPLIANT

The IPC's physical access control system is not year 2000 date code compliant. This system was not compliant when procured more than 10 years ago. As a result, the software could malfunction on January 1, 2000, leading to a disruption in the IPC's daily operations.

The year 2000 date code problem originated many years ago when software developers tried to conserve the use of costly computer storage space by allocating only two positions in storage to the year field. This practice has continued until recently. As an example, the year 1997 is stored as "97". In many time sensitive systems, January 1, 2000 will probably be interpreted as January 1, 1900 or other inaccurate dates.

The IPC utilizes an automated security system known as CCURE to control physical access to the entire facility. By design, this system is time sensitive. CCURE is used to identify and validate the card key holder, allow entry only at designated locations and record entries in an automated log. Systematically, the IPC's doors are locked at all times. According to the IBS Manager, the CCURE vendor has indicated that the system is not year 2000 date code compliant. If CCURE malfunctions, each of the IPC's 50 plus doors would be locked. Access to the IPC would have to be manually controlled by security guards at each door. The alternative would be to use only a few doors, with a few security guards, for the entire IPC. Since over 800 people access the IPC, the security bottle neck would disrupt the IPC's daily operation.

RECOMMENDATION 3

The NMO should require the Information System Services Section Manager, whose responsibility includes IPC facility management, to ensure that the IPC's physical access security system is year 2000 date compliant so that physical security at the IPC will not be compromised on the first day of the new century.

Management's Response

We are in the process of acquiring a new security system and JPL Security and Protective Services has included Buildings 600 and 601 and the Institutional Computing and Information Services (ICIS) requirements into the integrated security package for the Monitor Dynamics Inc. (MDI) system.

This system will be the heart of JPL’s electronic physical security monitoring system that is currently being fully integrated. The system is Year 2000 Code Compliant and will replace the CCURE Badge reader system currently being used in Buildings 600 and 601.

The first phase of the upgraded MDI system is currently undergoing final acceptance testing. JPL will roll out the badging and access controls in April 1998.

Evaluation of Management's Responses

The NMO's proposed actions are responsive to the OIG recommendation.

IMPLEMENT PASSWORD REQUIREMENT FOR AUTOMATED JOB SCHEDULING

Access to the automated job scheduling system (job scheduler) is not controlled with password requirements. This situation exists because terminals with access to the job scheduler system were moved from a physically secured location to an unsecured location, and management overlooked the need to logically secure access to the system. Lack of adequate security could result in unauthorized access to the job scheduler. This could have a negative impact on daily operations because automated business/administrative jobs may not be processed as scheduled by users.

The IBS currently operates in an IBM mainframe environment, which uses job scheduler software called CA-7 to support its processing environment. CA-7 provides operational controls which ensure that the computer will perform required job processing tasks properly and as scheduled. In order to control access to the system, CA-7's internal security features can be used or an interface to an external security package can be implemented. CA-7's internal security, which the IBS is utilizing, has an inherent security weakness in that a user only has to submit a user ID to obtain access. A password associated with the ID is not required. At the IBS, the user ID(s) are JPL badge ID numbers which are printed on every JPL picture badge. This increases the risk that someone could obtain unauthorized access to job scheduling functions. Potentially, jobs that are submitted to be processed based on the completion of other jobs might not be processed, some jobs might not be successfully executed, or scheduled jobs might not be processed at all. The option of interfacing CA-7 with the external security software would allow for a password requirement to be enforced.

RECOMMENDATION 4

The NMO should require the IBS Manager to evaluate the current CA-7 security environment and take appropriate action to implement a password requirement. While we recognize that the CA-7 software might be eliminated when the IBS migrates to a new client-server environment, consideration needs to be given to this security exposure in the interim.

Management's Response

The ACF/2 password requirement for CA-7 was implemented on July 16, 1997.

Evaluation of Management's Responses

The NMO's actions are responsive to the OIG recommendation.

STRENGTHEN PHYSICAL SECURITY FOR IBS's MAIN PRINTER

The data center's main output device is not physically secured. As a result, printed sensitive information is exposed to unnecessary disclosure.

A large IBM 3900 printer is used for JPL's administrative and financial reporting. The monthly output from this printer is approximately 1.5 million pages and includes:

- payroll information;
- payroll checks;
- financial journals;
- project status reports;
- NASA Cost & Expenditure Reports;
- budget information; and
- other pertinent financial reports.

Currently, the printer is located in the JPL mail room which is an open area without physical security. During a review of the payroll check printing process in March 1996, CalTech Internal Audit also noted that the printer location was not secure. JPL Payroll management responded to CalTech Internal Audit's observation by taking action to safeguard the paycheck printing process. The safeguard procedure requires the presence of a payroll representative at the printer area during the printing of payroll checks. However, the rest of the printing process remains unsecured with other financial information subject to unnecessary disclosure.

RECOMMENDATION 5

The NMO should require that the IBS Manager strengthen physical security at the printing area to prevent unauthorized access to printed information.

Management's Response

The mail room activity and the printer are currently located on the first floor of Building 171. No report data was or is available for casual viewing during printing or delivery. Therefore, no additional security controls are deemed required. However, to further enhance security, the printer is being moved to a room currently under construction in the basement of Building 171 which will provide for more secure printer operations. The printer was moved to the new location on February 27, 1998.

Evaluation of Management's Responses

The NMO's actions are responsive to the OIG recommendation.

ENHANCE ACCESS CONTROL IN THE IPC COMPUTER OPERATIONS AREA

Numerous optional security capabilities available in the physical access control system are not activated to enhance access control over the IPC computer operations area. IBS management determined at the time the system was implemented that these features were not warranted. However, utilizing some of these capabilities could decrease the risk of unauthorized access to the operations area.

The CCURE system is used to control physical access to the IPC as well as its computer operations areas. It has many optional security enhancement capabilities including:

- detecting and warning of a "tailgating" situation, whereby unauthorized access is gained by following an authorized cardholder into the facility;
- ensuring that guests are escorted through a facility and are not left unattended; and
- keeping track of the number of escorts and visitors in each area.

The IPC's computer operations area is an open region which is informally divided into different functional sections. Although access is restricted, it is not difficult, for example, for an individual to tailgate another into the facility. Once inside the operations area, tailgating could also occur in restricted sections within computer operations. Since the implementation of the system 10 years ago, management has not re-evaluated the cost and benefit of implementing some of CCURE's security enhancement capabilities in the current environment.

RECOMMENDATION 6

The NMO should require the IBS Manager to re-evaluate the need to implement some or all of CCURE's available capabilities to enhance security in the computer operations area.

Management's Response

The personnel who access the IPC operations area are very cognizant of their responsibilities and security awareness in this area is very good. JPL has reevaluated the need to implement some or all of CCURE’s security enhancement capabilities and believes that risk is low. Therefore in JPL’s opinion, any further security enhancements would be neither practical nor cost effective.

Evaluation of Management's Responses

The NMO's actions are responsive to the OIG recommendation.

PROVIDE VENDOR TECHNICAL SUPPORT FOR PHYSICAL ACCESS CONTROL SYSTEM

The physical access control system, CCURE, is at least 10 years old and operating without technical support and software maintenance support. This situation exists because management did not acquire CCURE vendor technical support and software maintenance services due to lack of funding. Lack of software maintenance support increases the risk of system failure and vulnerability to system crashes. Proper levels of technical support allow the computer and security staffs to use the system to its fullest capacity.

For example, without technical support, current staff is unable to electronically download database information in order to compare the existing valid personnel access records to current personnel records. This comparison would allow staff to identify inactive employees who still have access to the facility as well as employee changes in status, section, or group. Because manual comparison is extremely time consuming, it is being done infrequently. With JPL's on going reorganization and re-engineering activities, it is critical that this comparison be performed frequently.

RECOMMENDATION 7

The NMO should require the IBS Manager to obtain adequate support for CCURE. We recognize that CCURE might be replaced by the year 2000. Regardless of the system used, proper technical support and maintenance should be in place.

Management's Response

The existing unsupported system will be replaced as part of the implementation of the MDI system in April 1998 (see JPL response to recommendation 3). The MDI system will be fully supported by the vendor.

Evaluation of Management's Responses

The NMO's proposed actions are responsive to the OIG recommendation.

REENFORCE AND PERIODICALLY MONITOR VISITOR LOG-IN PROCEDURES

Visitor logs maintained by the IPC guard station are incomplete. These logs are incomplete because employees and security guards at the IPC are not enforcing their completion, as required by JPL procedures. Properly completing visitor logs enhances physical security controls over the IPC and provides a sufficient audit trail of visitor accesses.

The IPC maintains a visitor sign-in log at the security guard station, as required by JPL Security Practice 4-09-7 for Visitor Control. These sign-in logs identify such information as visitors' names, signatures, citizenship, who they represent, their JPL contacts, and in and out times. In a majority of the logs that we reviewed, visitors, JPL hosts, and guards had not always entirely completed the visitor logs.

RECOMMENDATION 8

The NMO should require the Manager of JPL Security and Protective Services to re-enforce and periodically monitor the visitor policy and procedures with respect to visitor logs.

Management's Response

Effective January 14, 1998, the Officer on duty at IPC will insure that each line required of the Visitor Sign-In Log is filled out completely and accurately. The shift Commander and Watch Sergeant will review the logs at the end of each shift, daily to verify compliance. The Administrative Captain will pick random samples of the logs and forward them to Guard Headquarters every two weeks for periodic monitoring by the Manager of Security and Protective Services and the Supervisor of Plant Protection. All officers assigned to IPC will be briefed that these logs must be properly maintained and completed. In addition, once each shift the supervisor will review these logs to insure that they are being properly completed.

Evaluation of Management's Responses

The NMO's proposed actions are responsive to the OIG recommendation.

ESTABLISH FORMAL PHYSICAL ACCESS POLICIES AND PROCEDURES FOR THE IPC

Management-approved policies and procedures for access to the IPC's computer operations area have not been developed. Without approved policies and procedures to restrict access to a need-to-know basis, physical security to the computer operations area may be vulnerable to unnecessary access because employees may not understand how access decisions are to be applied.

During the audit, the OIG was provided with three documents relating to IPC facility access. These documents, which have not been reviewed nor approved by JPL management, are not formal JPL policies and procedures. They imply that access to the computer operations area is granted on a need-to-know basis. However, "need-to-know" was not clearly defined. In addition, the documents did not address how personnel with limited access or visitors are to be supervised when they are in the computer operations area.

RECOMMENDATION 9

The NMO should require that IPC management establish formal physical access security policies and procedures for the IPC's computer operations area.

Management's Response

JPL Security and Protection is no longer responsible for the total security package in buildings 600 and 601, but is responsible for the area that houses the IPC function. The JPL policy "Identification for Laboratory Access" is applicable to the IPC area in buildings 600 and 601 and a copy of that policy has been provided to the NASA OIG.

In accordance with JPL policy, JPL Security restricts access into the IPC area to personnel who are on the assigned IPC personnel listing. In addition, there is a guard assigned to Building 600 at a stationary post to manage basic access.

Evaluation of Management's Responses

The NMO's actions are responsive to the OIG recommendation.

PERIODICALLY INVENTORY TAPE ASSETS

IBS does not have formal procedures to periodically inventory tape assets. Failure to conduct periodic inventories of tape assets increases the risk that any mishandling of tapes will go undetected.

Cartridge tape is a primary storage media used at the IPC. Tape silos automatically store tape cartridges that are frequently used. Less frequently used tapes are stored in open shelves managed by a tape librarian. The librarian sends tape backups to an offsite facility on a scheduled basis.

While the IPC tape library is physically secured within the computer operations area, its location is in an open area which allows access by anyone who has access to the computer operations area. This increases the risk that tapes can be accidentally or deliberately misplaced or removed from the tape library.

RECOMMENDATION 10

The NMO should require the IBS Manager to institute procedures for the periodic physical inventory of tape cartridges in the library and at the offsite backup facility. The inventory count should be performed by an individual who is independent of the tape management function.

Management's Response

On February 5, 1998, the Manager of Operations and Technical Support instructed OAO to perform spot audits of IBS tape assets on a quarterly basis. JPL believes this is a low risk item because there are numerous cameras and other physical security measures in place. Past records also support that there are few lost or misplaced tapes. The results of spot audits of the different libraries will be utilized to determine if periodic inventories by independent personnel are required.

Evaluation of Management's Responses

The NMO's proposed actions are responsive to the OIG recommendation.

STRENGTHEN HARDWARE AND SOFTWARE CHANGE MANAGEMENT PROCESS

The IPC disaster recovery coordinator is not an evaluator in the hardware and software change management process. Inadequate involvement of disaster recovery personnel could negatively impact disaster recovery testing and capability because disaster recovery plans may not be kept current.

IPC change control procedures exist for the submittal and processing of change requests. The procedures establish responsibilities for requesting, recording, and implementing changes to hardware, system software and application software. As part of this process, various personnel are responsible for evaluating the impact of changes and ensuring that formal documentation exists.

An IPC staff member is assigned the responsibility of coordinating and maintaining the IPC Disaster Recovery Plan. However, this individual is not a participant in the review of changes. As a result, disaster recovery plans may not be kept current, which could negatively impact disaster recovery testing and capability.

RECOMMENDATION 11

The NMO should require the Manager of Configuration Management, who has responsibility for change control, to include the disaster recovery coordinator in the change management process.

Management's Response

Since September 22, 1997, when IBS was reorganized, disaster recovery coordination, hardware and software change management, and security engineering have been incorporated into the IBS Technical Services section, ensuring close communication.

Evaluation of Management's Responses

The NMO's actions are responsive to the OIG recommendation.

OBJECTIVES, SCOPE, AND METHODOLOGY . . . . Appendix 1

OBJECTIVES

The objective of the audit was to determine whether an adequate internal control structure had been established to provide for a reliable computing environment, including:

- physical and environmental protection; and
- operating procedures that provide for the reliable management of computer operations.

SCOPE AND METHODOLOGY

The scope of the audit included a review of operating procedures associated with the IBS, as well as physical and environmental controls applicable to the entire IPC. As part of the audit, we reviewed the IPC facility, IBS operating procedures, and interviewed several key JPL and subcontractor employees.

MANAGEMENT CONTROLS REVIEWED

We evaluated general management controls over activities that are the responsibility of the IPC and IBS, including:

- physical and environmental protection;
- general computer operations;
- library management;
- data communications;
- storage management;
- backup and recovery; and
- software change management.

AUDIT FIELD WORK

Audit field work was conducted from January through July 1997 at JPL. We conducted the audit in accordance with generally accepted government auditing standards.

NASA MANAGEMENT INSTRUCTION FOR ASSURING THE SECURITY AND INTEGRITY OF NASA AUTOMATED INFORMATION RESOURCES (NMI 2410.7C) states that NASA'S automated information resources shall be provided a level of security and integrity consistent with the potential harm from their loss, inaccuracy, alteration, unavailability, or misuse.

This NMI applies to audit recommendations 5,6,7, and 10.

NASA AUTOMATED INFORMATION SECURITY HANDBOOK, NHB 2410.9A, JUNE 1993: **Section 208(b)** of this handbook requires centers to conduct periodic self-assessments and compliance reviews at Data Processing Installation's under their management cognizance at a minimum of 1 to 3 years. **NASA/JPL contract NAS7-1260, section H-55**, specifies that JPL utilize NHB 2410.9A to establish its security practices.

This Handbook applies to audit recommendation 1.

Section 303 of this handbook requires that each Center conduct risk assessments of information processing resources, including physical security and access controls. However, JPL's contract with NASA**, NAS7-1260, section H-55(b)**, allows deviation from handbook's chapter 3 which covers section 303. This deviation was documented in JPL's acceptance letter which specified the conditions to which JPL would comply with section 303.

This Handbook applies to audit recommendation 2.

JPL STANDARD PRACTICE INSTRUCTION 4-02-1 for Laboratory Visits requires visitors to follow the sign-in practice procedures at the visitor reception area. The sign-in procedures are described in JPL Security Practice 4-09-7 for Visitor Control.

This Standard applies to audit recommendation 8.

GOOD BUSINESS PRACTICES:

Physical security systems are critical to the security of normal operations. Since these systems are date sensitive, they need to meet year 2000 compliance requirements.

This practice applies to audit recommendation 3.

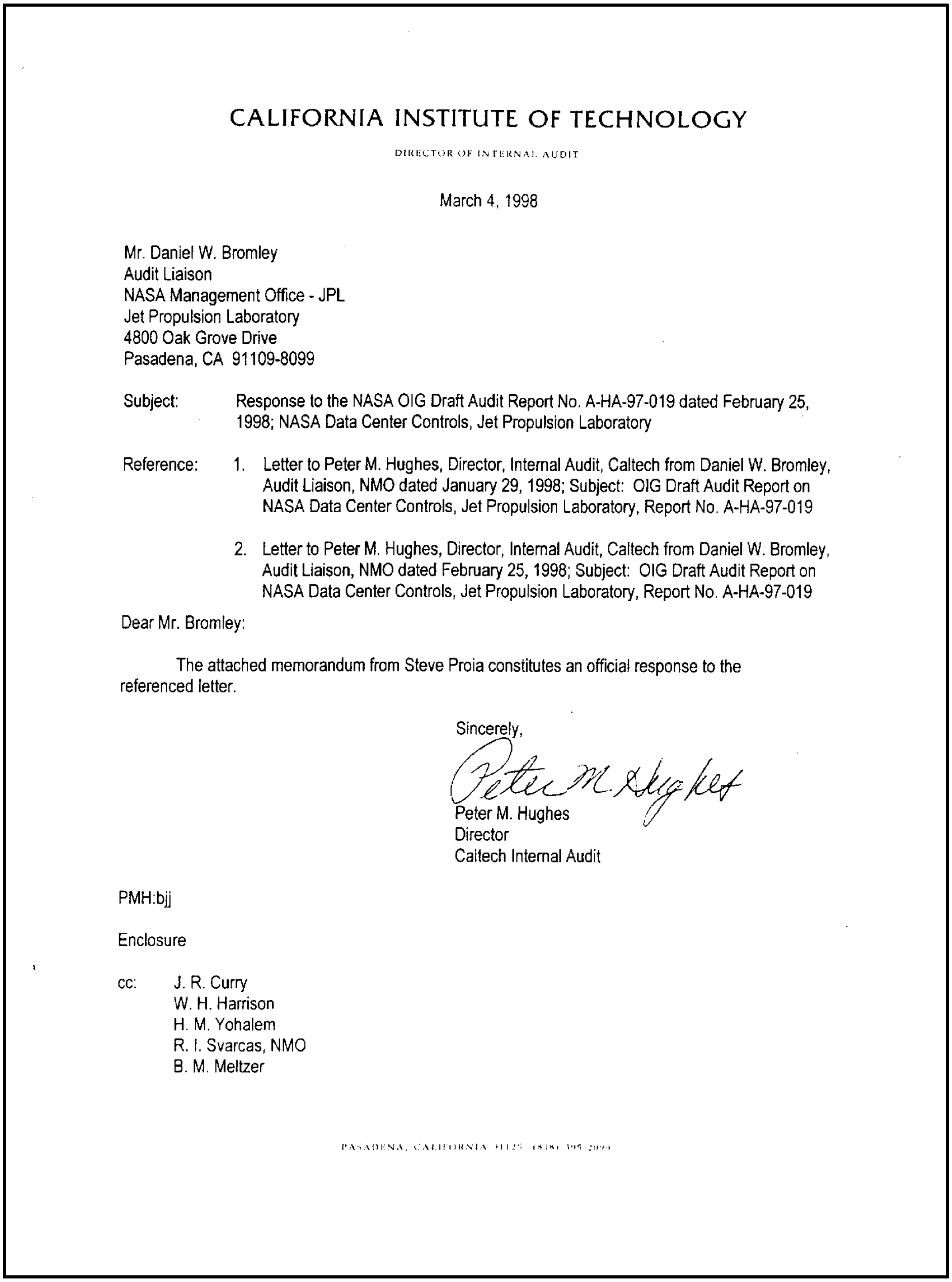
An adequately controlled data processing installation typically has a schedule of when jobs are to be processed and which data files are to be utilized. Scheduling software is often used to automatically submit jobs for processing on a predetermined basis. Because job scheduling is a critical function, logical access to scheduler software should be controlled through the use of passwords.

This practice applies to audit recommendation 4.

A good business practice in controlling physical access to a computer operation facility is to establish policies and procedures which limit access to a need-to-know basis. These policies and procedures should also address how other personnel with need of limited access or visitors

are to be granted access and supervised when in the computer operations area.
This practice applies to audit recommendation 9.

Software/hardware changes should be properly evaluated for impact, and approved by appropriate personnel. Personnel responsible for disaster contingency planning should be included in the change control process, because they have the responsibility of deciding whether a particular change has an impact on the contingency plan.
This practice applies to audit recommendation 11.



CALIFORNIA INSTITUTE OF TECHNOLOGY

DIRECTOR OF INTERNAL AUDIT

March 4, 1998

Mr. Daniel W. Bromley
Audit Liaison
NASA Management Office - JPL
Jet Propulsion Laboratory
4800 Oak Grove Drive
Pasadena, CA 91109-8099

Subject: Response to the NASA OIG Draft Audit Report No. A-HA-97-019 dated February 25, 1998; NASA Data Center Controls, Jet Propulsion Laboratory

Reference:

1. Letter to Peter M. Hughes, Director, Internal Audit, Caltech from Daniel W. Bromley, Audit Liaison, NMO dated January 29, 1998; Subject: OIG Draft Audit Report on NASA Data Center Controls, Jet Propulsion Laboratory, Report No. A-HA-97-019

2. Letter to Peter M. Hughes, Director, Internal Audit, Caltech from Daniel W. Bromley, Audit Liaison, NMO dated February 25, 1998; Subject: OIG Draft Audit Report on NASA Data Center Controls, Jet Propulsion Laboratory, Report No. A-HA-97-019

Dear Mr. Bromley:

The attached memorandum from Steve Proia constitutes an official response to the referenced letter.

Sincerely,

Peter M. Hughes

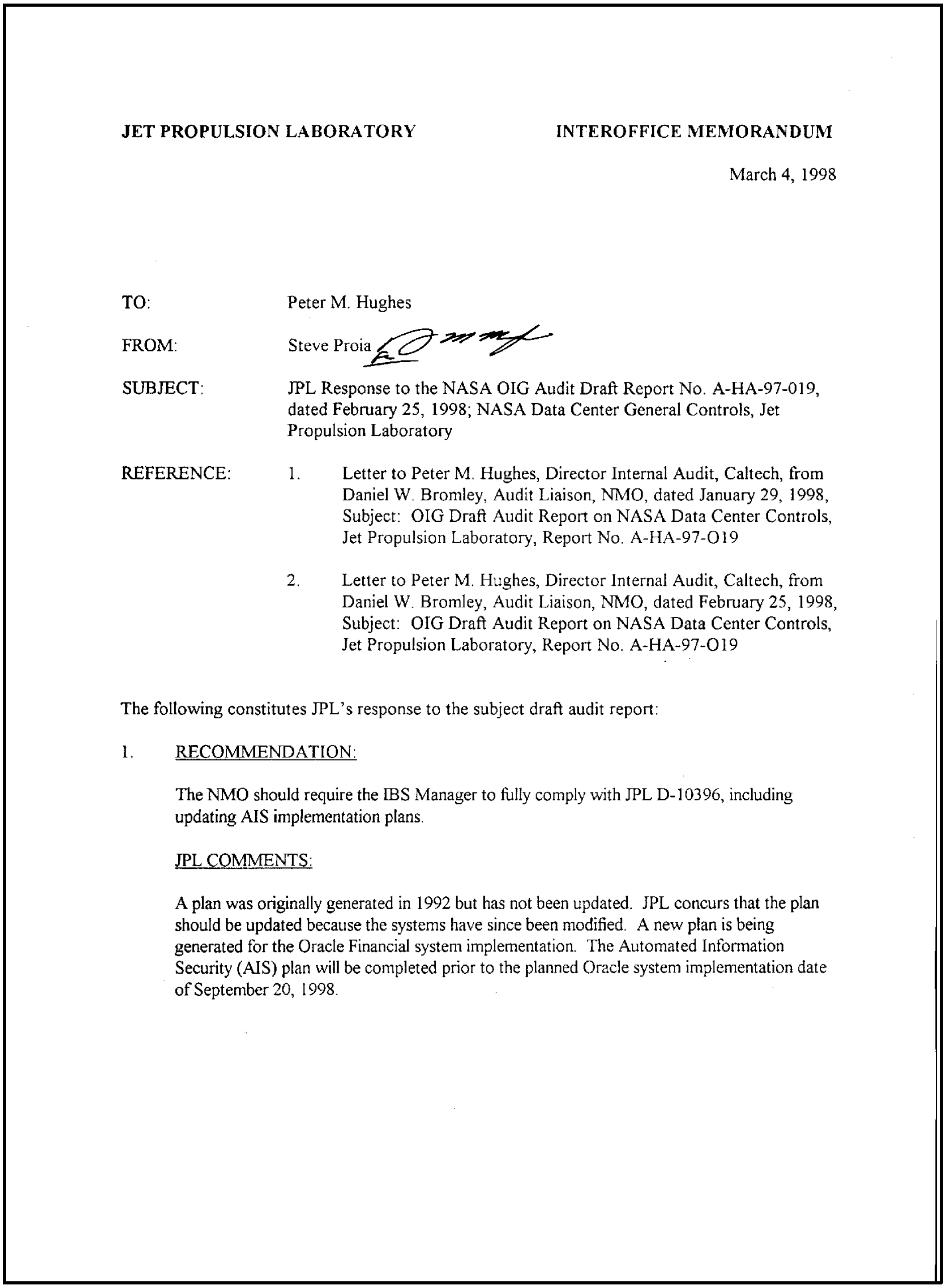
Peter M. Hughes
Director
Caltech Internal Audit

PMH:bjj

Enclosure

cc: J. R. Curry
W. H. Harrison
H. M. Yohalem
R. I. Svarcas, NMO
B. M. Meltzer

PASADENA, CALIFORNIA 91125 (818) 395-2000



JET PROPULSION LABORATORY **INTEROFFICE MEMORANDUM**

March 4, 1998

TO: Peter M. Hughes

FROM: Steve Proia

SUBJECT: JPL Response to the NASA OIG Audit Draft Report No. A-HA-97-019, dated February 25, 1998; NASA Data Center General Controls, Jet Propulsion Laboratory

REFERENCE:

1. Letter to Peter M. Hughes, Director Internal Audit, Caltech, from Daniel W. Bromley, Audit Liaison, NMO, dated January 29, 1998, Subject: OIG Draft Audit Report on NASA Data Center Controls, Jet Propulsion Laboratory, Report No. A-HA-97-O19

2. Letter to Peter M. Hughes, Director Internal Audit, Caltech, from Daniel W. Bromley, Audit Liaison, NMO, dated February 25, 1998, Subject: OIG Draft Audit Report on NASA Data Center Controls, Jet Propulsion Laboratory, Report No. A-HA-97-O19

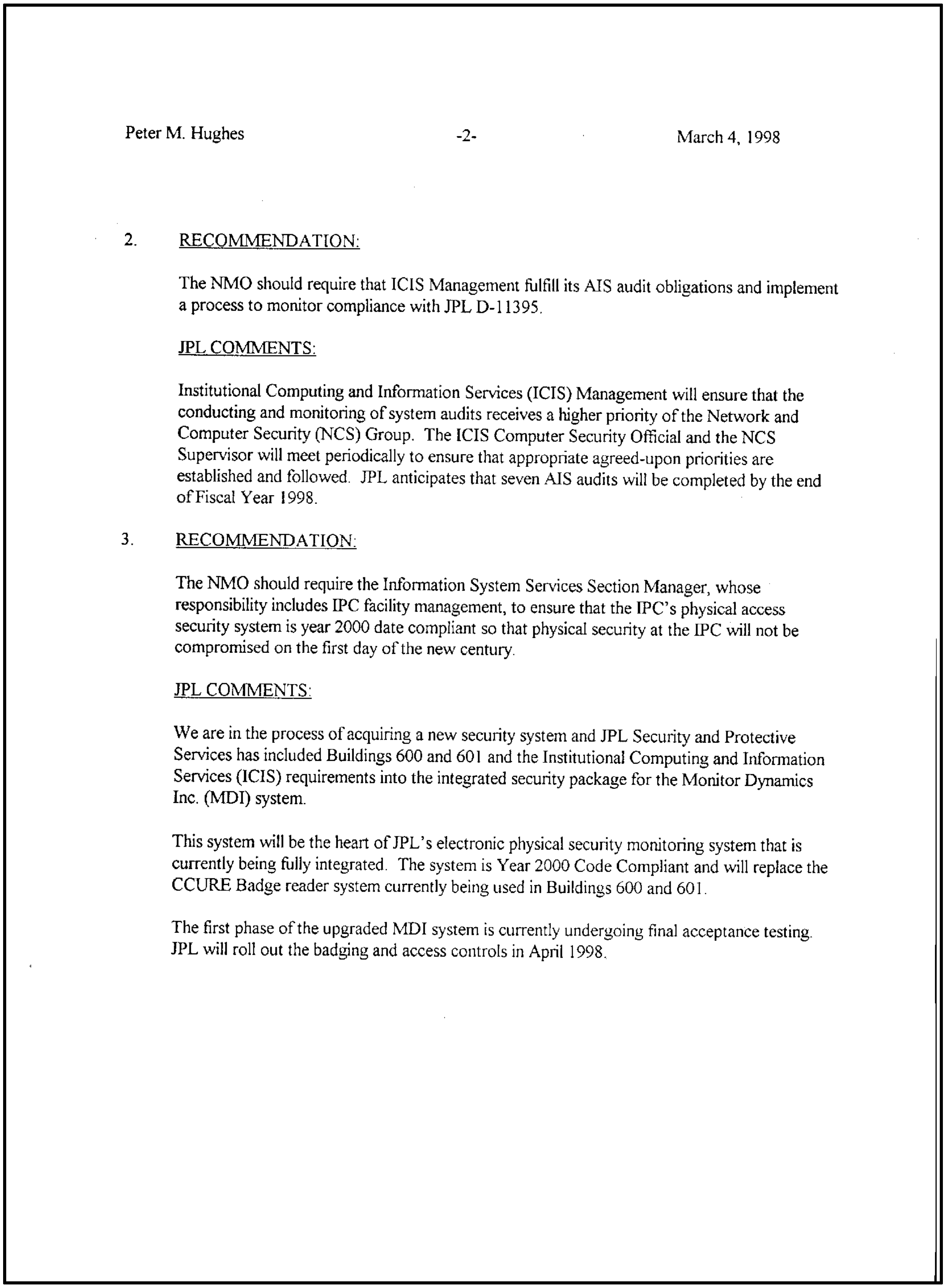
The following constitutes JPL's response to the subject draft audit report:

1. RECOMMENDATION:

The NMO should require the IBS Manager to fully comply with JPL D-10396, including updating AIS implementation plans.

JPL COMMENTS:

A plan was originally generated in 1992 but has not been updated. JPL concurs that the plan should be updated because the systems have since been modified. A new plan is being generated for the Oracle Financial system implementation. The Automated Information Security (AIS) plan will be completed prior to the planned Oracle system implementation date of September 20, 1998.



Peter M. Hughes -2- March 4, 1998

2. RECOMMENDATION:

The NMO should require that ICIS Management fulfill its AIS audit obligations and implement a process to monitor compliance with JPL D-11395.

JPL COMMENTS:

Institutional Computing and Information Services (ICIS) Management will ensure that the conducting and monitoring of system audits receives a higher priority of the Network and Computer Security (NCS) Group. The ICIS Computer Security Official and the NCS Supervisor will meet periodically to ensure that appropriate agreed-upon priorities are established and followed. JPL anticipates that seven AIS audits will be completed by the end of Fiscal Year 1998.

3. RECOMMENDATION:

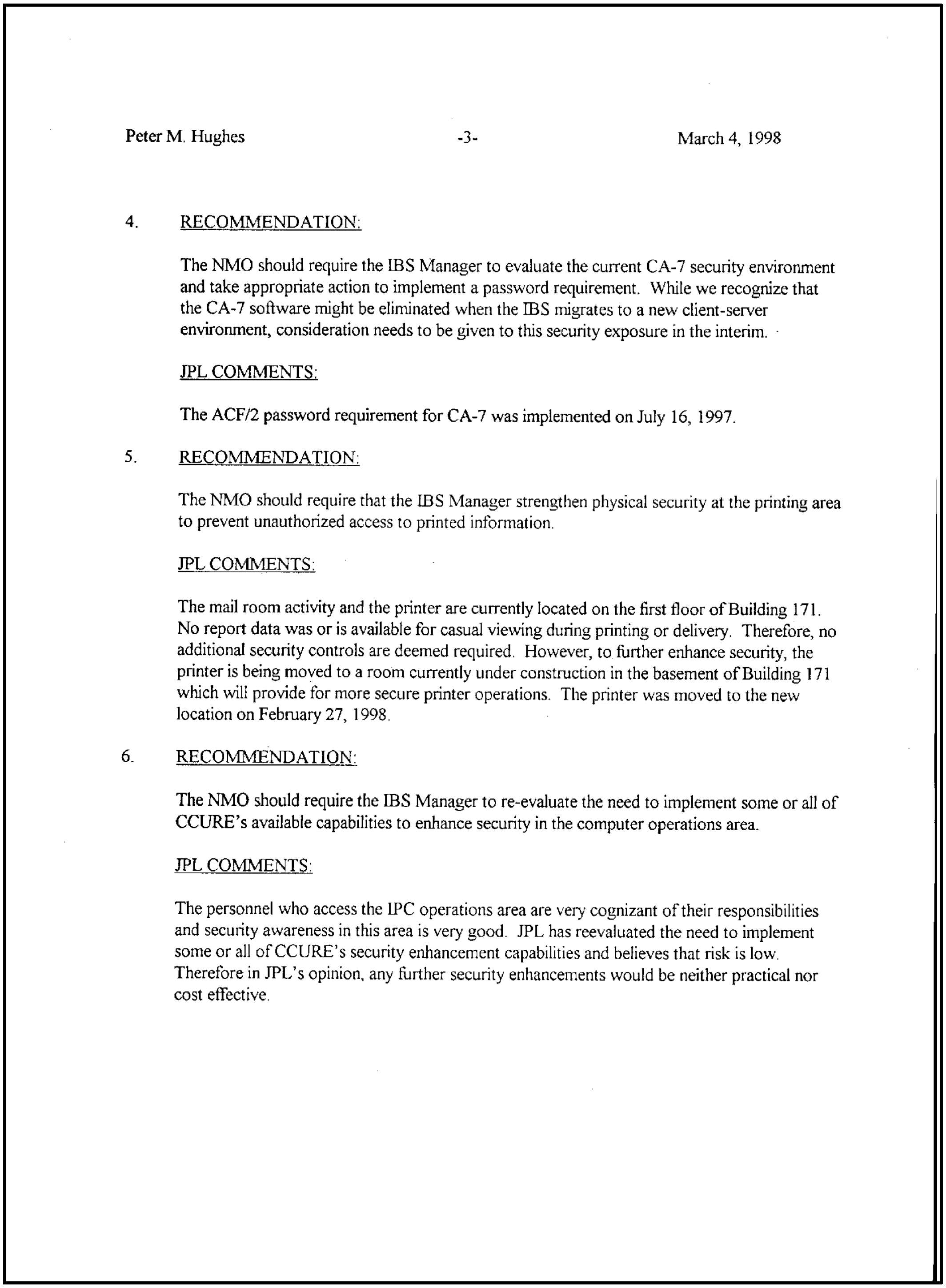
The NMO should require the Information System Services Section Manager, whose responsibility includes IPC facility management, to ensure that the IPC's physical access security system is year 2000 date compliant so that physical security at the IPC will not be compromised on the first day of the new century.

JPL COMMENTS:

We are in the process of acquiring a new security system and JPL Security and Protective Services has included Buildings 600 and 601 and the Institutional Computing and Information Services (ICIS) requirements into the integrated security package for the Monitor Dynamics Inc. (MDI) system.

This system will be the heart of JPL's electronic physical security monitoring system that is currently being fully integrated. The system is Year 2000 Code Compliant and will replace the CCURE Badge reader system currently being used in Buildings 600 and 601.

The first phase of the upgraded MDI system is currently undergoing final acceptance testing. JPL will roll out the badging and access controls in April 1998.



4. RECOMMENDATION:

The NMO should require the IBS Manager to evaluate the current CA-7 security environment and take appropriate action to implement a password requirement. While we recognize that the CA-7 software might be eliminated when the IBS migrates to a new client-server environment, consideration needs to be given to this security exposure in the interim.

JPL COMMENTS:

The ACF/2 password requirement for CA-7 was implemented on July 16, 1997.

5. RECOMMENDATION:

The NMO should require that the IBS Manager strengthen physical security at the printing area to prevent unauthorized access to printed information.

JPL COMMENTS:

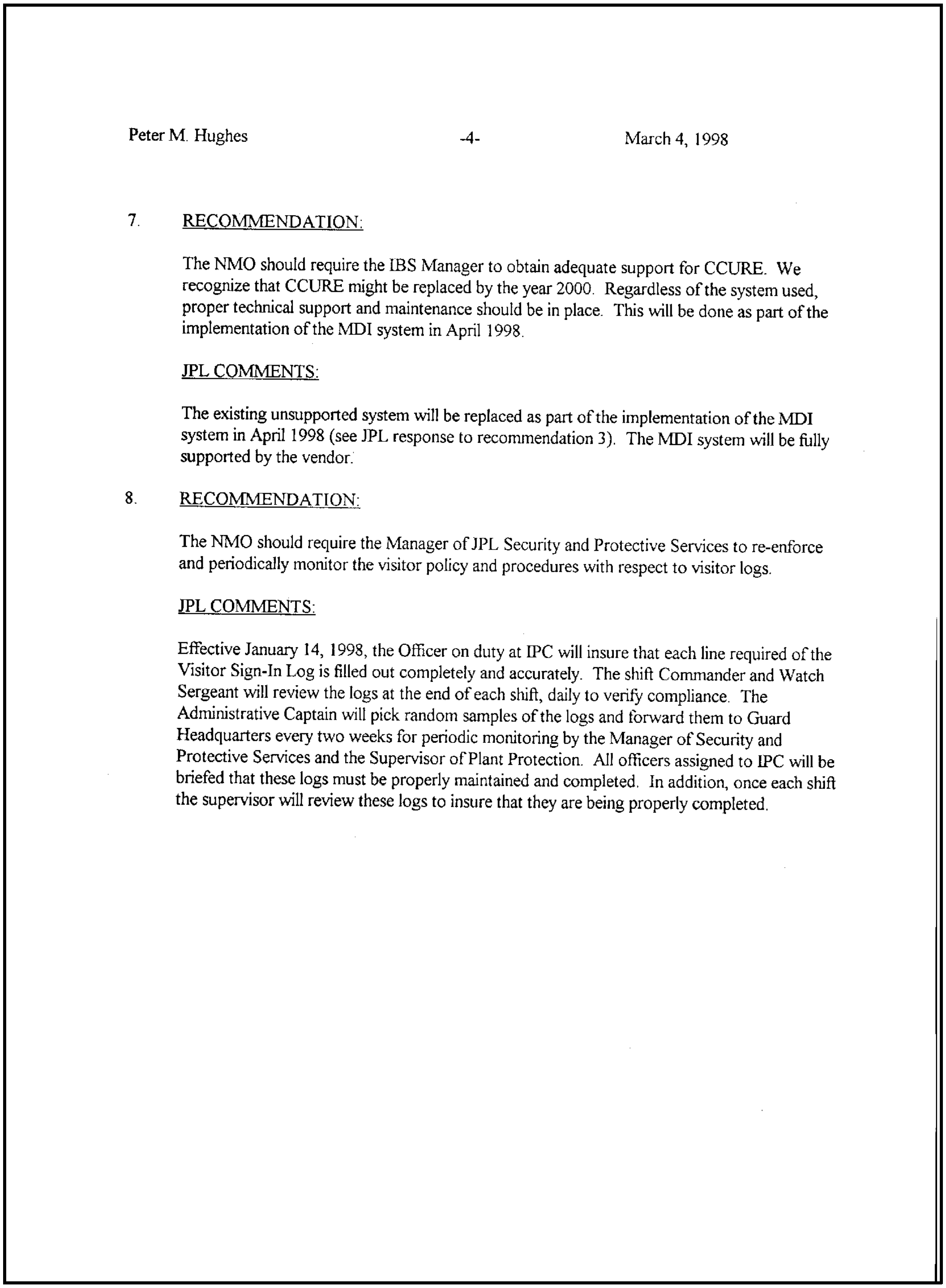
The mail room activity and the printer are currently located on the first floor of Building 171. No report data was or is available for casual viewing during printing or delivery. Therefore, no additional security controls are deemed required. However, to further enhance security, the printer is being moved to a room currently under construction in the basement of Building 171 which will provide for more secure printer operations. The printer was moved to the new location on February 27, 1998.

6. RECOMMENDATION:

The NMO should require the IBS Manager to re-evaluate the need to implement some or all of CCURE's available capabilities to enhance security in the computer operations area.

JPL COMMENTS:

The personnel who access the IPC operations area are very cognizant of their responsibilities and security awareness in this area is very good. JPL has reevaluated the need to implement some or all of CCURE's security enhancement capabilities and believes that risk is low. Therefore in JPL's opinion, any further security enhancements would be neither practical nor cost effective.



Peter M. Hughes -4- March 4, 1998

7. RECOMMENDATION:

The NMO should require the IBS Manager to obtain adequate support for CCURE. We recognize that CCURE might be replaced by the year 2000. Regardless of the system used, proper technical support and maintenance should be in place. This will be done as part of the implementation of the MDI system in April 1998.

JPL COMMENTS:

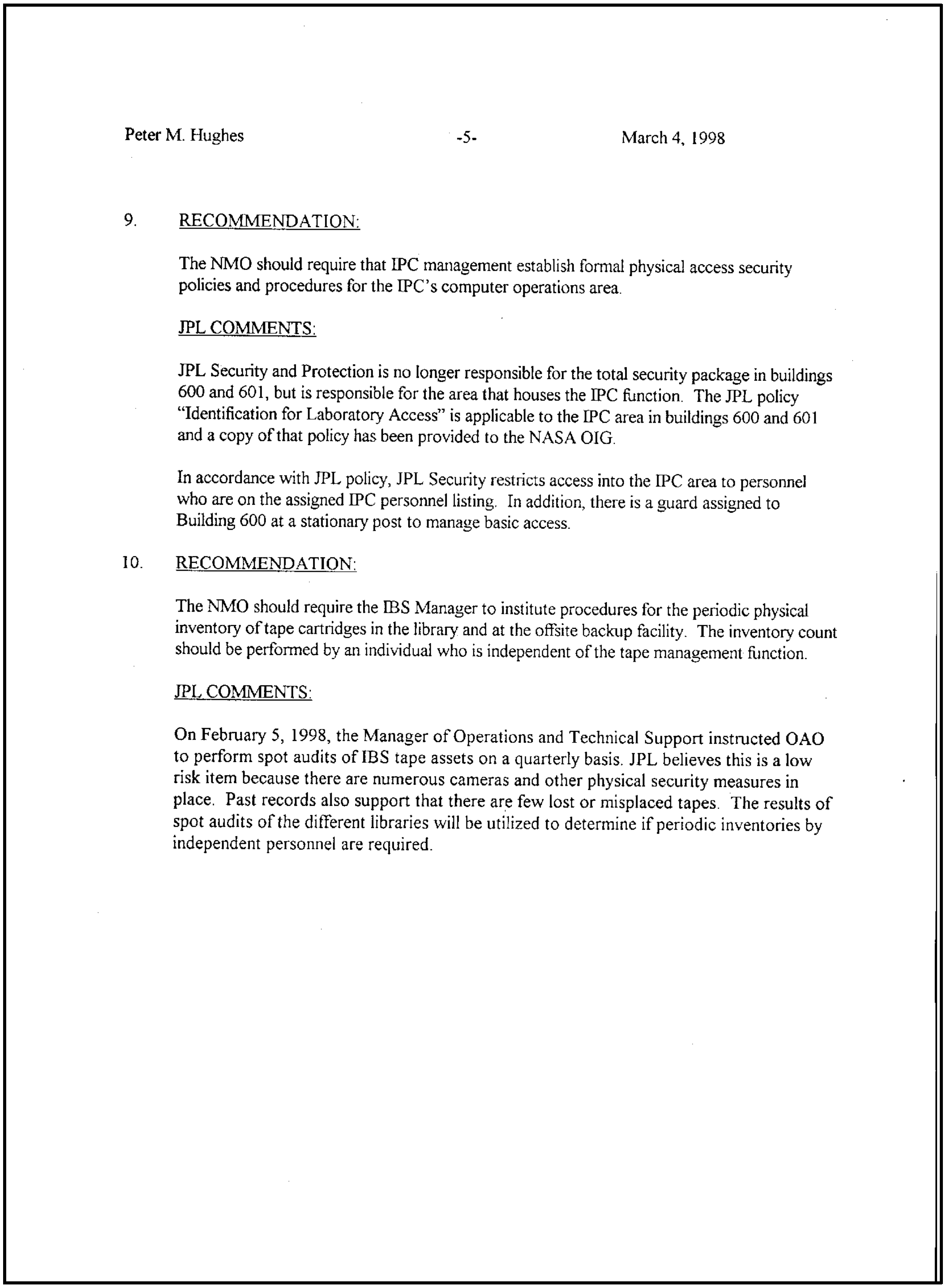
The existing unsupported system will be replaced as part of the implementation of the MDI system in April 1998 (see JPL response to recommendation 3). The MDI system will be fully supported by the vendor.

8. RECOMMENDATION:

The NMO should require the Manager of JPL Security and Protective Services to re-enforce and periodically monitor the visitor policy and procedures with respect to visitor logs.

JPL COMMENTS:

Effective January 14, 1998, the Officer on duty at IPC will insure that each line required of the Visitor Sign-In Log is filled out completely and accurately. The shift Commander and Watch Sergeant will review the logs at the end of each shift, daily to verify compliance. The Administrative Captain will pick random samples of the logs and forward them to Guard Headquarters every two weeks for periodic monitoring by the Manager of Security and Protective Services and the Supervisor of Plant Protection. All officers assigned to IPC will be briefed that these logs must be properly maintained and completed. In addition, once each shift the supervisor will review these logs to insure that they are being properly completed.



9. RECOMMENDATION:

The NMO should require that IPC management establish formal physical access security policies and procedures for the IPC's computer operations area.

JPL COMMENTS:

JPL Security and Protection is no longer responsible for the total security package in buildings 600 and 601, but is responsible for the area that houses the IPC function. The JPL policy "Identification for Laboratory Access" is applicable to the IPC area in buildings 600 and 601 and a copy of that policy has been provided to the NASA OIG.

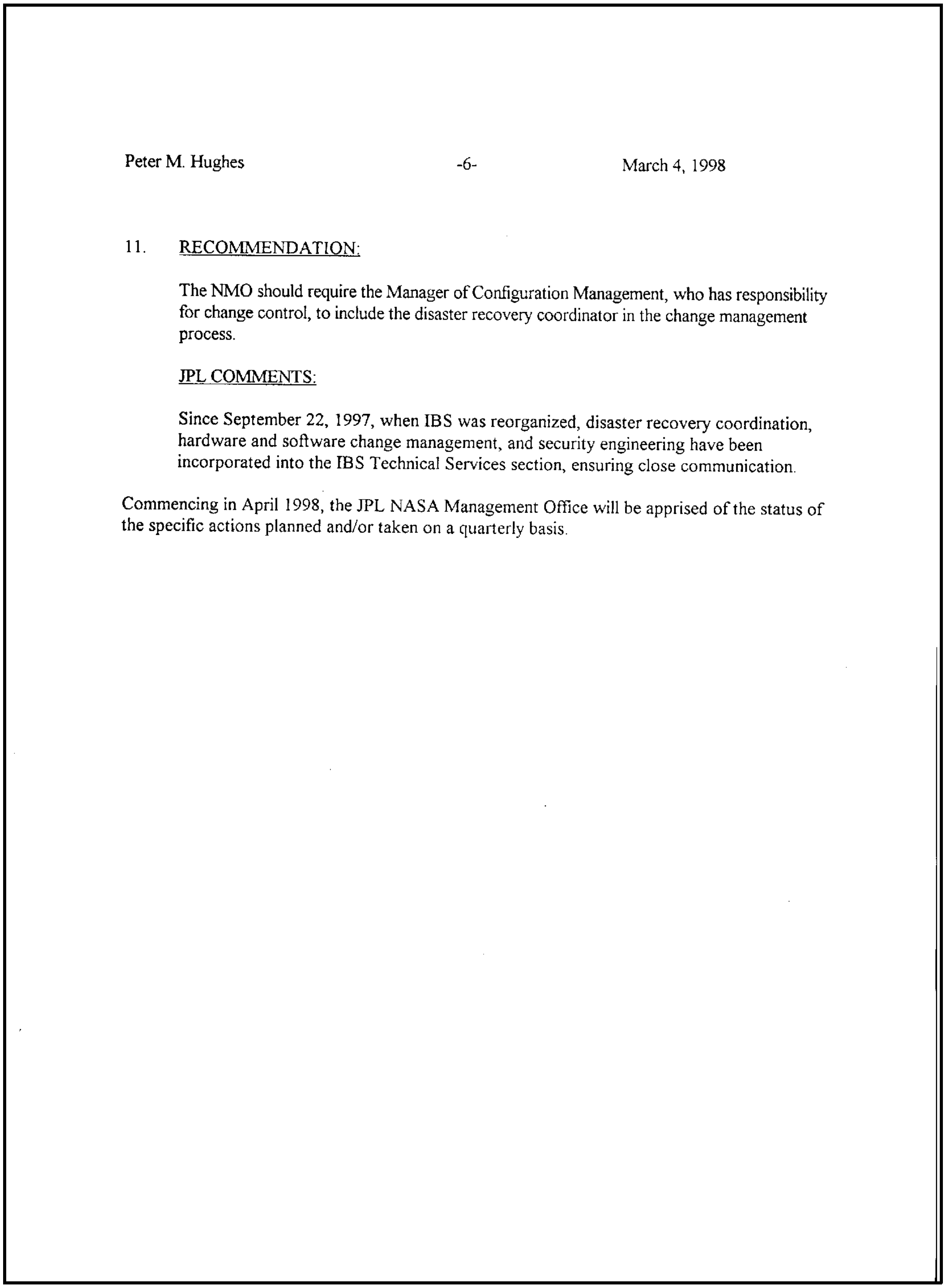
In accordance with JPL policy, JPL Security restricts access into the IPC area to personnel who are on the assigned IPC personnel listing. In addition, there is a guard assigned to Building 600 at a stationary post to manage basic access.

10. RECOMMENDATION:

The NMO should require the IBS Manager to institute procedures for the periodic physical inventory of tape cartridges in the library and at the offsite backup facility. The inventory count should be performed by an individual who is independent of the tape management function.

JPL COMMENTS:

On February 5, 1998, the Manager of Operations and Technical Support instructed OAO to perform spot audits of IBS tape assets on a quarterly basis. JPL believes this is a low risk item because there are numerous cameras and other physical security measures in place. Past records also support that there are few lost or misplaced tapes. The results of spot audits of the different libraries will be utilized to determine if periodic inventories by independent personnel are required.



Peter M. Hughes -6- March 4, 1998

11. RECOMMENDATION:

The NMO should require the Manager of Configuration Management, who has responsibility for change control, to include the disaster recovery coordinator in the change management process.

JPL COMMENTS:

Since September 22, 1997, when IBS was reorganized, disaster recovery coordination, hardware and software change management, and security engineering have been incorporated into the IBS Technical Services section, ensuring close communication.

Commencing in April 1998, the JPL NASA Management Office will be apprised of the status of the specific actions planned and/or taken on a quarterly basis.

REPORT DISTRIBUTION LIST . . . . Appendix 4

National Aeronautics and Space Administration (NASA) Headquarters
Code AO/Chief Information Officer
Code B/Chief Financial Officer (CFO/Comptroller)
Code G/General Counsel
Code J/Associate Administrator for Management Systems and Facilities
Code JM/Management Assessment Division (10 copies)
Code L/Associate Administrator for Legislative Affairs
Code S/Associate Administrator

NASA Field Installations
Director, Ames Research Center
Director, Dryden Flight Research Center
Director, Goddard Space Flight Center
Director, Jet Propulsion Laboratory
Director, Lyndon B. Johnson Space Center
Director, John F. Kennedy Space Center
Director, Langley Research Center
Director, Lewis Research Center
Director, George C. Marshall Space Flight Center
Director, John C. Stennis Space Center
Head, Goddard Institute for Space Studies
Manager, KSC VLS Resident Office (Vandenberg AFB)
Manager, Michoud Assembly Facility
Manager, NASA Management Office - JPL
Manager, JSC White Sands Test Facility

NASA Offices of Inspector General
Ames Research Center
Goddard Space Flight Center
Jet Propulsion Laboratory
Lyndon B. Johnson Space Center
John F. Kennedy Space Center
Langley Research Center
Lewis Research Center
George C. Marshall Space Flight Center
John C. Stennis Space Center

Chairman and Ranking Minority Member - Congressional Committees and Subcommittees:
Senate Committee on Appropriations
Senate Subcommittee on VA-HUD-Independent Agencies

REPORT DISTRIBUTION LIST Appendix 4

Senate Committee on Commerce, Science and Transportation
Senate Subcommittee on Science, Technology and Space
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on VA-HUD-Independent Agencies
House Committee on Government Reform and Oversight
House Committee on Science
House Subcommittee on Space and Aeronautics

Non-NASA Federal Organizations and Individuals
Assistant to the President for Science and Technology Policy
Deputy Associate Director, Energy and Science Division, Office of Management and Budget
Budget Examiner, Energy Science Division, Office of Management and Budget
Associate Director, National Security and International Affairs Division, General Accounting Office
Special Counsel, Subcommittee on National Security, International Affairs, and Criminal Justice
Professional Assistant, Senate Subcommittee on Science, Technology, and Space

MAJOR CONTRIBUTORS TO THIS AUDIT

Brent Melson - Program Director, Information Assurance
Phuong Quach - Information Assurance Auditor, Jet Propulsion Laboratory