

IG-97-035

**AUDIT
REPORT**

**NASA DATA CENTER FACILITY
LANGLEY RESEARCH CENTER**

August 28, 1997



National Aeronautics and
Space Administration

OFFICE OF INSPECTOR GENERAL

ADDITIONAL COPIES

To obtain additional copies of this audit report, contact the 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 Street, 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.

AIS	AUTOMATED INFORMATION SECURITY
COTR	CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE
CSO	COMPUTER SECURITY OFFICER
CSCC	CENTRAL SCIENTIFIC COMPUTING COMPLEX
DMSS	DISTRIBUTED MASS STORAGE SYSTEM
DPI	DATA PROCESSING INSTALLATION
EOS DAAC	EARTH OBSERVING SYSTEM DISTRIBUTED ACTIVE ARCHIVE CENTER
FSCS	FLIGHT SIMULATION COMPUTING SYSTEM
ISSD	INFORMATION SYSTEMS AND SERVICES DIVISION
ITS	INFORMATION TECHNOLOGY SECURITY
LARC	LANGLEY RESEARCH CENTER
SNS	SUPERCOMPUTING NETWORK SUBSYSTEM
UPS	UNINTERRUPTIBLE POWER SUPPLY

National Aeronautics and
Space Administration

Headquarters
Washington, DC 20546-0001



Reply to Attn of: W

August 28, 1997

TO: Langley Research Center
Attn: 106/Center Director

FROM: W/Acting Assistant Inspector General for Auditing

SUBJECT: Final Report
NASA Data Center Facility - LaRC
Assignment Number A-HA-97-022
Report Number IG-97-035

We have completed an audit of the Central Scientific Computing Complex at Langley Research Center. The purpose of the audit was to determine whether NASA's data centers are operated with adequate organizational and management controls, including physical security. In general, the controls for the Supercomputing Network Subsystem and the Distributed Mass Storage System were adequate. However, we identified several areas requiring management's attention, including (1) computer system access and physical security controls, (2) Automated Information Security Program implementation, (3) operational controls, and (4) testing of uninterruptible power supplies.

A draft report was issued on July 17, 1997. Management responded on August 14, 1997. The response is included after each recommendation and is presented in its entirety as Appendix 2. The response indicates that management has implemented corrective actions that are responsive to the intent of the recommendations. All the recommendations are considered closed with the issuance of this report.

We appreciate the cooperation and assistance provided to us throughout the audit by the Information Systems and Services Division personnel. If you have any questions or need additional information, please call Brent Melson, Program Director for Information Technology Audits, or me at 202-358-1232.

A handwritten signature in black ink that reads "Robert J. Wesolowski". The signature is written in a cursive, slightly slanted style.

Robert J. Wesolowski

Enclosure

cc:
JM/Mr. H. Robbins
LaRC/136/Mr. E. Taylor (4 copies)

TABLE OF CONTENTS

BACKGROUND	1
OBSERVATIONS AND RECOMMENDATIONS	3
STRENGTHEN SYSTEM ACCESS CONTROLS	3
REDUCE THE NUMBER OF PEOPLE AUTHORIZED UNESCORTED ACCESS ...	6
IMPROVE THE AUTOMATED INFORMATION SECURITY PROGRAM	8
FORMALIZE MANAGEMENT CONTROLS	10
PERFORM PERIODIC TESTING OF BACKUP POWER SUPPLIES	11
RESTORE BARRIER TO PREVENT UNAUTHORIZED ACCESS	12
APPENDIX 1 – OBJECTIVES, SCOPE, AND METHODOLOGY	15
APPENDIX 2 - MANAGEMENT'S RESPONSE	17
APPENDIX 3 - REPORT DISTRIBUTION	23

This page intentionally left blank.

BACKGROUND

NASA uses many different data center facilities to accomplish its mission. These facilities support mission operations, research activities, and financial activities. Langley Research Center (LaRC) has five major data center facilities:

- the Supercomputing Network Subsystem (SNS) and Distributed Mass Storage System (DMSS),
- the Flight Simulation Computing System (FSCS),
- the Business Computing System,
- the Earth Observing System Distributed Active Archive Center (EOS DAAC), and
- a facility for classified work.

This audit focused on the SNS and DMSS, which are managed and operated by the Information Systems and Services Division (ISSD). These systems share a common area within the Central Scientific Computing Complex (CSCC).

The SNS included a Cray Y-MP supercomputer and a mass storage capability that is part of the DMSS. DMSS consists of high performance, state-of-the-art file servers and storage management systems. LaRC uses the DMSS to store output from supercomputing programs and data from LaRC wind tunnels, and to back up information on many LaRC local area networks and workstations.

This page intentionally left blank.

OBSERVATIONS AND RECOMMENDATIONS

OVERALL EVALUATION The general data center management controls for the SNS and DMSS were effective. Personnel interviewed were knowledgeable and dedicated to providing the highest level of customer support possible within existing budget constraints. We identified several security, environmental, and management control weaknesses that increased the level of risk to the facility. As we identified specific controls that could be improved, ISSD managers quickly began taking corrective actions. ISSD personnel made many improvements before the field work was completed.

STRENGTHEN SYSTEM ACCESS CONTROLS Access to NASA computer systems was not limited to those NASA and contractor employees and grantees needing the resources to perform their jobs. Our review showed approximately half of the authorized users did not use the computer systems during the last year. Access to computer resources was not terminated when employees left or when grants and contracts were completed. This resulted in increased risk of unauthorized use of the systems and the vulnerability of the system to outside attacks.

OMB Circular A-130 requires the use of "least privilege" as an operational control. "Least privilege" is the practice of restricting a user's access or type of access to the minimum necessary to perform his or her job.

Our system use review showed approximately 45 percent of the 1,391 authorized SNS users and approximately 52 percent of the 1,498 authorized DMSS users had not used the computer systems during the last year.

To determine if system access was being removed as needed, we evaluated a random sample of 94 individuals authorized SNS access. We found ten individuals whose access should have been removed because they either were no longer employed by NASA or the contract or grant they worked on had ended. In addition, we found someone used the login name and password for three of these individuals to successfully access the SNS after their work for NASA had ended. Someone also used the login name and password for one of these individuals to successfully access the DMSS. We referred these improper access activities to the NASA Office of Inspector General, Assistant Inspector General for Investigations.

The following causes contributed to the problem:

- ISSD routinely granted access to the entire SNS when access to only part of the system was needed.
- LaRC's out-processing procedures for employees were not followed. Some people left the Center without having their computer access withdrawn.
- Contracting Officer's Technical Representatives (COTRs) and grant technical offices did not tell the Division Computing Managers to remove access when contracts were completed and grants expired.
- The annual revalidation of computer users was not effective.

Inactive users increase the risk that someone may use computer resources for unauthorized purposes. It also increases the risk of damage or denial of service from computer attacks. Computer hackers use inactive accounts to break into the computers and destroy files or deny use of the resources to valid users. Therefore, strong computer system controls must be implemented.

RECOMMENDATION 1

The Information Systems and Services Division Chief should change the procedures for issuing computer access. Individual's access to computer systems should be limited to those specific resources needed to do their work.

Management's Response

We concur with this recommendation. The procedures for authorizing access to the Central Scientific Computing Complex resources are being revised to correct the problems identified in the report and to provide adequate service and response to the customer user community. The new procedures for obtaining a user account will include an identification of the specific resources to which the user's needs warrant their access and will separately grant access to each resource. The database which maintains user access data is being revised to permit review and audit of authorizations. The specific procedures have been documented and were published to ensure they are well known by the users and system administrators. They will be annually reviewed by the Center ITS (Information Technology Security) Officer for compliance. The new procedures were completed with user notification and publication of the procedures on August 12, 1997.

*Evaluation of
Management's Response*

Management has taken appropriate actions to correct the problems. We have closed this recommendation.

RECOMMENDATION 2

The Information Systems and Services Division Chief conduct a revalidation of authorized users. Users who have not used the systems in a reasonable period should have their access canceled.

Management's Response

We concur with this recommendation. A revalidation of the authorization for user access to Central Scientific Computing Complex resources was completed in conjunction with the transfer of the supercomputing capability to the Ames Research Center. Each account was reviewed, the appropriate Division Computing Manager contacted, and renewal of authorization received. Of the 1400 accounts, 1200 were removed from service for the supercomputing resources.

*Evaluation of
Management's Response*

Management has taken appropriate action to correct the problem. We have closed this recommendation.

RECOMMENDATION 3

The Information Systems and Services Division Chief implement a password aging system that automatically locks out users who do not use the system within a specified period. Users who are locked out should be required to rejustify their need to use the system before access is renewed.

Management's Response

We concur with this recommendation. Password aging is now in effect for all Central Scientific Computing Complex resources. User accounts which have not been accessed in 6 months are "disused." Procedures for notification and rejustification of access are included in the FY 1997 ITS Plan issued on August 12, 1997.

*Evaluation of
Management's Response*

Management's actions are responsive to the recommendation. We have closed this recommendation.

RECOMMENDATION 4

The Center Information Technology Security Manager should periodically remind Division Computing Managers, Contracting Officer's Technical Representatives, and grant technical managers of their responsibility for having computer access withdrawn when personnel leave or grants and contracts end.

Management's Response

We concur with this recommendation. Currently, when the Central Scientific Computing Complex manager is notified of the departure of a user, their authorization is terminated; in some cases, the account ID

is transferred to another user for review and clean up of files; notification of the departure of an on-site employee or contractor is accomplished when their access badge is turned in. Three additional actions have been taken in response to this recommendation: establishment of additional checkpoints, periodic notification of managers, and independent auditing. First, a review of current procurement documentation indicates that service contracts include clause LaRC 52.239-90 of May 1991 which directs the contractor to "promptly notify the Contracting Officer's Technical Representative when an authorized user employee no longer requires computer access." Second, an annual notification will be sent to all COTRs and contractors from the Acquisition Division, reminding them of the procedures to be used in discontinuing contractor employee access to Langley computing resources. Third, the user accounts are being tracked by authorizing organization in the user database to periodic review. Procedures for these actions are documented along with the actions discussed in Recommendation 1.

*Evaluation of
Management's Response*

Management's actions are responsive to the recommendation. We have closed this recommendation.

***REDUCE THE
NUMBER OF PEOPLE
AUTHORIZED
UNESCORTED ACCESS***

LaRC used a cardkey system for controlling unescorted access to the individual rooms housing important computer and communications equipment at all times and to the CSCC after normal duty hours. Once issued, a cardkey remained active until the owner returned it. Responsible security personnel were not monitoring use of the cardkeys nor requiring periodic revalidation of the need for unescorted access. Also, there were no written procedures requiring the monitoring of cardkey use or revalidation of unescorted access privileges. This unnecessary access increased the risk of damage to the facility.

Unescorted access to data center facilities should be limited to personnel requiring frequent access to do their jobs. When personnel leave or change jobs, their access should be withdrawn.

We identified 303 NASA and NASA contractor personnel who had active cardkeys for unescorted access to rooms containing SNS, the DMSS, and FSCS components. During our review of ISSD and the Scientific Computing Operations, Maintenance, and Communications Services contractor personnel, we identified 25 people whose cardkeys should have been canceled. They included former NASA

and contractor employees and current employees who no longer needed access because of job changes.

LaRC organizations and NASA contractors failed to notify the cardkey system administrator when people left, were transferred to new organizations, or were assigned new duties. For example, when several system analysts jobs were changed from supporting the SNS to supporting the EOS DAAC, their access to the SNS facilities was not removed. In addition, the Computer Security Officer (CSO) allowed the issuance of cardkeys with an indefinite life. No one was making periodic checks to see how often and where the cardkeys were used. The individual who performed these checks retired in 1994. Due to NASA's downsizing, he was not replaced.

Granting access to individuals who do not need frequent unescorted access and continuing that access when it is no longer needed increases the possibility of intentional or accidental damage or destruction of equipment and data. The risk of theft and unauthorized use also increases.

After this problem was identified, the CSO began monthly reviews of cardkey use and placed a 1-year expiration on all new cards. In addition, he has established a program to revalidate the need for all active cardkeys.

RECOMMENDATION 5

The Information Systems and Services Division Computer Security Officer should monitor cardkey use and require that all personnel with active cardkeys revalidate their need for unescorted access.

Management's Response

We concur with this recommendation. All of the cardkey data entries were reviewed and all that had not been used within the past twelve months were removed from the database and the cardkey holder notified. Beginning in February 1997, all new or revalidated cardkeys that are issued will be valid for a maximum period of one year. At the end of the 12-month period, it is required that the cardkey request be resubmitted for revalidation. Also beginning in June 1997, and continuing over a 6-month period, all active cardkey holders will be notified and required to resubmit a request form for revalidation of their cardkey. This revised procedure will ensure that all current cardkey entries are revalidated, and through the annual revalidation process, monitoring of the database will continue.

*Evaluation of
Management's Response*

Management has taken appropriate action to correct the problem. We have closed this recommendation.

RECOMMENDATION 6

The Information Systems and Services Division Computer Security Officer require the use of expiration dates in the cardkey system to create a continuing review of unescorted access to computer facilities.

Management's Response

We concur with this recommendation. Refer to the management response to recommendation 5.

*Evaluation of
Management's Response*

Management has taken appropriate action to correct the problem. We have closed this recommendation.

RECOMMENDATION 7

The Information Systems and Services Division Computer Security Officer conduct periodic reviews of cardkey use to aid in identifying those people who have a cardkey, but no longer need access to specific areas.

Management's Response

We concur with this recommendation. Refer to the management response to recommendation 5. As stated in the management response to recommendation 5, the revalidation of all cardkey entries will occur at intervals that will not exceed twelve months. This process will ensure that only those users requiring access to specific areas will continue to be authorized for access.

*Evaluation of
Management's Response*

Management has taken appropriate action to correct the problem. We have closed this recommendation.

**IMPROVE THE
AUTOMATED
INFORMATION
SECURITY PROGRAM**

The Automated Information Security (AIS) program did not have current, formal plans and procedures. Management did not provide adequate resources to conduct the AIS program. This reduced both the program's effectiveness and the level of protection provided to computer resources.

"NASA Automated Information Security Handbook," NHB 2410.9A, requires that each Center develop a Center AIS plan. The Center plan summarizes the overall status and direction of AIS strategies and objectives, accomplishments, and on-going activities throughout a Center and at data processing installations (DPI) under the Center's cognizance. The Center plan should be updated annually. The handbook also requires a separate detailed plan for each DPI. The DPI plan elements include current controls, application sensitivities,

contingency plans, action schedules, review results, awareness and training, security tools, incident identification, and security contacts. The DPI plan must be kept current. OMB Circular A-130, "Management of Federal Information Resources," requires system security reviews when major changes occur or at least every 3 years.

LaRC did not have a current security plan. The most recent plan is for 1993. This plan is outdated as noted below.

- The FY 1993 Center AIS Plan listed eight level 2 computer systems; however, in an interview, the auditor was told there were only four DPIs. We did not find any documentation describing the composition of each DPI.
- The EOS DAAC, a major DPI, was not included in the plan.
- ISSD has removed or replaced much of the equipment listed in the FY 1993 Center plan.
- ISSD had removed security measures mentioned in the plan, such as the 24-hour physical security protection (guards and TV surveillance) for the CSCC.

DPI Plans Not Prepared

There was no DPI plan for the SNS or DMSS. Nor did we find any other official documents that provided a detailed description of the security procedures and standards that management had determined were necessary. There was no documentation to explain why a plan was not developed.

Security Reviews Not Performed

Also, ISSD did not perform periodic system security reviews. The last evidence we found of a system security review was the FY 1993 Risk Assessment. We did not find any documentation to indicate whether management took actions to correct the deficiencies identified in the FY 1993 Risk Assessment or decided to accept the risk and do nothing.

Within the ISSD, there was a culture of relying on informal decisions and procedures. Many procedures and decisions were not documented. When personnel responsible for the security program and risk assessments left, they took much of the knowledge of security requirements and what had been done with them.

The lack of plans, documentation of current security policies and procedures, and management decisions regarding security created weaknesses in the AIS program and increased the risk to SNS and DMSS resources and user data.

RECOMMENDATION 8

The ISSD Chief should ensure plans are developed, maintained, and implemented; and decisions on security issues are documented.

Management's Response

We concur with this recommendation. The existing Langley Research Center ITS Plan has been revised to reflect current conditions and systems and was completed on August 12, 1997. A formal ITS Plan for the Central Scientific Computing Complex has been prepared and was completed on August 12, 1997. Both plans provide for the retention of a formal, auditable record of decisions being made related to ITS matters.

Evaluation of Management's Response

Management has taken appropriate action to correct the problem. We have closed this recommendation.

***FORMALIZE
MANAGEMENT
CONTROLS***

There were no written policies, procedures, or standards for many operational aspects of the SNS and DMSS. Management controls in the form of operating policies, procedures, and standards are necessary to provide reasonable assurance that organization objectives will be achieved and that undesired events will be prevented or detected and corrected.

Policies should be explicit and current. Standards should describe specific requirements that must be met to comply with a given policy. Written documentation of these controls provides a record of how management wants the organization to function and aids in transmitting this information to employees and contractors.

Areas lacking documentation included:

- end user and system administrator responsibilities for security and control;
- use of powerful system utility programs that could result in unauthorized data manipulation, accidental or deliberate destruction of existing data files, bypassing operating system controls, or overriding password protection;

- storage management; and
- backup and recovery of data and programs.

ISSD management did not believe written policies and procedures were necessary. For many years, the turnover of personnel was low, making it possible for the organization to function informally and operate by relying on the historical knowledge of its personnel.

The loss of long-term employees over the last 3 years and recent reorganizations have greatly reduced the corporate knowledge. Managers and employees working in areas new to them lack the historical knowledge and do not have the benefit of written documentation to aid them in their daily work. The many recent and future changes, such as the ISSD reorganization and the shutdown of the Cray Y-MP computer, create the need to change operating procedures. The lack of written directives will increase the time and effort needed to determine which controls should be changed and what the new controls should be.

RECOMMENDATION 9

The Information Systems and Services Division Chief should develop formal policies, procedures, and standards describing the management controls necessary for operating the data processing installations.

Management's Response

We concur with this recommendation. Formal documentation of the existing procedures for management controls of the Central Scientific Computing Complex has been prepared and was completed on August 12, 1997.

Evaluation of Management's Response

Management's actions are responsive to the recommendation. We have closed this recommendation.

PERFORM PERIODIC TESTING OF BACKUP POWER SUPPLIES

Uninterruptible Power Supplies (UPS) should be tested periodically to determine if they will function properly when needed. The UPS for the DMSS had not been tested regularly. Facilities and operations management personnel did not think periodic testing was necessary and were concerned that a lengthy recovery period might be necessary if the UPS failed during the test and the system crashed. This could have resulted in loss of data and loss of DMSS availability for a few days that would have been preventable.

When we brought this issue to the attention of the Building 1268 Facility Manager, he implemented a periodic testing program for all UPSs in the CSCC.

RECOMMENDATION 10

The Building 1268 Facility Manager should develop and implement a program for periodic testing of the UPS.

Management's Response

We concur with this recommendation. A purchase order for preventive and remedial maintenance support for the three Uninterruptible Power Supplies (UPS) that are no longer covered under a manufacturer's warranty was issued to EPE Technologies on December 9, 1996. Under this purchase order with EPE, there will be two scheduled preventive checks that will fully test the operation and backup of the UPS systems. These tests will include bypassing that verified production system loading would be expected during actual power loss situations. The remaining three UPS systems are under factory warranty, and are tested in the same manner as the other three systems. The EPE factory representative was on-site at LaRC on May 7, 1997, and an outage system test was performed on all five UPS systems that were installed at that time.

Evaluation of Management's Response

Management has taken appropriate action to correct the problem. We have closed this recommendation.

RESTORE BARRIER TO PREVENT UNAUTHORIZED ACCESS

The existing walls and cardkey controlled doors did not prevent unauthorized access to the rooms containing the SNS and DMSS computer systems. A combination of true floor to ceiling walls and controlled doors are necessary to control entry to computer facilities.

We found the wall between rooms 2092 and 2086 in building 1268 went only from the raised floor to the dropped ceiling. Unauthorized access to the Cray Y-MP computer and DMSS could be achieved by using a ladder to climb over the wall or taking out the raised floor panels and going under it. Room 2092 was originally part of a large computer facility. This room's two exterior walls were part of the barriers that restricted access to the facility. The wall between rooms 2092 and 2086 was an interior wall. When ISSD removed the computer equipment located in room 2092, they converted the room to office space. They deactivated the cardkey reader that controlled the door to room 2092 from the hallway. These actions made the wall between room 2092 and 2086 an exterior wall.

Access to the building 1268 complex is not controlled during normal work hours. The combination of the open building and the inadequate wall results in uncontrolled access to the data facility. This increases the risk of theft or intentional damage or destruction of equipment and data.

The Building 1268 Facility Manager reactivated the cardkey reader for the door to room 2092.

RECOMMENDATION 11

The Building 1268 Facility Manager should secure the facility. Reactivating the cardkey control for the door from the hallway to room 2092 and making room 2092 part of the facility is probably the quickest and cheapest solution.

Management's Response

We concur with this recommendation. The cardkey to room 2092 was activated on June 2, 1997, and the room is now secured.

***Evaluation of
Management's Response***

Management has taken appropriate action to correct the problem. We have closed this recommendation.

This page intentionally left blank.

OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVE

Our objective was to determine whether general data central controls for the SNS and the DMSS at LaRC were sufficient to achieve a secure and reliable processing environment.

***SCOPE AND
METHODOLOGY***

We interviewed ISSD civil service personnel and contractor personnel to obtain an understanding of the general data center controls and procedures. We reviewed plans and formal directives. We sampled from lists of authorized computer users and personnel authorized physical access to the computer facilities to learn how well the security controls were working. We toured the specific rooms that contain the computer equipment and reviewed facility records in checking physical security and environmental conditions.

***MANAGEMENT
CONTROLS
REVIEWED***

We reviewed general policies, procedures, and standards for the following data center areas:

- agency review and monitoring,
- physical security,
- environmental protection,
- general computer operations activities,
- library functions,
- data communications networks,
- storage management,
- file retention and backup/recovery procedures, and
- software change management.

AUDIT FIELD WORK

We performed field work at LaRC from November 1996 to April 1997. We conducted the audit in accordance with generally accepted government auditing standards.

This page intentionally left blank.

MANAGEMENT'S RESPONSE

National Aeronautics and
Space Administration
Langley Research Center
Hampton, VA 23681-0001



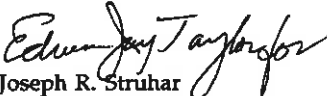
Reply to Atn of: 136

August 14, 1997

TO: W/Acting Assistant Inspector General for Auditing
FROM: 109/Langley Research Center
Management Control Officer
SUBJECT: Draft Audit Report A-HA-97-022, NASA Data Center
Facility, Langley Research Center

Submitted for your consideration are the Center responses to 11 recommendations contained in the draft report. The audited organization concurs with the recommendations and believes they have taken the necessary action to correct and close them.

Questions regarding the responses can be directed to Jay Taylor the Center Audit Liaison representative at 757-864-2605.


Joseph R. Struhar

National Aeronautics and
Space Administration
Langley Research Center
Hampton, VA 23681-0001



Reply to ATR 6:

157

AUG 13 1997

TO: 109/Chief Financial Officer
THRU: 136/Audit Liaison Representative
FROM: 157/Assistant Division Chief, ISSD
SUBJECT: Draft Audit Report Response, Assignment Number A-HA-97-022

ISSD has completed the review of the recommendations that were submitted following the audit of the Central Scientific Computing Complex at Langley Research Center. Following is our comments relative to each of the recommendation presented in the draft audit report. If you have any questions, or require additional information, please contact me at extension 47065, or Sam McPherson at extension 46639

Recommendation 1: The Information Systems and Services Division Chief should change the procedures for issuing computer access. An individual's access to computer systems should be limited to those specific resources needed to do their work.

Management's Response to Recommendation 1:

We concur with this recommendation. The procedures for authorizing access to the Central Scientific Computing Complex resources are being revised to correct the problems identified in the report and to provide adequate service and response to the customer user community. The new procedures for obtaining a user account will include an identification of the specific resources to which the user's needs warrant their access and will separately grant access to each resource. The database which maintains user access data is being revised to permit review and audit of authorizations. The specific procedures have been documented and were published to ensure they are well known by the users and system administrators. They will be annually reviewed by the Center ITS (Information Technology Security) Officer for compliance. The new procedures were completed with user notification and publication of the procedures on August 12, 1997.

Recommendation 2: The Information Systems and Services Division Chief conduct a revalidation of authorized users. Users who have not used the systems in a reasonable period should have their access canceled.

Management's Response to Recommendation 2:

We concur with this recommendation. A revalidation of the authorization for user access to Central Scientific Computing Complex resources was completed in conjunction with the transfer of the supercomputing capability to the Ames Research Center. Each account was reviewed, the appropriate Division Computing Manager contacted, and renewal of authorization received. Of the 1400 accounts, 1200 were removed from service for the supercomputing resources.

Recommendation 3: The Information Systems and Services Division Chief implement a password aging system that automatically locks out users who do not use the system within a specified period. Users who are locked out should be required to rejustify their need to use the system before access is renewed.

Management's Response to Recommendation 3:

We concur with this recommendation. Password aging is now in effect for all Central Scientific Computing Complex resources. User accounts which have not been accessed in 6 months are "disused." Procedures for notification and rejustification of access are included in the FY 1997 ITS Plan issued on August 12, 1997.

Recommendation 4: The Center Information Technology Security Manager should periodically remind Division Computing Managers, Contracting Officer's Technical Representatives, and grant technical managers of their responsibility for having computer access withdrawn when personnel leave or grants and contracts end.

Management's Response to Recommendation 4:

We concur with this recommendation. Currently, when the Central Scientific Computing Complex (CSCC) manager is notified of the departure of a user, their authorization is terminated; in some cases, the account ID is transferred to another user for review and clean up of files; notification of the departure of an on-site employee or contractor is accomplished when their access badge is turned in. Three additional actions have been taken in response to this recommendation: establishment of additional check-points, periodic notification of managers, and independent auditing. First, a review of current procurement documentation indicates that service contracts include clause LaRC 52.239-90 of May 1991 which directs the contractor to "promptly notify the Contracting Officer's Technical Representative (COTR) when an authorized user employee no longer requires computer access." Second, an annual notification will be sent to all COTRs and contractors from the Acquisition Division, reminding them of the procedures to be used in discontinuing contractor employee access to Langley computing resources. Third, the user accounts are being tracked by authorizing organization in the user database to periodic review. Procedures for these actions are documented along with the actions discussed in Recommendation 1.

Recommendation 5: The Information Systems and Services Division Computer Security Officer should monitor cardkey use and require that all personnel with active cardkeys revalidate their need for unscorted access.

Management's Response to Recommendation 5:

We concur with this recommendation. All of the cardkey data entries were reviewed and all that had not been used within the past twelve months were removed from the database and the cardkey holder notified. Beginning in February 1997, all new or revalidated cardkeys that are issued will be valid for a maximum period of one year. At the end of the 12-month period, it is required that the cardkey request be resubmitted for revalidation. Also beginning in June 1997, and continuing over a 6-month period, all active cardkey holders will be notified and required to resubmit a request form for revalidation of their cardkey. This revised procedure will ensure that all current cardkey entries are revalidated, and through the annual revalidation process, monitoring of the database will continue.

Recommendation 6: The Information Systems and Services Division Computer Security Officer require the use of expiration dates in the cardkey system to create a continuing review of unescorted access to computer facilities.

Management's Response to Recommendation 6:

We concur with this recommendation. Refer to the management response to recommendation 5.

Recommendation 7: The Information Systems and Services Division Computer Security Officer conduct periodic reviews of cardkey use to aid in identifying those people who have a cardkey, but no longer need access to specific areas.

Management's Response to Recommendation 7:

We concur with this recommendation. Refer to the management response to recommendation 5. As stated in the management response to recommendation 5, the revalidation of all cardkey entries will occur at intervals that will not exceed twelve months. This process will ensure that only those users requiring access to specific areas will continue to be authorized for access.

Recommendation 8: The ISSD Chief should ensure plans are developed, maintained, and implemented, and decisions on security issues are documented.

Management's Response to Recommendation 8:

We concur with this recommendation. The existing Langley Research Center ITS Plan has been revised to reflect current conditions and systems and was completed on August 12, 1997. A formal ITS Plan for the Central Scientific Computing Complex has been prepared and was completed on August 12, 1997. Both plans provide for the retention of a formal, auditable record of decisions being made related to ITS matters.

Recommendation 9: The Information Systems and Services Division Chief should develop formal policies, procedures, and standards describing the management controls necessary for operating the data processing installations.

Management's Response to Recommendation 9:

We concur with this recommendation. Formal documentation of the existing procedures for management controls of the Central Scientific Computing Complex has been prepared and was completed on August 12, 1997.

Recommendation 10: The Building 1268 Facility Manager should develop and implement a program for periodic testing of the UPS.

Management's Response to Recommendation 10:

We concur with this recommendation. A purchase order for preventive and remedial maintenance support for the three Uninterruptible Power Supplies(UPS) that are no longer covered under a manufacturer's warranty was issued to EPE Technologies on December 9, 1996. Under this purchase order with EPE, there will be two scheduled preventive checks that will fully test the operation and backup of the UPS systems. These

tests will include bypassing that verified production system loading would be expected during actual power loss situations. The remaining three UPS systems are under factory warranty, and are tested in the same manner as the other three systems. The EPE factory representative was on-site at LaRC on May 7, 1997, and an outage system test was performed on all five UPS systems that were installed at that time.

Recommendation 11: The Building 1268 Facility Manager should secure the facility. Reactivating the cardkey control for the door from the hallway to room 2092, and making room 2092 part of the facility is probably the quickest and cheapest solution.

Management's Response to Recommendation 11:

We concur with this recommendation. The cardkey to room 2092 was activated on June 2, 1997, and the room is now secured.

Ronald L. Baker
Ronald L. Baker
47065

cc:
157/ISSD
179/PIO
157C/CIO
179/S. A. McPherson
136/Audit Liaison

179/SAMcPherson:ldb 08-12-97 (45792)

This page intentionally left blank.

REPORT DISTRIBUTION

National Aeronautics and Space Administration (NASA) Headquarters

Code AO/Chief Information Officer
Code B/Chief Financial Officer
Code B/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 R/Associate Administrator for Aeronautics and Space Transportation Technology
Code R/Information Technology Officer
Code W/Inspector General (10 copies)

NASA Field Installations

Director, Langley Research Center
Chief Financial Officer, Langley Research Center (5 copies)
Chief Information Officer, Langley Research Center

NASA Offices of Inspector General

Ames Research Center
Dryden Flight Research Center
Goddard Space Flight Center
Jet Propulsion Laboratory
Lyndon B. Johnson Space Center
John F. Kennedy Space Center
Langely Research Center
Lewis Research Center
George C. Marshall Space Flight Center
John C. Stennis Space Center

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, Subcommittee on Science, Technology, and Space c/o Tom Cooley

**Chairman and Ranking Minority Members - Congressional Committees and
Subcommittees**

Senate Committee on Appropriations
Senate Committee on VA-HUD-Independent Agencies
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

Congressional Members

The Honorable Pete Sessions, U.S. House of Representatives

Major Contributors to the Report

James W. Geith, Auditor

Gregory B. Melson, Program Director for Information Technology Audits

Patricia C. Reid, Audit Program Assistant

