IG-97-030

# AUDIT REPORT

## RAPID ACTION

# PHYSICAL SECURITY AT ARC'S NAS FACILITY

July 18, 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 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.

National Aeronautics and
Space Administration
**Headquarters**
Washington, DC 20546-0001

Reply to Attn of: **W**

**July 18, 1997**

**TO:** **Ames Research Center**
**Attn: D/Center Director**

**FROM:** **W/Acting Assistant Inspector General for Auditing**

**SUBJECT:** **Final Rapid Action Report on Physical Security at ARC's Numerical Aerospace Simulation (NAS) Facility**
**Assignment Number A-HA-97-051**
**Report Number IG-97-030**

During our audit of data center operations at the Ames Research Center (ARC) NAS Facility, we found that the facility does not have adequate backup and/or contingency security procedures in place to deal with key-card access system failures. On March 27, 1997, the facility's keypad and key-card access system failed completely, leaving the facility unsecured. It remained unsecured until May 1, 1997. As a result of this condition, a group of people gained unauthorized access to one of the NAS main computer rooms.

On May 9, 1997, NAS management prepared a written report detailing the interim security measures it planned to implement to secure the NAS facility until a new key-card system is installed. Although these interim security measures address our immediate concerns, NAS management needs to reassess its long-term physical security measures to ensure that the NAS facility will be adequately secured in the future.

The OIG issued a draft rapid action report to ARC management on June 12, 1997. Management's response sufficiently addresses our recommendations, and is included in its entirety as Appendix B of the report.

In accordance with NMI 9910.1B, please include our office in the concurrence cycle to close Recommendations 3 and 4 of the report. We consider Recommendations 1 and 2 closed on issuance of this report. If you have any questions, please call Mr. Brent Melson, Program Director - Information Technology Audits, at Headquarters, or me on (202) 358-1232.

Robert J. Wesolowski

Enclosure

cc:
AO/Chief Information Officer (w/encl.)
JM/Management Assessment Division (w/10 encl.)
R/OASTT Chief Information Officer (w/encl.)
ARC/W/Program Director for Information Technology (w/o encl.)
I/Director, Office of the Director of Information Systems (w/encl.)
IA/Chief Information Officer (w/encl.)
IN/Acting Manager, NAS Systems Division (w/encl.)
J/Audit Liaison Representative (w/6 encl.)

# *TABLE OF CONTENTS*

This page intentionally left blank.

## *BACKGROUND*

The NASA Office of Inspector General is conducting an audit evaluating the adequacy of general controls over Ames Research Center's (ARC) Numerical Aerospace Simulation (NAS) Program Facility data center operations. While conducting our audit of the NAS data center operations, we identified a condition that warrants management's immediate attention. We have issued this rapid action report because of the significance and time-sensitivity of this condition. The NAS Program focuses resources on solving critical problems in aeroscience, space technology, and related applications by utilizing the power of the most advanced supercomputers available. A key-card access system controls access to the buildings which house the NAS Facility.

The NAS facility is recognized nationwide as the premier location to prototype new, large-scale computer systems; undertake the largest aerospace simulation problems attempted; and perform leading-edge research. Additionally, the NAS facility is considered the centerpiece for other NASA IT projects and programs such as the High Performance Computing and Communications Program and the Consolidated Supercomputing Management Office.

## *OVERALL EVALUATION*

The NAS Facility does not have adequate backup or contingency security procedures to deal with key card access security system breakdowns. Audit work completed to date has disclosed a serious physical security condition at the NAS facility. On March 27, 1997, the key-card access system failed completely, leaving the facility unsecured. One group of people gained unauthorized access to one of the NAS main computer rooms. As a result, physical security has been compromised. NAS management needs to take immediate corrective action. According to NASA's Equipment Management System (NEMS), assets valued at over $81 million are at risk. NAS management did not implement supplemental security measures until after a visit from the OIG on May 1, 1997.

## *NAS KEY-CARD ACCESS SYSTEM FAILURES*

The NAS keypad and key-card access system (key-card access system) has broken down about once every 3 months over the past year. The breakdowns range from minor, when individual doors do not work correctly, to major breakdowns when the entire system ceases to function. The most recent major system breakdown

occurred on March 27, 1997, when the computer system controlling the key-card access system, crashed. Since then, the key-card access system has remained completely inoperable. Backup and/or contingency plans were not in place to provide for adequate protection of the NAS facility assets after the system failed.

---

***BACKUP SYSTEM OR CONTINGENCY PLANS NOT IN PLACE***

On April 10, 1997, we visited the facilities when the OIG became aware of this latest system breakdown. We were informed by NAS personnel that there was no backup system, and that no contingency security plans were put in place. The auditor-in-charge advised NAS management of our concerns regarding this condition and suggested that supplemental security measures be implemented. On May 1, we conducted a tour of the facilities and observed no changes in supplemental security measures. During numerous visits to the facility from April 10 to May 1, 1997, we noted the following conditions at the NAS facilities.

***Open Access Doors Permit Unauthorized Entry***

**The Main NAS Facility Building:** Before shutting down the key-card access system computer for repairs, NAS employees set the doors to rooms 226 and 230 in "open" mode to allow unrestricted access into those rooms. Once inside room 226, access is unrestricted into room 227, which houses the control room for the entire NAS facility. According to the NEMS, the value of the computing assets within these three rooms is $30.2 million.

Room 230 houses the NAS Mass Storage Subsystem (NAStore), and various other processors that support the system. The NAStore system provides permanent storage for data generated by hundreds of scientific users of the two Cray supercomputers housed in room 229. Once inside room 230, only one locked door secures access to these two Cray supercomputers and related computing assets valued at over $51 million.

The outside doors to the building are left open from 6:00 a.m. to 6:00 p.m. After 6:00 p.m., these doors are manually locked. Accordingly, from 6:00 a.m. to 6:00 p.m. during the period March 27 to May 1, 1997, anyone at the center had direct access to the computer equipment located in rooms 226, 227, and 230. NAS management initiated no additional ARC security patrols during this timeframe.

***NAS Security Incident***

On May 1, 1997, an "unscheduled" group of about six junior high-aged students and two accompanying adult leaders (non-NAS personnel) gained unauthorized and unrestricted access to computer rooms 226 and 230. The group simply tested the doors, found they were open, and walked in. Only after the group was already inside room 230 did anyone from the NAS facility stop them from continuing the unauthorized tour.

***Doors Propped or Taped Open***

**NAS Support Buildings A and B:** We observed that each of the four entrance doors into building A were either propped open or the door latches were taped open (see Exhibit 1 for pictures of doors propped open).

Room 119, at the center of building B, houses NAS routing and networking equipment used for connecting workstations within building B, as well as equipment used for indirect connection to the main computer resources housed in the main NAS building. The door to room 119 is controlled by the key-card access system. We found that door propped open, allowing us unrestricted access to all of the equipment housed within room 119.

The outside doors to both buildings A and B have remained in this open condition during weekday evening hours and over weekends during the period March 27 to May 1, 1997. Again there were no indications that additional ARC security patrols were either requested or made during this timeframe.

We confirmed the above conditions through subsequent on-site physical observations and contacts with NAS personnel and contractors.

---

***INTERIM SECURITY PLAN INSTITUTED***

On May 2, 1997, NAS management and representatives from ARC's Code I met with the OIG to discuss this security issue. As a result of this meeting, NAS management prepared a report dated May 9, 1997, entitled "NAS Facility Interim Security Report." The report details the temporary security measures the NAS Systems Division has put in place since May 1, 1997. These interim measures adequately address our immediate concerns. NAS management needs to maintain these security measures until the new security system has been installed and thoroughly tested.

| | |
|---|---|
| ***CONCLUSION*** | The NAS facility does not have adequate backup and/or contingency security procedures in place to deal with key-card access security system breakdowns. As a result of this condition, physical security at the facility has been compromised to the point that "unauthorized" access to one of the main computer rooms was allowed to occur. NAS management needs to take immediate action to develop and implement a contingency plan that will adequately protect the NAS facility from future key-card access system failures. |
| ***RECOMMENDATION 1*** | The NAS Systems Division (Acting) Manager should maintain the supplemental security measures identified in the NAS Facility Interim Security Report dated May 9, 1997, until a new security system has been installed and thoroughly tested. |
| ***Management's Response*** | CONCUR. The security measures detailed in the NAS Facility Interim Report have been in place since May 1, 1997. They will continue as needed until the replacement card access is in place. The Security Report detailed a schedule for the installation and test of this new system, which is scheduled to be operational by July 1, 1997. This installation is on schedule and the new card access system is already functioning on more than 60% of the facility. The most critical areas have been brought up on the new system first. |
| ***Evaluation of Management's Response*** | The actions taken and to be taken satisfy the intent of the recommendation. |
| ***RECOMMENDATION 2*** | The NAS Systems Division (Acting) Manager should evaluate the costs and benefits of installing a backup system to the new keypad and key-card system currently planned to be installed. |
| ***Management's Response*** | CONCUR. The new card access system is over 10 years newer than the system it is replacing. The technology utilized in the new system has addressed the issue of system failure, and a backup system is not necessary. The new system does not have any single points of failure, all critical functions in the system have backups, and the system uses a distributed hierarchy of processors, all which normally work together but can work independently if necessary. Virtually the only way the whole system can fail is if every component in the system failed. We are also stocking an inventory of spare parts, including key pads and readers, so that we can quickly address any individual reader failures. |

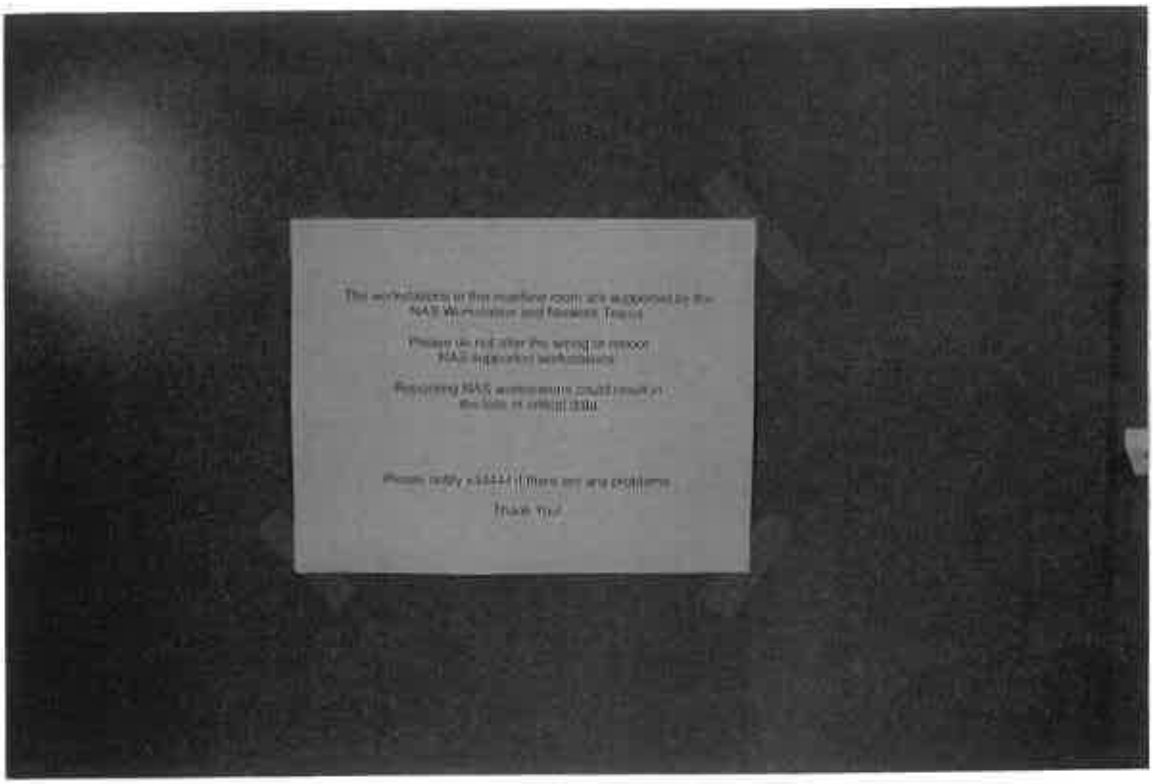
| | |
|---|---|
| ***Evaluation of Management's Response*** | The actions taken satisfy the intent of the recommendation. |

| | |
|---|---|
| ***RECOMMENDATION 3*** | The NAS Systems Division (Acting) Manager should establish a contingency security plan that is automatically placed in effect when the access system fails. |
| ***Management's Response*** | CONCUR. The NAS Facility Interim Security Report dated May 9, 1997, is currently being modified to more generally address this issue. This plan will be in place by July 15, 1997. |
| ***Evaluation of Management's Response*** | The actions to be taken satisfy the intent of the recommendation. |

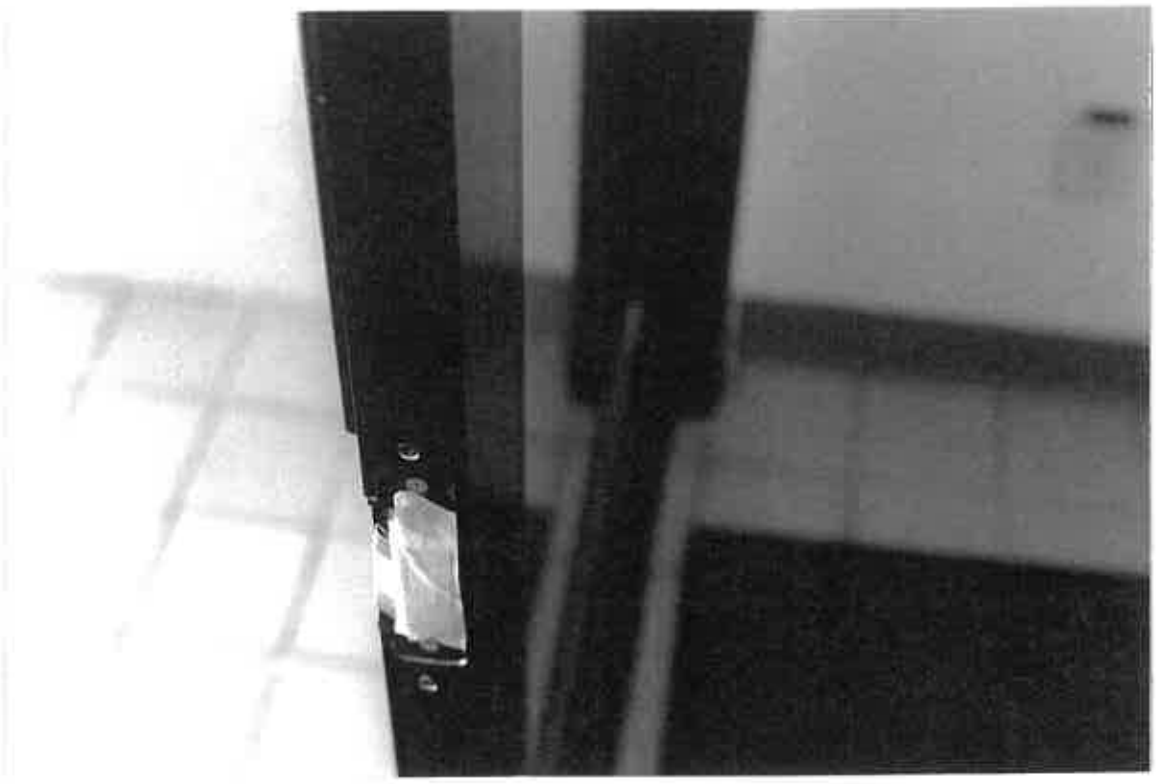
| | |
|---|---|
| ***RECOMMENDATION 4*** | The NAS Systems Division (Acting) Manager should evaluate and document its policy and procedures for permitting/conducting tours of the NAS facility. |
| ***Management's Response*** | CONCUR. Included with the NAS Facility Interim Security Report was a draft NAS Tour Policy. This policy is currently under review and will be adopted by July 15, 1997. |
| ***Evaluation of Management's Response*** | The actions to be taken satisfy the intent of the recommendation. |

DOOR PROPPED OPEN AT NAS
SUPPORT BUILDING B

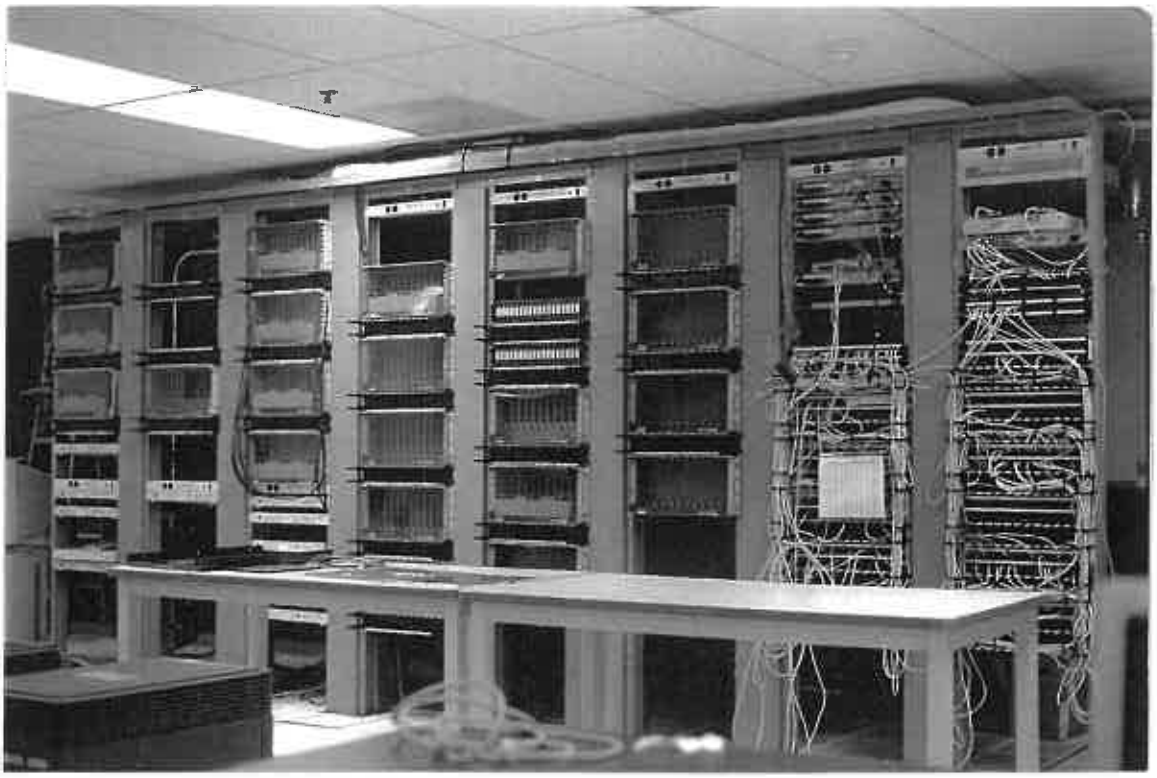
DOOR PROPPED OPEN TO ROOM 119
IN NAS SUPPORT BUILDING B



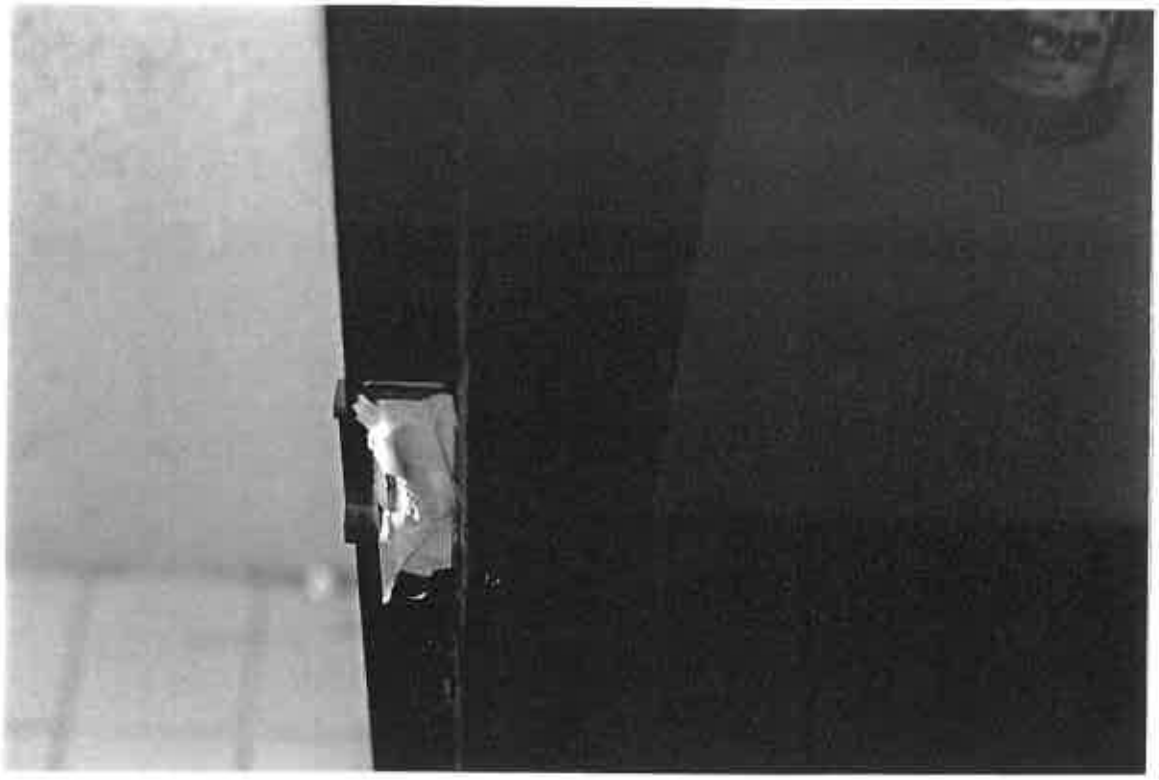
SIGN ON DOOR TO ROOM 119
NAS SUPPORT BUILDING B



TAPED DOOR AT NAS SUPPORT BUILDING B



EQUIPMENT IN ROOM 119, NAS SUPPORT BUILDING B



TAPED DOOR AT NAS SUPPORT BUILDING B

NEWSPAPER IN DOOR AT NAS SUPPORT BUILDING B

NEWSPAPER IN DOOR AT NAS SUPPORT BUILDING A

PIECE OF WOOD IN DOOR AT NAS SUPPORT BUILDING A

| | |
|---|---|
| ***OBJECTIVES*** | Our audit objective was to determine whether the (NAS) data center facilities have adequate physical and environmental controls, and are managed in a manner that provides for a secure and reliable processing environment. These controls include physical security, environmental controls and the management of general data center activities. |
| ***SCOPE AND METHODOLOGY*** | In addressing our objective, we interviewed NAS management officials, employees, and contractors; made numerous on-site visits to the NAS facilities; examined various NAS policy and procedures documents; and reviewed other relevant documents. |
| ***AUDIT FIELD WORK*** | Audit field work began in December 1996 and continues at ARC. The audit is being performed according to generally accepted government auditing standards, and includes such examinations and tests of applicable records and documents as are considered necessary in the circumstances. |

National Aeronautics and
Space Administration
**Ames Research Center**
Moffett Field, CA 94035-1000

Reply to Attn of: J:241-11

JUL 1 1997

TO: NASA Headquarters
Attn: W/Robert J. Wesolowski, Assistant Inspector General for Auditing

FROM: Director of Center Operations

SUBJECT; Draft Audit Report on Physical Security at ARC's Numerical Aerospace Simulation (NAS) Facility, Ames Research Center, Assignment No. A-HA-97-051

We have reviewed the subject report and appreciate the opportunity to respond.

RECOMMENDATION 1

The NAS Systems Division (Acting) Manager should maintain the supplemental security measures identified in the NAS Facility Interim Security Report dated May 9, 1997, until a new security system is installed and thoroughly tested.

RESPONSE: CONCUR

The security measures detailed in the NAS Facility Interim Report (Exhibit #3 to the IG Rapid Action Report), have been in place since May 1, 1997. They will continue as needed until the replacement card access is in place. The Security Report detailed a schedule for the installation and test of this new system, which is scheduled to be operational by July 1, 1997. This installation is on schedule and the new card access system is already functioning on more than 60% of the facility. The most critical areas have been brought up on the new system first.

RECOMMENDATION 2

The NAS Systems Division (Acting) Manager should evaluate the cost and benefits of installing a backup system to the new keypad and key-card system currently planned to be installed.

RESPONSE: CONCUR

The new card access system is over 10 years newer than the system it is replacing. The technology utilized in the new system has addressed the issue of system failure, and a backup system is not necessary. The new system does not have any single points of failure, all critical functions in the system have backups, and the system uses a distributed hierarchy of processors, all which normally work together but can work independently if necessary. Virtually the only way the whole system can fail is if every component in the system failed. We are also stocking an inventory of spare parts, including key pads and readers, so that we can quickly address any individual reader failures.

RECOMMENDATION 3

The NAS Systems Division (Acting) Manager should establish a contingency security plan that is automatically placed in effect when the access system fails.

RESPONSE: CONCUR

The NAS Facility Interim Security Report (Exhibit #3 to the IG Rapid Action Report) dated May 9, 1997, is currently being modified to more generally address this issue. This plan will be in place by July 15, 1997.

RECOMMENDATION 4

The NAS Systems Division (Acting) Manager should evaluate and document its policy and procedures for permitting/conducting tours of the NAS Facility.

RESPONSE: CONCUR

Included with the NAS Facility Interim Security Report (Exhibit #3 in the IG Rapid Action Report) was a draft NAS Tour Policy. This policy is currently under review and will be adopted by July 15, 1997.

Based on the information provided, the Center requests closure of Recommendations 1 and 2. If you have questions or need further information, please contact Katie Garcia at (415) 604-5669.

Jana M. Coleman

cc:
NASA HQ/Code JM/Mitzi Peterson
ARC
258-5/M. Chancellor
15-1/C. Herbert

# *DISTRIBUTION LIST*

**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 System 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/Chief Information Officer Representative
Code S/Associate Administrator for Space Science

**NASA Field Installations**

D/Director, Ames Research Center
I/Director, Office of the Director of Information Systems, Ames Research Center
IA/Chief Information Officer, Ames Research Center
IN/Manager, Numerical Aerospace Simulation Systems Division, Ames Research Center

**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

**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

**Non-NASA Federal Organizations and Individuals (cont.)**

Associate Director, National Security and International Affairs Division, General Accounting Office
Special Counsel, Subcommittee on National Security, International Affairs, and Criminal Justice

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

Senate Committee on Appropriations
Senate Subcommittee 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 THIS REPORT*

| | |
|---|---|
| *HEADQUARTERS* | Gregory B. Melson, Program Director |
| *AMES RESEARCH CENTER* | Michael D. Morigeau, Auditor-in-Charge |