IG-97-039

AUDIT REPORT

NASA DATA CENTER GENERAL CONTROLS MARSHALL SPACE FLIGHT CENTER

September 30, 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, D.C. 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, D.C. 20026. The identity of each writer and caller can be kept confidential upon request to the extent permitted by law.

ACF2	Access Control Facility/2
IBM	International Business Machines
ISSO	Information Systems Services Office
LeRC	Lewis Research Center
LPAR	Logical Partition
MSFC	Marshall Space Flight Center
NACC	NASA Automated Data Processing Consolidation Center
NACOMN	NASA Common System
OIG	Office of Inspector General
OMB	Office of Management and Budget

National Aeronautics and
Space Administration

Headquarters
Washington, DC 20546-0001

SEP 30 1997

Reply to Attn of: W

TO: George C. Marshall Space Flight Center
Attn: DA01/Center Director

FROM: W/Acting Assistant Inspector General for Auditing

SUBJECT: Final Audit Report
NASA Data Center Facility - MSFC
Assignment Number A-HA-97-024
Report Number IG-97-039

We have completed an audit of the NASA Automated Data Processing (ADP) Consolidation Center (NACC) at Marshall Space Flight Center. The purpose of the audit was to determine whether NACC management has established an adequate internal control structure to provide for a reliable computing environment. In general, the controls for the NACC were adequate. We did identify several areas requiring management's attention, including (1) physical security, (2) environmental protection, (3) technical standards, (4) security administration, (5) software change management, and (6) tape management.

A discussion draft report was issued on August 7, 1997. Management responded on September 9, 1997. The response is included after each recommendation and is presented in its entirety as Appendix 3. The response indicates that management has implemented or will implement 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 Services Office personnel. If you have any questions or need additional information, please call Brent Melson, Program Director - Information Technology Audits, or me at (202) 358-1232.

Robert J. Wesolowski
Robert J. Wesolowski

Enclosure

cc:
AO/R. West
JM/D. Green
MSFC/AI01/C. Houston
BE/J. Kerby
DE01/S. McGuire Smith

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

INTRODUCTION

NASA is consolidating all administrative systems running on IBM architecture mainframes at the NASA Automated Data Processing (ADP) Consolidation Center (NACC), located at Marshall Space Flight Center (MSFC). Six centers moved their administrative system workloads to NACC in 1994 and 1995. Four centers moved their administrative workloads to an interim NACC-managed facility at Lewis Research Center (LeRC) in 1996. NACC plans to relocate those workloads to MSFC by the end of FY 1997.

The Information Systems Services Office (ISSO) at MSFC has primary responsibility for overseeing the operations of the NACC. Within the ISSO, the NACC Project Office has overall responsibility for managing the effort.

NACC is primarily responsible for computer operations, systems reliability, systems software, configuration management, and strategic planning. Each Center is responsible for application development and maintenance, database administration, and security administration for their respective systems. NACC has mirrored each Center's configuration into a logical partition (LPAR) on an IBM compatible processor. Separate copies of the operating system run in separate partitions on the same physical processor and each partition shares the processor's resources. This provides a great deal of flexibility in dividing processor power and allocating storage between partitions. While each partition is dependent on the integrity of the common hardware, each operating system is independent of failures in other partitions.

A primary goal of consolidation is to achieve cost savings and efficiencies by converting hardware and software licenses to enterprise licensing structures. Centers are converting to a standard suite of software products to eliminate redundant software and decrease software maintenance costs. NACC plans to consolidate individual Center partitions into common user partitions.

THIS PAGE INTENTIONALLY LEFT BLANK

Observations and Recommendations

General Evaluation

The NACC Project Office has done a highly commendable job of establishing and operating a consolidated facility. They devote a significant amount of effort to achieving and maintaining a well-controlled environment. This report provides recommendations we believe will help improve NACC management controls. These recommendations address issues in the areas of physical security, environmental security, technical standards, security administration, change management, and tape management. Our audit objectives, scope, and methodology are discussed in Appendix 1 of this report. Applicable criteria associated with our recommendations are identified in Appendix 2.

Strengthen Facility Access Controls

NACC does not have a procedure in place to periodically conduct reviews and document the status of individuals granted physical access to the computing facility. While NACC management indicated that past reviews have been conducted, they do not have a formal procedure requiring periodic reviews. It is important to require reviews, since failure to periodically review the status of facility access authority could allow employees who no longer need the access to retain access authority.

A magnetic key-card reader system controls access to the NACC facility. The MSFC Security Office administers the system, including adding and deleting authorized users. The MSFC Information Systems Services Office authorizes certain individuals to grant and remove card access for data center contractor and facilities support personnel. The MSFC Security Office grants and removes access for personnel such as fire fighters, police, and security guards.

NACC management stated that access reviews were conducted in mid-1995 and mid-1996. However, they do not have periodic access review procedures. Also, the prior reviews were not documented. These periodic reviews would determine whether only those who need NACC facility access have it and the access control system is updated in a timely manner to reflect terminations, transfers, or changes in job functions.

RECOMMENDATION 1

The Director, ISSO, should establish a procedure to periodically review key-card access privileges to NACC facilities. The review should include all individuals with access and should determine whether:

- individuals have a justifiable need for access at the time of the review;
- the system is being updated to reflect changes to access privileges in a timely manner; and
- the employee check-out process is being conducted properly for terminations, including the surrendering of key-cards.

Management's Response

Concur. The NACC has developed a procedure, that will become effective October 1, 1997, requiring an annual review of the total list of personnel that have been granted key-card access to the NACC facility. ISSO will coordinate this activity with the MSFC Security Office to ensure only appropriate personnel have access privileges. The Security Office is responsible for the Marshall Access Control System (MACS) which monitors all the controlled access areas at the Center. Security Office personnel are in the process of conducting a Center-wide verification of all controlled access areas, including all the NACC facilities, and are approximately 80% complete. Individuals determined to no longer require access, will be promptly removed.

Based on this information, we consider this recommendation closed upon issuance of the final report.

Evaluation of Management's Response

The actions taken satisfy the intent of the recommendation.

RECOMMENDATION 2

The Director, ISSO should ensure that the periodic review of key-card access privileges to NACC facilities is documented.

Management's Response

Concur. The procedure requires that the results of the annual review be documented.

Based on this action, we consider this recommendation to be closed upon issuance of the final report.

Evaluation of Management's Response

The actions taken satisfy the intent of the recommendation.

DEVELOP STRATEGY FOR IMPLEMENTATION OF TECHNICAL STANDARDS

Data centers establish naming standards to provide consistency in identifying meaningful information about a resource. In the case of data set (file) names, information such as who owns it, its contents, and why it exists are usually important. Data centers typically encode the identity of the owner in the data set name. For example, data sets belonging to the Accounts Receivable department may begin with "AR" or some other notation that is meaningful to users. Another part of the name might serve to describe why it exists, such as "P" for production or "T" for test data sets. Specific naming standards must be developed based on both the data center's and the user's particular needs.

Although naming standards requirements for data sets and account codes exist in the NACC environment, there is no strategy for implementing them across all user systems. This situation exists because centers moved 15 unique workloads with their own standards to the NACC. Lack of standard data set names will inhibit the NACC's ability to consolidate center partitions into general use partitions. Lack of standard account codes will inhibit the NACC's ability to track resource utilization and costs in a general use environment.

A NACC inter-center working group has been established to propose standards and implementation strategies, and to evaluate customer impacts of implementing technical standards. The group found that there was no consistent standard across NACC systems for data set names and account codes.

The working group recognizes that the lack of data set naming standards is a problem that inhibits consolidating Center applications into fewer partitions. Examples of potential problems in a consolidated environment without good data set naming standards include the inability to identify center-specific applications, and the existence of duplicate names, which the operating system will not allow.

Lack of standard account codes will inhibit NACC's ability to track resource utilization and resulting costs below the operating system level. Thus, the NACC might not be able to meet any future full costing requirements or to recover costs through chargeback to users.

The working group has developed standards for data set names and account codes. However, a strategy to implement them has not been developed, primarily because the impact on resources at the centers has not been determined. Centers may be losing the support necessary to accomplish such an effort.

RECOMMENDATION 3

The Director, ISSO, should evaluate the potential payback from standardizing data set names and account codes, and develop a strategy to address the problems that will be encountered due to a lack of standards. The impact of available resources, full cost accounting, legacy systems (replacement of systems resulting from the Integrated Financial Management Project or moved to a client/server platform), and reducing the number of logical partitions should be considered.

Management's Response

Concur. The NACC has been tasked by the Agency Chief Information Office (CIO) to develop a Strategic Plan, which is currently being developed. As a part of that plan, the NACC will provide guidelines and strategies by which the current operation can continue to reduce costs. The NACC will recommend that established standards be put in place in general use environments so that resources and staffing can be provided for fewer system images. The Strategic Plan will recommend that data sets and accounting be standardized so that further consolidation, in addition to the system rehosting that has already been completed, can be accomplished. The NACC Strategic Plan is being developed by ISSO for review by MSFC Center Management, Code M, and the NASA CIO Council. It is scheduled for completion during the first quarter of Fiscal Year 98.

Based on this action, we consider this recommendation closed upon issuance of the final report.

Evaluation of Management's Response

The actions to be taken satisfy the intent of the recommendation.

Establish Reviews of Security Implications for Product Installations

Each software product used at the NACC may have security implications that must be considered during the product installation or upgrade process. Because the NACC installs the products and security administration functions reside at each center, security ramifications associated with product installations may not be known to center security administrators. Lack of knowledge on the part of center security administrators about potential security issues associated with a product could lead to inadequate protection of a NACC system.

In the NACC environment, centers handle logical security administration. NACC systems programmers located at MSFC install and maintain commercial-off-the-shelf (COTS) system software products within each center's operating environment. The installation of a new product or upgrade could have potential security ramifications that center security administrators may be unaware of since they do not receive vendor documentation unless they request it, and NACC does not perform formal security impact assessments for new product installs and upgrades.

Examples of security issues associated with a new install or upgrade include:

- the inclusion of vendor-supplied user IDs and passwords that come with some COTS products. Vendors document these user IDs and passwords in their product documentation. Failure by an installation to properly restrict access to them through logical security protection could result in unauthorized system access;
- high-risk utility programs that require restricted access control; and

- programs that have the potential for modifying the operating system.

There is currently no procedure for users to request and the NACC to conduct full security impact assessments.

RECOMMENDATION 4

The Director, ISSO, should institute procedures to make security impact assessments available to centers prior to installing each new product and upgrade.

Management's Response

Concur. Change Management Procedure OPM-311 was modified and will become effective October 1, 1997, to include the NACC Security Coordinator as impact evaluator on all Change Requests (CR). The INFOMAN software used to control changes to NACC hardware/software was also modified to include the NACC Security Coordinator as an impact evaluator on all CRs. An activity record is generated for each CR and an Email is sent to the Security Coordinator informing that person of a new request. The Security Coordinator will be responsible for completing COTS product security impact assessments and providing them to the Center Security Administrators for review. The CR for the product install cannot be closed without the closure of this activity record by the Security Coordinator.

Based on this action, we consider this recommendation closed upon issuance of the final report.

Evaluation of Management's Response

The actions taken satisfy the intent of the recommendation.

STRENGTHEN CHANGE MANAGEMENT PROCESS

The NACC Disaster Recovery Coordinator is not an evaluator in the 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.

NACC operating procedures exist for submitting and processing change requests. The procedures establish responsibilities for requesting, recording, and implementing changes to the NACC's baseline hardware and software configuration. They provide a methodology for assessing the risks associated with the implementation of software, hardware, network, facility, and environmental changes to the NACC. As part of the process, various personnel evaluate the impact of changes and ensure that formal documentation exists.

The NACC Disaster Recovery Plan, dated January 1997, created a Disaster Recovery Coordinator position, with responsibility for maintaining the Plan. It recognizes the need for the Coordinator to be involved in change management. Currently, the Coordinator is not designated as a participant in the review of changes. Lack of involvement in the process could result in failure to keep NACC disaster recovery plans current. Outdated plans could negatively impact disaster recovery testing and capability.

RECOMMENDATION 5

The Director, ISSO, should formally include the NACC Disaster Recovery Coordinator in the change management process.

Management's Response

Concur. Change Management Procedure OPM-311 was modified and will become effective October 1, 1997, to include the Disaster Recovery Coordinator (DRC) as impact evaluator on all Change Requests. The INFOMAN software used to control changes to NACC hardware/software was modified to include the DRC as an impact evaluator on all CRs. An activity record is generated for each CR and an Email is sent to the DRC informing that person of a new request. The CR cannot be closed without the closure of this activity record by the DRC.

Evaluation of Management's Response

The actions taken satisfy the intent of the recommendation.

PERIODICALLY INVENTORY TAPE ASSETS

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

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

While the NACC tape library is physically secured within the facility, it is located in an open area that allows access by anyone who has access to the NACC facility. This increases the risk that tapes can be accidentally or deliberately misplaced or removed from the tape library. An inventory of tape cartridges was performed for each NACC workload as part of consolidation, but management has not implemented subsequent inventories as a formal procedure.

RECOMMENDATION 6

The Director, ISSO, should institute a procedure requiring periodic physical inventories of tape assets at the NACC facility and at the offsite backup facility. Due to the large number of tapes managed, the cost of conducting a total inventory may not be justified. Inventories could be conducted using a sampling plan by individuals independent of the tape management function.

Management's Response

Concur. To ensure integrity and quality data transmission, NACC Operations personnel implemented a formalized procedure for performing a full tape library inventory that will become effective October 1, 1997. The procedure states that at least three logical operating partitions and one silo will be inventoried on a quarterly basis. A listing of all active tape ranges from each computer system will be provided to non-tape management Operations personnel to begin the inventory. A full audit will also be performed on the NACC StorageTek 4400 automated cartridge systems. This audit is performed on low tape activity days in the silo. Also, during this inventory a random selection of tapes from each logical operating environment will be TAPEMAPPED to ensure that the internal header of the tape matches the header defined in the Tape Management Catalog.

Based on this action, we consider this recommendation closed upon issuance of the final report.

Evaluation of Management's Response

The actions taken satisfy the intent of the recommendation.

Install Door on Tape Backup Storage Room

The NACC has not installed a door to restrict access to the tape backup storage room at the offsite backup facility. This increases the chance of tapes becoming accidentally or intentionally misplaced.

The NACC stores its tape backups, including disaster recovery tapes, in a storage room located at a contractor-leased facility near MSFC. As part of our audit, we conducted a site inspection of the storage room. We observed that the room does not have a door to control access to it. The room is adjacent to the work areas assigned to various contractor personnel who do not have tape management responsibilities.

Recommendation 7

The Director, ISSO, should ensure that a locked, fire-rated door restricts access to the room housing tape backups.

Management's Response

Concur. Management has identified space in the basement of Building 4201 at MSFC to house tape backups. The two rooms which have been identified are in the process of being vacated. The tape backups will be located in two separate rooms for which access is controlled by key card. The relocation of the tape backups should be completed in the first quarter of Fiscal Year 1998.

Based on this action, we consider this recommendation closed upon issuance of the final report.

Evaluation of Management's Response

The actions to be taken satisfy the intent of the recommendation.

Perform Independent Security Monitoring

The NACC does not perform independent security monitoring in one NACC-managed partition where systems programmers also have security administration responsibilities. These dual job responsibilities exist primarily due to a lack of resources. As a result, security administrators could grant themselves accesses not needed to perform their jobs as systems programmers.

In order to support NACC accounting and chargeback, configuration management, and other general use software, the NACC has established a separate partition known as the "Common" system (NACOMN). No user applications exist in this partition. The NACC has total responsibility for the system, including security administration. The Access Control Facility/2 (ACF2) is the product used to implement security for the common system environment.

During our review, we noted that individuals assigned ACF2 responsibilities for this partition also have systems programming responsibilities. These individuals have powerful ACF2 privileges to administer security. These privileges allow them to create or change rules governing access to system data, programs, and other resources within their scope of authority. Management said it would not be cost-effective to employ an independent ACF2 administrator solely for this system.

While we agree with their position, the risk exists that security administrators could grant access not needed to perform their jobs as systems programmers. We believe a reasonable control is a periodic review of these privileges to ensure proper use.

RECOMMENDATION 8

The Director, ISSO, should institute a procedure to periodically and independently review the privileges and activities of those personnel with dual security administration and systems programming responsibilities. The periodic review should include an evaluation of the ACF2 rules authorized to those individuals, a review of any accesses not authorized by ACF2 rules, and the possible use of ACF2 capabilities to restrict the scope of authority that they have.

Management's Response

Concur. The NACC is implementing an Operating Procedure that details methods and mechanisms for controlling and maintenance of access security for the NACOMN, NAPROD, and JSCIN-A logical operating environments. The procedure will be effective October 1, 1997. The NACC is the central point of contact for controlling USERID's for these systems. The procedure details the process for reviewing access reports for violations and monthly audit reports for individuals with dual security and systems responsibilities. These daily and monthly reports will be reviewed by the NACC Security Coordinator, independently of systems programmers. Impact assessments will be conducted by NACC management personnel to determine if violations are a breach of security. All violations will be reported to the NASA Security Office and maintained in an incident log, along with the formal written determination. Periodic review of the ACF2 hierarchy will also be conducted by the NACC Security Coordinator.

Based on this action, we consider this recommendation closed upon issuance of the final report.

Evaluation of Management's Response

The actions to be taken satisfy the intent of the recommendation.

Conduct More Frequent Environmental Protection Reviews

The MSFC Facilities Office has identified two fire protection problems within the NACC facility. These include an existing condition and a problem caused by ongoing utility work in the facility. These conditions put the facility at risk because they could serve as conduits for fire.

The MSFC Facilities Office manages building projects associated with the NACC facility, including ensuring compliance with all current building codes. In addition, the Facilities Office conducts inspections when a major modification is made to the building structure. In response to our questions about fire protection, the Facilities Office conducted a review of the NACC facility. Overall, conditions were acceptable, with the following two exceptions:

- several holes resulting from utility penetrations were found in the walls; and
- an interior wall did not extend to the floor structure above.

The utility penetration holes were not sealed properly with a fire stopping material. The interior wall existed prior to the creation of the NACC. The Facilities Office was unable to determine if there were other problems with walls above the ceiling due to limited access or interference with utilities. In response to these findings, they issued a work request to have the wall penetration problems corrected. They have also written a task order to have an engineering firm prepare a study to determine if there are other building code problems.

RECOMMENDATION 9

The Director, ISSO, should request that more periodic reviews by the Facilities Office be conducted due to ongoing construction activities at the NACC that may not meet the definition of a major building modification.

Management's Response

Concur. A Form 199 MSFC Facility Work Request (FWR) was implemented on June 14, 1997, to resolve the penetration of the walls in the NACC computer room. All identified holes were filled as specified on the FWR.

A Task Order (TO) was issued by the Facilities Office on March 14, 1997, to examine whether there are any other building code issues that need to be addressed. The TO was assigned to the Center's facilities engineering contractor, AJT. No assigned date has been announced by AJT for completion of the TO. NACC will continue to monitor this issue until the study is performed.

The NACC is responsible for updating the NACC Risk Assessment, including risks due to facility construction. When the Risk Assessment is updated, either as scheduled or as a result of major workload or processing changes, ISSO will coordinate the results of its reviews and cost/benefit analyses, of identified facility risks, with the MSFC Facilities Office. Also, the NACC will request that the Facilities Office conduct a yearly review of the NACC facility, comparable to that which was done to address audit concerns.

Based on this action, we consider this recommendation closed upon issuance of the final report.

Evaluation of Management's Response

The actions taken satisfy the intent of the recommendation.

OBJECTIVES

The objective of the audit was to determine whether NACC management has established an adequate internal control structure 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 was limited to the NACC facility at MSFC. As part of the audit, we reviewed NACC facilities and operating procedures, and interviewed several MSFC and contractor employees. We did not review and are not expressing an opinion on the management, security, or integrity of individual Center partitions.

MANAGEMENT CONTROLS REVIEWED

We evaluated general management controls over activities that are the responsibility of the NACC, 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 May 1997 at MSFC and NASA Headquarters. We conducted the audit in accordance with generally accepted government auditing standards.

THIS PAGE INTENTIONALLY LEFT BLANK

Audit Criteria . . . . *Appendix 2*

OMB Circular A-123, Management Accountability and C, requires that management controls provide reasonable assurance that assets are safeguarded against loss or unauthorized use.

This Circular applies to audit recommendations 1, 3, 4, 5, 6, 7, and 9

OMB Circular A-130, Management of Federal Information Resources, requires that controls be established to assure adequate security for all information processed, transmitted, or stored in Federal automated information systems.

This Circular applies to audit recommendations 1, 4, 5, 7, and 8.

OPM-309, Operating Procedure For NASA Automated Data Processing Consolidation Center Security, requires that entry to data processing facilities be restricted to those who have a specific need for access.

This operating procedure applies to audit recommendations 1, 2 and 7.

THIS PAGE INTENTIONALLY LEFT BLANK

MANAGEMENT'S RESPONSE .... *APPENDIX 3*

National Aeronautics and
Space Administration
George C. Marshall Space Flight Center
Marshall Space Flight Center, AL 35812

Reply to Attn of: DE01

SEP 09 1997

TO: Office of Inspector General
Attn: W/Robert J. Wesolowski

FROM: DE01/Susan McGuire Smith

SUBJECT: OIG Discussion Draft Report on Audit of NASA Data Center Facility - MSFC, Assignment No. A-HA-97-024

We have reviewed the subject report, and our detailed comments are enclosed. We agree with the overall evaluation that the NACC Project Office has done a highly commendable job of establishing and operating the consolidated facility. We also concur with the report's recommendations for improving management controls.

If you have any questions or need additional information regarding our comments, please contact BE01/Danny Walker at (205) 544-0100.

Susan McGuire Smith

Susan McGuire Smith
Associate Director

Enclosure

MSFC RESPONSE TO OIG DISCUSSION DRAFT REPORT ON NASA DATA CENTER FACILITY - MSFC, ASSIGNMENT NUMBER A-HA-97-024

Our comments and responses to the report recommendations are presented below.

RECOMMENDATION 1:

The Director, ISSO, should establish a procedure to periodically review key-card access privileges to NACC facilities. The review should include all individuals with access and should determine whether:

- individuals have a justifiable need for access at the time of the review,
- the system is being updated to reflect changes to access privileges in a timely manner, and
- the employee check-out process is being conducted properly for terminations, including the surrendering of key-cards

MSFC RESPONSE:

Concur. The NACC has developed a procedure, that will become effective October 1, 1997, requiring an annual review of the total list of personnel that have been granted key-card access to the NACC facility. ISSO will coordinate this activity with the MSFC Security Office to ensure only appropriate personnel have access privileges. The Security Office is responsible for the Marshall Access Control System (MACS) which monitors all the controlled access areas at the Center. Security Office personnel are in the process of conducting a Center-wide verification of all controlled access areas, including all the NACC facilities, and are approximately 80% complete. Individuals determined to no longer require access, will be promptly removed.

Based on this information, we consider this recommendation closed upon issuance of the final report.

RECOMMENDATION 2:

The Director, ISSO should ensure that the periodic review of key-card access privileges to NACC facilities is documented.

MSFC RESPONSE:

Concur. The procedure requires that the results of the annual review be documented.

Based on this action, we consider this recommendation to be closed upon issuance of the final report.

RECOMMENDATION 3:

The Director, ISSO should evaluate the potential payback from standardizing data set names and account codes, and develop a strategy to address the problems that will be encountered due to a lack of standards. The impact of available resources, full cost accounting, legacy systems (replacement of systems resulting from the Integrated Financial Management Project or moved to a client/server platform), and reducing the number of logical partitions should be considered.

MSFC RESPONSE:

Concur. The NACC has been tasked by the Agency Chief Information Office (CIO) to develop a Strategic Plan, which is currently being developed. As a part of that plan, the NACC will provide guidelines and strategies by which the current operation can continue to reduce costs. The NACC will recommend that established standards be put in place in general use environments so that resources and staffing can be provided for fewer system images. The Strategic Plan will recommend that data sets and accounting be standardized so that further consolidation, in addition to the system rehosting that has already been completed, can be accomplished. The NACC Strategic Plan is being developed by ISSO for review by MSFC Center Management, Code M, and the NASA CIO Council. It is scheduled for completion during the first quarter of Fiscal Year 98.

Based on this action, we consider this recommendation closed upon issuance of the final report.

RECOMMENDATION 4:

The Director, ISSO should institute procedures to make security impact assessments available to Centers prior to installing each new product and upgrade.

MSFC RESPONSE:

Concur. Change Management Procedure OPM-311 was modified and will become effective October 1, 1997, to include the NACC Security Coordinator as impact evaluator on all Change Requests (CR). The INFOMAN software used to control changes to NACC hardware/software was also modified to include the NACC Security Coordinator as an impact evaluator on all CRs. An activity record is generated for each CR and an Email is sent to the Security Coordinator informing that person of a new request. The Security Coordinator will be responsible for completing COTS product security impact assessments and providing them to the Center Security Administrators for review. The CR for the product install cannot be closed without the closure of this activity record by the Security Coordinator.

Based on this action, we consider this recommendation closed upon issuance of the final report.

RECOMMENDATION 5:

The Director, ISSO should formally include the NACC Disaster Recovery Coordinator in the change management process.

MSFC RESPONSE:

Concur. Change Management Procedure OPM-311 was modified and will become effective October 1, 1997, to include the Disaster Recovery Coordinator (DRC) as impact evaluator on all Change Requests. The INFOMAN software used to control changes to NACC hardware/software was modified to include the DRC as an impact evaluator on all CRs. An activity record is generated for each CR and an Email is sent to the DRC informing that person of a new request. The CR cannot be closed without the closure of this activity record by the DRC.

Based on this action, we consider this recommendation closed upon issuance of the final report.

RECOMMENDATION 6:

The Director, ISSO should institute a procedure requiring periodic physical inventories of tape assets at the NACC facility and at the offsite backup facility. Due to the large number of tapes managed, the cost of conducting a total inventory may not be justified. Inventories could be conducted using a sampling plan by individuals independent of the tape management function.

MSFC RESPONSE:

Concur. To ensure integrity and quality data transmission, NACC Operations personnel implemented a formalized procedure for performing a full tape library inventory that will become effective October 1, 1997. The procedure states that at least three logical operating partitions and one silo will be inventoried on a quarterly basis. A listing of all active tape ranges from each computer system will be provided to non-tape management Operations personnel to begin the inventory. A full audit will also be performed on the NACC StorageTek 4400 automated cartridge systems. This audit is performed on low tape activity days in the silo. Also, during this inventory a random selection of tapes from each logical operating environment will be TAPEMAPPED to ensure that the internal header of the tape matches the header defined in the Tape Management Catalog.

Based on this action, we consider this recommendation closed upon issuance of the final report.

RECOMMENDATION 7:

The Director, ISSO should ensure that a locked, fire-rated door restricts access to the room housing tape backups.

MSFC RESPONSE:

Concur. Management has identified space in the basement of Building 4201 at MSFC to house tape backups. The two rooms which have been identified are in the process of being vacated. The tape backups will be located in two separate rooms for which access is controlled by key card. The relocation of the tape backups should be completed in the first quarter of Fiscal Year 1998.

Based on this action, we consider this recommendation closed upon issuance of the final report.

RECOMMENDATION 8:

The Director, ISSO should institute a procedure to periodically and independently review the privileges and activities of those personnel with dual security administration and systems programming responsibilities. The periodic review should include an evaluation of the ACF2 rules authorized to those individuals, a review of any accesses not authorized by ACF2 rules, and the possible use of ACF2 capabilities to restrict the scope of authority that they have.

MSFC RESPONSE:

Concur. The NACC is implementing an Operating Procedure that details methods and mechanisms for controlling and maintenance of access security for the NACOMN, NAPROD, and JSCIN-A logical operating environments. The procedure will be effective October 1, 1997. The NACC is the central point of contact for controlling USERID's for these systems. The procedure details the process for reviewing access reports for violations and monthly audit reports for individuals with dual security and systems responsibilities. These daily and monthly reports will be reviewed by the NACC Security Coordinator, independently of systems programmers. Impact assessments will be conducted by NACC management personnel to determine if violations are a breach of security. All violations will be reported to the NASA Security Office and maintained in an incident log, along with the formal written determination. Periodic review of the ACF2 hierarchy will also be conducted by the NACC Security Coordinator.

Based on this action, we consider this recommendation closed upon issuance of the final report.

RECOMMENDATION 9:

The Director, ISSO should request that more periodic reviews by the Facilities Office be conducted due to ongoing construction activities at the NACC that may not meet the definition of a major building modification.

MSFC RESPONSE:

Concur. A Form 199 MSFC Facility Work Request (FWR) was implemented on June 14, 1997, to resolve the penetration of the walls in the NACC computer room. All identified holes were filled as specified on the FWR.

A Task Order (TO) was issued by the Facilities Office on March 14, 1997, to examine whether there are any other building code issues that need to be addressed. The TO was assigned to the Center's facilities engineering contractor, AJT. No assigned date has been announced by AJT for completion of the TO. NACC will continue to monitor this issue until the study is performed.

The NACC is responsible for updating the NACC Risk Assessment, including risks due to facility construction. When the Risk Assessment is updated, either as scheduled or as a result of major workload or processing changes, ISSO will coordinate the results of its reviews and cost/benefit analyses, of identified facility risks, with the MSFC Facilities Office. Also, the NACC will request that the Facilities Office conduct a yearly review of the NACC facility, comparable to that which was done to address audit concerns.

Based on this action, we consider this recommendation closed upon issuance of the final report.

THIS PAGE INTENTIONALLY LEFT BLANK

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 M/Associate Administrator
Code M/Chief Information Officer Representative

NASA Field Installations

Chief Information Officer, Marshall Space Flight Center
Chief Financial Officer, Marshall Space Flight Center
Director, Ames Research Center
Director, Dryden Flight Research Facility
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
Dryden Flight 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 of each of the following 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

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

Congressional Members

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

MAJOR CONTRIBUTORS TO THE REPORT

Brent Melson - Program Director, Information Technology Audits
Mindy Vuong - Information Technology Auditor, Kennedy Space Center