IG-98-005

# AUDIT REPORT

## NASA DATA CENTER GENERAL CONTROLS
## JOHNSON SPACE CENTER

**January 29, 1998**

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.

## ACRONYMS

| | |
|---|---|
| FEIDS | Flight Equipment Interface Devices |
| JSC | Johnson Space Center |
| KSC | Kennedy Space Center |
| MSFC | Marshall Space Flight Center |
| NASA | National Aeronautics and Space Administration |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| PCZ | Physical Control Zone |
| SPF | Software Production Facility |
| STS | Space Transportation System |
| UPS | Uninterruptable Power Source |
| USA | United Space Alliance |

# TABLE OF CONTENTS

# DATA CENTER GENERAL CONTROLS

## BACKGROUND

Johnson Space Center (JSC) has several large computer facilities supporting various mission operations. These facilities are:

- Software Production Facility (SPF)
- Shuttle Avionics and Integration Laboratory
- Shuttle Mission Training Facility
- Integrated Planning System
- Mission Control Center

We limited our audit to the SPF data center. United Space Alliance (USA) operates and manages the facility under the Space Flight Operations Contract, NAS9-20000. USA is a joint venture of Boeing Aerospace and Lockheed Martin Corporation. We selected the facility because it plays a major role in the preparation of space flights for the Space Shuttle Program.

The SPF assimilates the unique hardware and software configuration requirements for each Space Transportation System (STS) flight. The SPF staff develops and customizes orbiter flight software for each specific space shuttle mission. After exhaustive verification, SPF transmits this software to the Kennedy Space Center (KSC) for loading onboard the space shuttle. The facility also generates mission-specific products and reconfigures ground based software to support specific flight profiles and payloads. The entire National Aeronautics and Space Administration (NASA) STS program, as well as KSC, Marshall Space Flight Center (MSFC), Boeing Aerospace North America, and JSC, utilizes the SPF for data collection, review, and approval.

The SPF facility consists of two Hosts, Automated Operations, Flight Equipment Interface Devices (FEIDS) and a Harris Night Hawk Firewall. The Hosts consist of two International Business Machines plug-compatible Amdahl Central Processing Units and associated standard peripheral devices. Custom built automation computer hardware operates the mainframes 7 days-a-week, 24 hours-a-day. The FEIDS, custom built computer hardware, check flight software for proper execution.  The firewall monitors and controls traffic between the network and the subnets.  Interactive and/or batch file transfer is authorized to and from any authorized SPF user on a connected network.  Authorized interactive SPF users are Boeing Aerospace North America, Loral, JSC, KSC, MSFC, and USA.

## OBSERVATIONS AND RECOMMENDATIONS

### *OVERALL EVALUATION*

SPF's physical and environmental protection and comprehensive operating procedures are adequate. USA has done a highly commendable job of operating the SPF facility. Dedicated data center personnel provide their users with baseline flight data, reconfiguration software tools, and a management control structure that should provide for a reliable computing environment. This report provides recommendations we believe will help improve SPF management controls. These recommendations address issues in the areas of security and environmental control. 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 PHYSICAL ACCESS CONTROLS TO THE SPF*

JSC Security provides a comprehensive security program supporting NASA and JSC resources and programs, including the protection of personnel, information, equipment, operations and facilities. Their physical security program includes controlling site entry and access to critical facilities and resources. Written procedures exist for contractors to notify JSC Security when employees are terminated or otherwise have their access revoked. Written procedures also exist to ensure that the physical access control system, known as the Central Security Control System, is updated in a timely manner. However, these procedures are not always being followed. As a result, individuals no longer needing SPF physical access may still have it.

Physical access to the SPF is granted to those individuals who have a valid business need. In a list dated January 18, 1997, the Central Security Control System identified 777 individuals with SPF access. We sampled 57 individuals to validate their need for physical access. Our sample identified 25 individuals who did not need physical access but remained on the physical access list. Of the 25, 20 were not current employees. Five were current employees but no longer needed physical access.

The procedures state NASA contractors should notify JSC Security in writing when individuals terminate or otherwise have their access revoked. According to a JSC Physical Security Specialist, the contractors are not always notifying JSC in a timely manner.

However, in one instance noted in our testing, a contractor notified JSC Security of several individuals that no longer needed SPF physical access. These individuals remained on the physical access list. The JSC Physical Security Specialist could not determine why the individuals where not removed from the list.

Without following the procedures in place, the SPF is susceptible to physical access by individuals who no longer require it to perform their jobs. This increases the possibility of losses from intentional or accidental damage, destruction, or theft of equipment and data.

***RECOMMENDATION 1***

The Chief, Security Branch, Center Operations Directorate, should enforce existing operating procedures to ensure that contractors provide timely written information regarding terminations/revocations of employees with physical access to the SPF facility.

***Management's Response***

As stated in the report, procedures are in place to ensure that only individuals requiring access to the Software Production Facility (SPF) be allowed to enter. Contractors are obligated to notify JSC Security when an employee terminates. The access lists are reviewed periodically, and if a person has not used his or her card to gain access to a controlled area within the past six months, that person’s access privileges are deleted. The Designated Approving Officials for each of the controlled areas also perform an annual review and recertification of all personnel with access privileges. This requirement is found in the JSC Security Manual, Section 8.1.8 which states: ‟…Contractor personnel having a local personnel or security office surrender their badge to the respective authorized company representative before termination. The badge is then returned to the Security Division with written notification of the individual employee’s termination. All other persons possessing a badge return it to their JSC sponsor or directly to Security.” Paragraph 11.5.2 states: ‟…The badge office must be notified immediately when an employee with PCZ access terminates. When so notified, the individual’s access to all PCZ will be deleted.”

There is currently no requirement in the JSC Security Manual to require a contractor to notify JSC Security when a change in a work assignment results in the loss of the employee’s need for access. We recognized the need for this, and the JSC Security Division has been working with JSC procurement officials to develop standard contract clauses requiring contractors to provide notification to JSC Security when an employee’s need for access to controlled areas changes. A

Data Requirements Description (DRD) titled, "Security Reporting Requirements,” was drafted by the JSC Industrial Security Specialist and submitted to procurement in July 1997.

The DRD requires, among other things: "Provide the following information...d. - Change in a cleared employee’s status and/or an employee participating in special access programs such as the Mission Critical Space Systems Personnel Reliability Program (PRP), NASA Resource Protection (NRP) Program, and Information Technology (IT/AIS) Security Program (i.e., name, marital status, citizenship, death, termination of employment or clearance, different position or work assignment/relocation, employee becomes a representative of a foreign interest, etc.)”

This clause was added to Lockheed Martin Contract NAS9-19100 on August 1, 1997, as modification #69. The clause is now undergoing legal and procurement review and approval to become a standard clause in all JSC contracts.

All Security personnel will be reminded to adhere to the procedures. With procedures in place and actions underway to strengthen those procedures, and your acceptance of those actions, we will consider this recommendation closed on issuance of the final report.

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

We have reviewed the information related to recommendation 1 and management's response to the recommendation. We feel management's actions are responsive to our concern. As a result, we consider this recommendation closed.

## *RECOMMENDATION 2*

The Chief, Security Branch, Center Operations Directorate, should enforce existing operating procedures to ensure all terminations/revocations are immediately entered into the Central Security Control System.

***Management's Response***

All Security Division personnel will be reminded to adhere to the existing procedures. The JSC Security Manual states in Chapter 11.5.2 Terminations: "When an individual terminates Government or contractor employment, he/she is responsible for turning in his/her PCZ card. NASA employees will not be allowed to clear the site until their PCZ cards have been returned to the Security Division. For contractor or other Government agency employees, a corporate security officer or responsible agency official will retrieve the PCZ card at the same time the JSC badge is retrieved. …The badge office must be notified immediately when an employee with PCZ access terminates. When so notified, the individual’s access to all PCZ’s will be deleted. If the employee has been terminated for cause, he/she must be denied PCZ access at the same time he/she is notified of termination. This will be done by notifying the Security Division of the termination before notifying the employee. The building 1 security receptionist will furnish the building 30 badge office a monthly list of expired visit requests, which will be checked against the PCZ master access list. Any person whose clearance expired will no longer be allowed PCZ access.”

Detailed procedures on how to complete terminations in the Central Security Control System (CSCS) are found in the Mission Control Center Procedures and Training Manual, section 12, which is located in the Building 30 Badge Office, room 1100. All Security personnel will be reminded to immediately enter data into the Central Security Control System.

With these procedures in place and reminders to employees to follow them, we will consider this recommendation closed on issuance of the final report.

### *Evaluation of Management's Response*

We have reviewed the information related to recommendation 2 and management's response to the recommendation. We feel management's action is responsive to our concern. As a result, we consider this recommendation closed.

## *EVALUATE NEED FOR PROTECTION FROM POWER OUTAGES*

An Uninterruptable Power Source (UPS) forms a defense strategy against power problems. A UPS is a power conditioning and supply system. It provides protection against short-term power outages until the user can start a backup generator or shut down the computer and network systems safely. It also provides for cleaner power which may help reduce computer maintenance needs. The SPF is not protected with a UPS. USA does not believe a UPS is required or cost-justified. However, a feasibility study or a cost/benefit analysis has not been conducted. Without a UPS, the SPF is vulnerable to data loss during a commercial power outage. USA believes the current commercial power source, Houston Lighting and Power, is reliable because the SPF has never been down for long periods due to a power outage. In our opinion, a UPS is a generally accepted protection system. A UPS prevents information loss, reduces interruption, and provides reasonable continuity of computer services should adverse events occur that would prevent normal operations. We believe a UPS feasibility study and cost/benefit analysis should be conducted.

***RECOMMENDATION 3***

The Space Shuttle Program Office should conduct a feasibility study and a cost/benefit analysis for a UPS.

***Management's Response***

The Software Production Facility is a vital Shuttle resource and we agree with the finding and intent of the recommendation. The USA will perform a feasibility study and cost/benefit analysis to include a summary of any power related SPF changes through the report date. This will be completed by March 30, 1998.

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

The action to be taken by USA is responsive to our concern. We will review the contractor's feasibility study and cost/benefit analysis and, therefore, request to be included in the concurrence cycle for closure of the recommendation.

# OBJECTIVES, SCOPE, AND METHODOLOGY

### *OBJECTIVES*

The objective of the audit is to determine whether an adequate internal control structure has been established to provide for a reliable Software Production Facility (SPF) computing environment, including:

- physical and environmental protection, and
- comprehensive operating procedures.

### *SCOPE AND METHODOLOGY*

We interviewed Johnson Space Center (JSC) civil service and United Space Alliance (USA) contractor personnel to understand the general SPF controls and procedures. We reviewed JSC and USA SPF standards, policies and procedures. We toured the SPF facility and reviewed records to evaluate physical security and environmental conditions. We sampled physical access and authorized computer users lists to evaluate security controls.

### *MANAGEMENT CONROLS REVIEWED*

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

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

### *AUDIT FIELD WORK*

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

# RELEVANT POLICIES

***SECTION 4.17.3 OF JSC CENTRAL SECURITY CONTROL SYSTEM OPERATING PROCEDURES, REVISION B***

states when the Building 30 Security Badging Office is informed that an individual no longer has authorized Physical Control Zone (PCZ) access, the receptionist will immediately delete all access from the system and retrieve, if possible, the PCZ badge. This operating policy applies to Recommendations 1 and 2.

***SECTION 8.1.8 OF JSCM 1600D, JSC SECURITY MANUAL***

states the NASA or JSC badge is returned to the Security Division when it is no longer needed... Contractor personnel having a local personnel or security office surrender their badge to the respective authorized company representative before termination. The badge is then returned to the Security Division with written notification of the individual employee's termination. This operating policy applies to Recommendations 1 and 2.

***SECTION 11.5.2 OF JSCM 1600D, JSC SECURITY MANUAL***

states when an individual terminates Government or contractor employment, he/she is responsible for turning in his/her PCZ card... For contractor or other Government agency employees, a corporate security officer or responsible agency official will retrieve the PCZ card at the same time the JSC badge is retrieved. The PCZ card will be protected and either delivered to the Building 30 Security Badging Office or mailed to the Security Division as soon as possible. The badge office must be notified immediately when an employee with PCZ access terminates. When so notified, the individual's access to all PCZ's will be deleted. This operating policy applies to Recommendations 1 and 2.

***APPENDIX III, SECTION A.3 OF OFFICE OF MANAGEMENT AND BUDGET (OMB) CIRCULAR A-130***

states agencies shall implement and maintain a program to assure adequate security is provided for all agency information collected, processed, transmitted, stored or disseminated in general support systems and major applications. Among other things, application security plans shall provide for establishing and periodically testing the capability to perform the agency function supported by the application in the event of failure of its automated support. This operation policy applies to Recommendation 3.

### *Section 302(f) of NASA Handbook 2410.9A*

states appropriate disaster recovery plans and contingency plans must be established and maintained to prevent loss of information, minimize interruption, and provide reasonable continuity of computer and network services should adverse events occur that would prevent normal operations.  This operations policy applies to Recommendation 3.

### *GOOD BUSINESS PRACTICES*

The OMB and NASA Handbook criteria do not specifically address an Uninterruptable Power Source (UPS) as part of adequate contingency planning.  However, good business practices would dictate an undesirable condition exists when a UPS does not protect a critical system, such as the SPF.  This practice applies to Recommendation 3.

## REPORT DISTRIBUTION LIST

### National Aeronautics and Space Administration (NASA) Officials-In-Charge

Code A/Office of the Administrator
Code AD/Deputy Administrator
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 M/Associate Administrator for Space Flight
Code MC/CIO Representative
Code MX/Audit Liaison

### NASA Director, Field Installations

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

### NASA Offices of Inspector General

Ames Research Center
Goddard Space Flight Center
Jet Propulsion Laboratory
John F. Kennedy Space Center
Langley Research Center
Lewis Research Center
George C. Marshall Space Flight Center
John C. Stennis Space Center

## Johnson Space Center Officials

Code AI/Chief Information Officer
Code AI/JSC Computer Security Official
Code BD/Audit Liaison Representative
Code DA/Director, Mission Operations Directorate
Code DB/Chief, Systems Development and Operations Division
Code DB/ SPF Resident Office Manager
Code JA/Director, Center Operations Directorate
Code MA/Manager, Space Shuttle Program

## Chairman and ranking minority member of each of the following 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

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

## Congressional Members:

Honorable Pete Sessions, U.S. House of Representatives

## MAJOR CONTRIBUTORS TO THE REPORT

| | |
|---|---|
| ***JOHNSON SPACE CENTER*** | Brenda K. Conley, Auditor-in-Charge |
| ***NASA HEADQUARTERS*** | Gregory B. Melson, Program Director - Information Technology Audits |