

**AUDIT  
REPORT**

---

**UNIX OPERATING SYSTEM SECURITY AND  
INTEGRITY [WITHHELD PER EXEMPTION  
(B)(5)] AT  
GODDARD SPACE FLIGHT CENTER**

**March 29, 2000**

---

**[Withheld per exemption (b)(5)]**



National Aeronautics and  
Space Administration

**OFFICE OF INSPECTOR GENERAL**

## **Additional Copies**

To obtain additional copies of this report, contact the Assistant Inspector General for Auditing at (202) 358-1232, or visit [www.hq.nasa.gov/office/oig/hq/issuedaudits.html](http://www.hq.nasa.gov/office/oig/hq/issuedaudits.html).

## **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, Room 8V69  
300 E Street, SW  
Washington, DC 20546-0001

## **NASA Hotline**

To report fraud, waste, abuse, or mismanagement, contact the NASA OIG Hotline at (800) 424-9183, (800) 535-8134 (TDD), or at [www.hq.nasa.gov/office/oig/hq/hotline.html#form](http://www.hq.nasa.gov/office/oig/hq/hotline.html#form); or write to 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.

Please complete the reader survey at the end of this report or at <http://www.hq.nasa.gov/office/oig/hq/audits.html>.

---

## **Acronyms**

[withheld per exemption (b)(5)]

ID Identification

IT Information Technology

[withheld per exemption (b)(5)]

NPG NASA Procedures and Guidelines

OMB Office of Management and Budget

W

March 29, 2000

TO: A/Administrator

FROM: W/Inspector General

SUBJECT: INFORMATION: UNIX Operating System Security and Integrity  
Report Number IG-00-024

The NASA Office of Inspector General has completed an audit of Unix Operating System Security and Integrity [withheld per exemption (b)(5)] at Goddard Space Flight Center. We found that the [withheld per exemption (b)(5)] did not have an adequate information technology (IT) security program. [withheld per exemption (b)(5)]

### **Background**

NASA uses the UNIX<sup>1</sup> operating system<sup>2</sup> in a variety of major, [withheld per exemption (b)(5)] computing environments. One of NASA's major information systems that uses UNIX is the [withheld per exemption (b)(5)] at Goddard Space Flight Center. [withheld per exemption (b)(5)]

### **Recommendations**

We recommended that the Director, Goddard Space Flight Center (1) improve personnel screening, the process for granting access to computer systems, [withheld per exemption (b)(5)], and protection of critical system files; (2) establish policies for privileged operations and system backups; and (3) implement proactive security monitoring.

### **Management Response and OIG Evaluation**

Goddard management agreed that it is important to implement proper controls to reasonably assure system, program, and data security and integrity. However, Goddard has classified the [withheld per exemption (b)(5)] as a [withheld per exemption (b)(5)] information system. The Center has not yet completed its reassessment of whether certain [withheld per exemption (b)(5)] should be classified as [withheld per exemption (b)(5)] information

---

<sup>1</sup> A powerful and complex operating system (further described in Appendix B).

<sup>2</sup> Software that manages the basic operations of a computer system (see Appendix B).

systems which imposes a significant amount of additional security controls above those currently required.

Based on our interpretation of NASA Procedures and Guidelines (NPG) 2810.1, "Security of Information Technology," all [withheld per exemption (b)(5)] should be classified as [withheld per exemption (b)(5)] information systems. The NPG was issued 7 months ago, yet Goddard has not made a final decision on how to classify some of the [withheld per exemption (b)(5)].

Even if we had applied the security criteria for [withheld per exemption (b)(5)] systems in performing our audit of the security controls currently implemented, the systems would not have met most of those criteria. While Goddard has agreed to at least full implementation of security for the [withheld per exemption (b)(5)] at least at the level required for [withheld per exemption (b)(5)] systems, we still request Goddard to provide a specific response to each recommendation. A summary of the status of all the recommendations is in the Executive Summary of the report.

**[original signed by]**

Roberta L. Gross

Enclosure

Final Report on Audit of Unix Operating System Security  
and Integrity [withheld per exemption (b)(5)]  
at Goddard Space Flight Center

[withheld per exemption (b)(5)]

**FINAL REPORT**  
**UNIX OPERATING SYSTEM SECURITY AND INTEGRITY [withheld per  
exemption (b)(5)] AT GODDARD SPACE FLIGHT CENTER**

**[withheld per exemption (b)(5)]**

W

March 29, 2000

TO: Y/Associate Administrator for Earth Science  
Code 100/Director, Goddard Space Flight Center

FROM: W/Assistant Inspector General for Auditing

SUBJECT: Final Report on the Audit of Unix Operating System Security and Integrity  
[withheld per exemption (b)(5)] at Goddard Space Flight Center  
Assignment Number A9904000  
Report Number IG-00-024

The subject final report is provided for your use and comment. Please refer to the Executive Summary for the overall audit results. Our evaluation of your response is incorporated into the body of the report. Management provided an interim response and stated that they would provide more specific information later. We request that management provide by April 28, 2000, the specific corrective actions planned, ongoing, and completed or an estimated completion date. Also, please notify us when action has been completed on the recommendations, including the extent of testing performed to ensure corrective actions are effective. All recommendations will remain open for reporting purposes.

If you have questions concerning the report, please contact Mr. Gregory B. Melson, Program Director for Information Assurance Audits, at (202) 358-2588; Mr. Ernest L. Willard, Audit Program Manager, at (650) 604-2676; or Mr. James W. Geith, Auditor-in-Charge, at (301) 286-7943. We appreciate the courtesies extended to the audit staff. The final report distribution is in Appendix E.

**[original signed by]**

Russell A. Rau

Enclosure

cc:

AO/Chief Information Officer

**[withheld per exemption (b)(5)]**

## ***Contents***

**Executive Summary, i**

**Introduction, 1**

**Findings and Recommendations, 2**

Finding A., [withheld per exemption (b)(5)] 2

Finding B. [withheld per exemption (b)(5)] Security Controls, 5

Finding C. Protection of Critical Log, 6

Finding D. Privileged Operations, 8

Finding E. System Security Monitoring, 9

Finding F. System Backup, 11

**Appendix A - Objectives, Scope, and Methodology, 13**

**Appendix B - Glossary, 15**

**Appendix C - Federal Guidance Related to Information Technology  
Security, 16**

**Appendix D - Management's Response, Error! Bookmark not defined.**

**Appendix E - Report Distribution, 22**

# NASA Office of Inspector General

IG-00-024  
A9904000

March 29, 2000

## UNIX Operating System Security and Integrity [withheld per exemption (b)(5)] at Goddard Space Flight Center

### Executive Summary

**Background.** NASA uses the UNIX<sup>3</sup> operating system<sup>4</sup> in a variety of [withheld per exemption (b)(5)] computing environments. One of NASA's [withheld per exemption (b)(5)] information systems that uses UNIX is the [withheld per exemption (b)(5)] at Goddard Space Flight Center (Goddard). [withheld per exemption (b)(5)]<sup>5</sup>

**Objectives.** The overall objective was to determine whether the [withheld per exemption (b)(5)] at Goddard has implemented controls at the host computer level to provide reasonable assurance of system, program, and data security and integrity. We reviewed the adequacy of basic controls (physical security; system backups; system startup; default accounts; systems administration; account security, and system security monitoring) for 2 [withheld per exemption (b)(5)] UNIX host<sup>6</sup> computers in the [withheld per exemption (b)(5)]. Details of our objective, scope, and methodology are in Appendix A.

Appendix B contains a glossary of terms used in this report.

**Results of Audit.** The [withheld per exemption (b)(5)] did not have an adequate information technology (IT) security program. Specifically, Goddard management did not assign sufficient priority to IT security. Our detailed findings follow:

- [withheld per exemption (b)(5)]
- [withheld per exemption (b)(5)]
- [withheld per exemption (b)(5)]<sup>7</sup>
- [withheld per exemption (b)(5)]

---

<sup>3</sup> A powerful and complex operating system (further described in Appendix B).

<sup>4</sup> Software that manages the basic operations of a computer system (see Appendix B).

<sup>5</sup> [withheld per exemption (b)(5)]

<sup>6</sup> A computer network interconnects many computer processors called hosts, each of which is capable of supplying computing services to network users. Each host computer contains an operating system that supports applications processes (see Appendix B).

<sup>7</sup> [withheld per exemption (b)(5)]



- Proactive security monitoring and reviewing were not being accomplished for the [withheld per exemption (b)(5)] (Finding E). [withheld per exemption (b)(5)]
- System backup policies were inadequate, increasing the possibility that backup copies would be unusable or unavailable when needed (Finding F).

Unauthorized access to the [withheld per exemption (b)(5)] computers by a user who has other than superuser privileges could result in loss of [withheld per exemption (b)(5)] support and the loss of [withheld per exemption (b)(5)] some data. Unauthorized access with superuser privileges would give the user complete control of the computer system and could result in catastrophic loss of services.

Goddard personnel took prompt corrective action on a number of these deficiencies.

**Recommendations.** Goddard management should improve personnel screening, the process for granting access to computer systems, [withheld per exemption (b)(5)], and protection of critical system files; establish policies for privileged operations and system backups; and implement proactive security monitoring.

**Management's Response.** Although management fully concurred in principle with the importance of implementing and maintaining proper security controls, management did not provide planned corrective actions for each recommendation. Also, Goddard has not yet made its reassessment of whether certain [withheld per exemption (b)(5)] centers, [withheld per exemption (b)(5)] should be classified as [withheld per exemption (b)(5)] information systems or as [withheld per exemption (b)(5)] information systems.

**Evaluation of Response.** We consider all recommendations unresolved and open. In response to the final report, we request additional comments that specify planned corrective actions.

## **Introduction**

NASA stores [withheld per exemption (b)(5)] information as both data and programs on many UNIX-based computers in data centers and user-controlled areas. Because NASA used UNIX in [withheld per exemption (b)(5)] computing environments, it must be subject to IT security requirements to ensure that data and programs are protected from unauthorized or accidental modification, damage, destruction, or disclosure. UNIX is an extraordinarily complex operating system. Many vendors have developed their own versions of the UNIX operating system and hardware. [withheld per exemption (b)(5)]

[paragraph withheld per exemption (b)(5)]

The [withheld per exemption (b)(5)] perform the system administration responsibilities for the [withheld per exemption (b)(5)] computer systems. (The terms [withheld per exemption (b)(5)] and system administrators are interchangeable for the purposes of this report.)

UNIX systems are favorite targets of hackers. Without adequate UNIX security controls, the [withheld per exemption (b)(5)] IT systems could be compromised by an unauthorized source.

## Findings and Recommendations

---

### **Finding A.** [withheld per exemption (b)(5)]

[paragraph withheld per exemption (b)(5)]

#### **Federal and NASA Policies and Procedures on Personnel Screening**

Office of Management and Budget (OMB) Circular No. A-130, "Management of Federal Information Resources," February 8, 1996, requires that individuals who are authorized to bypass significant technical and operational security controls of a system must be screened both before being authorized to bypass controls and periodically thereafter.

NASA Procedures and Guidelines (NPG) 1620.1, " Security Procedures and Guidelines," November 18, 1999, requires a National Agency Check<sup>8</sup> for civil service and contractor personnel who require access to IT systems that process sensitive information.

NPG 2810.1, "Security of Information Technology," August 26, 1999, requires that individuals who are authorized to bypass significant technical and operational security controls of a system must be screened before being granted access.

#### **Federal and NASA Policies and Procedures on Access Authorization**

OMB Circular A-130 and NPG 2810.1, require that individuals be granted the minimum privileges necessary to accomplish their tasks.

NPG 2810.1 requires that system administrators grant accounts only to individuals who have had the appropriate personnel screening. The NPG also requires that system administrators receive an Account Request Document approved by a Government management official responsible for the individual before the system administrators grant the individual access to a computer system. The Account Request Document must contain a statement indicating that the requestor acknowledges an understanding of and intention to comply with a statement concerning user responsibilities, possible monitoring of their computer use, and that failure to abide by the provisions may constitute grounds for administrative action and/or civil or criminal prosecution. (See Appendix C for further details on Federal and NASA IT security requirements.)

#### **Access Authorization**

Before a system administrator can give someone an account on an information system that processes sensitive information, three things must occur.

---

<sup>8</sup> See Appendix C, under Personnel Screening, for a description of a National Agency Check.

- First, the Center must conduct a personnel screening to determine whether the individual is eligible to be issued an account. The level of screening that is required depends on which access privileges the individual needs to perform his or her job and the nature of the information that the individual uses.
- Second, an Account Request Document must be prepared. The document includes: identification information for the requester; the requester's citizenship; the system or group of systems for which an account is being requested, the level of user privileges afforded to the account, the requester's signature, and the date the requester acknowledges an understanding of and intention to comply with the rules and conditions associated with having an account.
- Third, a Government management official or a Government designee responsible for the individual must approve the request.

### **Personnel Screening**

Goddard had not performed the National Agency Checks required by NPG 1620.1 on 16 of the 20 contractor personnel who have access to [withheld per exemption (b)(5)] computer systems, including one system administrator for the [withheld per exemption (b)(5)]. System administrators have the authority to bypass significant technical and operational security controls of a system. The other personnel had access to sensitive information [withheld per exemption (b)(5)]. The screenings were not performed because Goddard's policy was to not perform personnel screenings solely for granting access to IT systems. This policy did not comply with Federal and NASA policy.

The failure to conduct personnel screenings degraded the information technology security environment and increased the possibility of unauthorized access and misuse of Government resources and information that could result in the loss of [withheld per exemption (b)(5)].

### **Access Authorization Procedures**

[paragraph withheld per exemption (b)(5)]

[withheld per exemption (b)(5)] The General Accounting Office also identified that NASA was not providing required security training in an audit report titled "Information Security, Many NASA Mission Critical-Systems Face Serious Risks," Report Number GAO/AIM-99-47, dated May 1999. [withheld per exemption (b)(5)]

[withheld per exemption (b)(5)]<sup>9</sup>

### **Acknowledgement of User Responsibilities**

---

<sup>9</sup> [withheld per exemption (b)(5)]

Users were not required to sign a statement acknowledging their security responsibilities or that that their use of Government computer systems was subject to monitoring and that unauthorized use could result in administrative action and/or civil or criminal prosecution. Although the statement is required by NPG 2810.1, the [withheld per exemption (b)(5)] contractor had not established procedures for authorizing access to the [withheld per exemption (b)(5)] computer systems.

The failure to have users sign an acknowledgment of their responsibilities degraded information technology security. The failure to have users acknowledge the fact that their use of Government systems is subject to monitoring can impede the investigation of unauthorized use of computer systems and reduce the Government's ability to prosecute misuse in the civil and criminal courts.

Shortly after we notified them during the audit, the system administrators started correcting these problems by establishing account access procedures. All [withheld per exemption (b)(5)] personnel have now signed Account Request Forms acknowledging: (1) their responsibilities, (2) that their use of Government computer systems is subject to monitoring, and (3) that unauthorized use can result in administrative action and/or civil or criminal prosecution.

## **Recommendations, Management's Response, and Evaluation of Response**

**The Director, Goddard Space Flight Center, should:**

- 1. Direct the Center Chief of Security to change the Goddard policy on performing personnel screenings to comply with Federal and NASA directives.**
- 2. Direct the Center Chief of Security, Center Information Technology Security Manager, and the [withheld per exemption (b)(5)] to take immediate action to perform the required personnel screenings.**
- 3. [withheld per exemption (b)(5)]**

**Management's Response.** Management concurred with the importance of implementing proper controls, but did not provide specific comments on the recommendations. The complete text of management's response in Appendix D.

**Evaluation of Management's Response.** We request that the Director, Goddard Space Flight Center, provide additional comments on the recommendations including specific planned actions.

**Finding B.** [withheld per exemption (b)(5)] **Security Controls**

[section withheld per exemption (b)(5)]<sup>1011</sup>

---

<sup>10</sup> [withheld per exemption (b)(5)]

<sup>11</sup> [withheld per exemption (b)(5)]

## **Finding C. Protection of Critical Log**

The [withheld per exemption (b)(5)] system administrators did not save to a secure secondary location an automated log, which is critical to monitoring unauthorized access. This condition existed because system administrators believed the system was secure and that protecting the log entries was not necessary. [withheld per exemption (b)(5)]

### **Agency Policy Related to Audit Trails**

NPG 2810.1 requires, as part of the minimum IT security requirements, that NASA systems provide “. . . audit trails or a journal of security-relevant events” (see Appendix C). The NPG defines an audit trail as a chronological record of computer activities and states that an audit trail “. . . should be sufficient to enable the reconstruction and examination of a sequence of events, environments, activities, procedures, or operations from inception to final result.” The NPG requires that these journals for mission information systems be kept for 12 months.

### **One Audit Trail**

[section withheld per exemption (b)(5)].

## **Recommendation, Management's Response, and Evaluation of Response**

7. [withheld per exemption (b)(5)].

**Management's Response.** Management did not provide specific comments on this recommendation (see Appendix D).

**Evaluation of Management's Response.** We request that management provide additional comments on this recommendation that specify planned corrective actions.



## **Finding D. Privileged Operations**

[section withheld per exemption (b)(5)]<sup>12</sup>

---

<sup>12</sup> [withheld per exemption (b)(5)]

## **Finding E. System Security Monitoring**

[paragraph withheld per exemption (b)(5)]

### **NASA Policies and Procedures**

For [withheld per exemption (b)(5)] systems, NPG 2810.1 requires that management implement a process that accomplishes the following:

- Ensures the system journal records security-related events.
- Reviews journals daily or when problems are suspected.
- Records successful and failed logons and logoffs.
- Records all successful and failed file openings and closings.
- Records all file creation/modification/deletion events.
- Ensures that journals identify programs being executed, users, source device files, and the time, date, and success or failure of all access attempts.

Additionally, the NPG requires that each system “. . . have a System Administrator who will ensure that the protective security measures of the system are functional and who will maintain its security posture.” The system administrator’s responsibilities include:

- Using IT security tools to assist in detecting modifications to the system and monitoring audit logs.
- Ensuring that security controls are in place and functioning.

### **Logging and Review of System Activity**

[withheld per exemption (b)(5)]<sup>13</sup>

Tools such as UNIX accounting utilities and third-party software are available to assist and enhance security monitoring. [withheld per exemption (b)(5)]

### **Recommendation, Management's Response, and Evaluation of Response**

---

<sup>13</sup> [withheld per exemption (b)(5)]

**9. The Director, Goddard Space Flight Center, should direct the [withheld per exemption (b)(5)] to record and review system events as required by NPG 2810.1.**

**Management's Response.** Management did not provide specific comments on this recommendation (Appendix D).

**Evaluation of Management's Response.** We request that the Director, Goddard Space Flight Center, provide specific planned actions on the recommendation in response to the final report.

## **Finding F. System Backup**

The system administrators had not developed management-approved policies covering backups of the operating systems, applications, and other information on the [withheld per exemption (b)(5)] host computers. This occurred because Goddard management had not complied with Agency IT security policies. As a result, restoration of the operating system from the backup copies may take longer than necessary. Further, it may not be possible to restore an uncompromised version of the operating system from the backup copies, if the system is compromised.

### **NASA Policy Regarding System Backup**

NPG 2810.1 requires that management implement a process for systems that:

- Retains journals<sup>14</sup> at least 1 year.
- Backs up the operating systems at least monthly and when modified.
- Retains operating system backups for at least 1 year.
- Stores in an external location the most recent backup copies or backup copies made immediately before the most recent.

### **Backup Operations**

Daily and weekly backups of the [withheld per exemption (b)(5)] host computers were being made to hard drives on other computers in the [withheld per exemption (b)(5)]. Monthly backups of one of the two host computers that we reviewed were being made to tapes that were stored in the [withheld per exemption (b)(5)]. However, there was only one backup copy. The system administrators used the same set of tapes each month. As a result, the system journals and backup copies were not retained for at least 1 year as required.

Because there was only a single copy of the backup tapes, there was no off-site storage of a backup copy of the operating system and journals. However, the [withheld per exemption (b)(5)] had a copy of the operating system and application software that the system administrators could use to rebuild the computer systems.

The [withheld per exemption (b)(5)] contractor had no policies for testing the backups to ensure they are useable. Having backup copies is not sufficient to ensure that a system can be restored if necessary. Backup copies must be tested periodically to determine they are actually useable.

---

<sup>14</sup> The journals contain the security-related events and other events described in Finding E.

These conditions existed because Goddard management had not given adequate priority to IT security and had not ensured that the [withheld per exemption (b)(5)] developed and implemented policies for system backup that comply with Agency policy.

### **Potential Impact**

The lack of adequate backup copies of the operating system could delay restoration of the [withheld per exemption (b)(5)] systems in the event of an emergency that made the [withheld per exemption (b)(5)] unusable. If computer hackers compromise the operating systems, the lack of a series of backups makes it more difficult to restore a version of the operating system that has not been compromised and to investigate the compromise.

As a result of our audit, the [withheld per exemption (b)(5)] system administrators implemented a weekly backup on the [withheld per exemption (b)(5)] computers. This process provides off-site storage for a backup copy of the system software. In addition, the system administrators created formal procedures for backup operations including semiannual testing of the data.

### **Recommendation, Management's Response, and Evaluation of Response**

**10. The Director, Goddard Space Flight Center, should direct the [withheld per exemption (b)(5)] to develop and implement adequate policies for backups of the [withheld per exemption (b)(5)] operating systems.**

**Management's Response.** Management did not provide specific comments on this recommendation (see Appendix D).

**Evaluation of Management's Response.** We request that the Director, Goddard Space Flight Center, provide specific planned actions on the recommendation in response to the final report.

## Appendix A. Objectives, Scope, and Methodology

---

### Objectives

The overall objective was to determine whether the [withheld per exemption (b)(5)] at Goddard has implemented controls at the host computer level to provide reasonable assurance of system, program, and data security and integrity. We reviewed selected UNIX hosts in the [withheld per exemption (b)(5)] for basic controls (physical security, system backups, system startup, default accounts, systems administration, account security, and audit and monitoring).

### Scope and Methodology

We performed work at Goddard by reviewing 2 [withheld per exemption (b)(5)] UNIX host computers, [withheld per exemption (b)(5)]. We selected these computers because they supported information systems that Goddard had designated as [withheld per exemption (b)(5)]. During the audit field work, we reviewed the following:

- General Accounting Office reports related to NASA IT Security.
- Federal and NASA directives (listed in Appendix C) governing the management and use of information systems.
- Goddard policies and procedures applicable to the [withheld per exemption (b)(5)].
- Physical access security for the hosts.
- [withheld per exemption (b)(5)] policies, procedures, and practices for system backup.
- System startup and shutdown procedures and permissions and contents of startup files.
- Default passwords to determine whether they had been changed.
- Responsibilities of system administrators.
- Security controls for user and root logons.
- Account security, including password security controls.
- System security monitoring functions.

We also:

- Interviewed Goddard civil service and [withheld per exemption (b)(5)] personnel to identify policies and procedures relating to UNIX security.
- Utilized various resources for reference information [withheld per exemption (b)(5)] for UNIX security guidelines.

Our audit procedures are not intended to address audit coverage of all potential security weaknesses, or to provide an opinion on the overall security of the [withheld per exemption (b)(5)] infrastructure. [withheld per exemption (b)(5)]

### **Management Controls Reviewed**

We reviewed Federal and NASA policies and procedures relating to [withheld per exemption (b)(5)] control and management to determine whether the policies and procedures for UNIX security were adequate. We identified the weaknesses discussed in the Findings section of the report.

### **Prior Audit Coverage**

The General Accounting Office issued an audit report titled "Information Security, Many NASA Mission Critical-Systems Face Serious Risks," Report Number GAO/AIM-99-47, May 1999.

### **Audit Field Work**

We performed field work from July 1999 through February 2000 at Goddard. We performed the audit in accordance with generally accepted government auditing standards.

## Appendix B. Glossary

---

**Console.** The combination of display monitor and keyboard (or other device that allows input). Another term for console is terminal. The term console usually refers to a terminal attached to a minicomputer or mainframe and used to monitor the status of the system.

**Host.** A computer network interconnects many computer processors called hosts; each is capable of supplying computing services to network users. Each host computer contains an operating system that supports applications processes.

**Log in.** The identification and authentication sequence that authorizes a user's access to a computer. Conversely, "log out" is the sequence that terminates user access to the system.

[Paragraph withheld per exemption (b)(5)]

**Operating System.** Software that manages the basic operations of a computer system. The software calculates how the computer main memory will be apportioned, how and in what order to handle tasks assigned to it, how to manage the flow of information into and out of the main processor, how to send material to the printer for printing and to the screen for viewing, how to receive information from the keyboard, etc. In short, the operating system handles the computer's basic housekeeping. MS-DOS, UNIX, and Windows NT are a few examples of operating systems.

**Superuser.** A user who is granted special privileges if the correct password is supplied when logging in. The user name for this account is normally "root." A user must be "root" to perform many system administration tasks, such as changing ownership and permissions for a file or directory that the user does not own.

**UNIX.** An immensely powerful and complex operating system. UNIX provides multi-tasking, multi-user capabilities that allow both multiple programs to be run simultaneously and multiple users to use a single computer. On a single-user system, such as MS-DOS, only one person at a time, on an individual task basis, can use a computer's files, programs, and other resources. UNIX works on many different computers. This means you can often take applications software that runs on UNIX and move it – with little changing – to a bigger, different computer or to a smaller computer. This process of moving programs to other computers is known as "porting." Today, the UNIX operating system is available on a wide range of hardware, from small personal computers to the most powerful mainframes, from a multitude of hardware and software vendors.

**User ID.** User identification. A unique character string used in a computer to identify a user.



## Appendix C. Federal Guidance Related to Information Technology Security

---

**OMB Circular No. A-130, "Management of Federal Information Resources."** Circular No. A-130 provides uniform Government-wide information resources management policies. Appendix III of the Circular establishes a minimum set of controls to be included in Federal automated information security programs.

**NPG 1620.1, "Security Procedures and Guidelines."** NPG 1620.1 "provides internal guidelines and procedures to assist NASA Centers in complying with the minimum standards, requirements, and specifications for the protection of personnel, sensitive unclassified/classified information, material, facilities, and resources in the possession of NASA, as well as the basic information regarding the assignment of management responsibilities."

**NPG 2810.1, "Security of Information Technology."** NPG 2810.1 cancels NASA Automated Information Security Handbook (NHB 2410.9A), dated June 1993, and became effective on August 26, 1999. NPG 2810.1

. . . describes the NASA IT Security Program, providing direction designed to ensure that safeguards for the protection of the integrity, availability, and confidentiality of IT resources (e.g., data, information, applications, and systems) are integrated into and support the missions of NASA. . . . NASA's IT Security Program is a set of policies, procedures, and guidance for ensuring the security of the Agency's IT resources.

Appendix A of NPG 2810.1, "Baseline IT Security Requirements," lists ". . . the minimum technical, procedural, and physical IT security requirements for protecting NASA's IT resources." Appendix A, Section A.6.1 of NPG 2810.1, "Operating System Integrity," ". . . describes the requirements for ensuring operating system integrity on NASA multi-user computers."

### Personnel Screening

OMB Circular No. A-130, Appendix III, paragraph A.3.a.(2).(c), requires screening for individuals who are authorized to bypass significant technical and operational security controls of a system commensurate with the risk and magnitude of harm they could cause. Such screening shall occur prior to an individual being authorized to bypass controls and periodically thereafter. Paragraph A.3.b.(2).(c), requires that

. . . controls such as separation of duties, least privilege and individual accountability be incorporated in major applications and application rules. . . . Least privilege is the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job.

## Appendix C

---

Where such controls ". . . cannot adequately protect the application or information in it, screen individuals commensurate with the risk and magnitude of the harm they could cause."

NPG 1620.1, paragraph 3.2.2, requires a National Agency Check for civil service and contractor personnel who require access to IT systems that process sensitive information in compliance with Appendix III of OMB Circular No. A-130. The National Agency Check consists of a review of:

- a. Investigative and criminal history files of the Federal Bureau of Investigation, including a technical fingerprint search;
- b. Office of Personnel Management Security/Suitability Investigations Index;
- c. Department of Defense's Defense Clearance and Investigations Index; and
- d. Such other national agencies (for example, Central Intelligence Agency, Immigration and Naturalization Service) as appropriate to the individual's background.

NPG 2810.1, paragraph 2.2.8.2.c, requires that system administrators grant accounts only to individuals who have had the appropriate personnel screening. Paragraph 4.5.1.2, states,

Some positions require special access privileges in order to do the assigned job or duties. These are "Public Trust" positions since they can affect the integrity, efficiency, or effectiveness of the system to which they have been granted privileged access. Screening for suitability, prior to being granted access, is required.

Paragraph 4.5.3.1.a, states, "Privileged access -- Can bypass, modify, or disable the technical and operational security controls."

[withheld per exemption (b)(5)]**Security**

[section withheld per exemption (b)(5)]

---

## Appendix C

### Individual Accountability and Controlled Access Protection

OMB Circular A-130, Appendix III, paragraph B.a.(c), states:

Individual accountability consists of holding someone responsible for his or her actions. In a general support system, accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them.

NPG 2810.1, paragraph A.6.4.3, "Controlled Access Protection," states:

Controlled access protection is the ability of the system to control the circumstances under which users have access to resources. Management will ensure that all systems that are accessed by more than one user will provide the following controlled access protection when those users do not have the same authorization to use all of the information on the system:

- Provides individual electronic accountability through identification and authentication of each system user.
- Provides audit trails or a journal of security-relevant events.

## **Security Monitoring**

NPG 2810.1, paragraph 2.2.8.1, states "Each system will have a System Administrator who will ensure that the protective security measures of the system are functional and who will maintain its security posture."

Paragraph 2.2.8.2 of NPG 2810.1 provides a list of security responsibilities. The responsibilities include:

- Periodically using tools to verify and/or monitor compliance to password guidelines.
- Using IT security tools to assist in detecting modifications to the system and monitoring audit logs.
- Ensuring that security controls are in place and functioning.

The [withheld per exemption (b)(5)] host computers have the ability to record (in journals) important system events. These journals can be used as an audit trail to investigate system or security problems. NPG 2810.1, Appendix A, paragraph A.6.1.3, states:

## Appendix C

---

Management will implement a process that accomplishes the following (for Mission Information systems):

- Ensures system journals record security-related events.
- Reviews journals daily or when problems are suspected.
- Records successful and failed logons/logoffs.
- Records all successful and failed file opens and closes.
- Records all file creation/modification/deletion events.
- Ensures journals identify programs being executed, users, source devices, files, and the time, date, and success or failure of all access attempts.

### System Backup

NPG 2810.1, Appendix A, paragraph A.6.1.4, states:

To ensure continuity of operation, copies of important software and data will be made and retained. NASA Internet server log files shall be processed according to the NASA records retention procedure. (See NPG 1441.1C, Records Retention Schedules, for retention requirements and procedures.) Management will implement a process that accomplishes the following (for Mission Information systems):

- Retains journals at least 1 year or 3 generations (whichever is longer)
- Backs up the operating systems and key system services at least monthly and when modified
- Retains operating system backups for at least 1 year
- Stores the most recent or most recent minus one backup external to the Center

## Appendix D. Management's Response

National Aeronautics and  
Space Administration  
**Goddard Space Flight Center**  
Greenbelt, MD 20771



Reply to Airtel of 201

**MAR 24 2000**

TO: NASA Headquarters  
Attn: W/Assistant Inspector General for Auditing

FROM: 100/Director

SUBJECT: Interim Response to Office of Inspector General (OIG) Draft Report on  
Audit of UNIX Operating System Security and Integrity [REDACTED]  
[REDACTED] at Goddard Space Flight Center  
(GSFC), Assignment A9904000, February 17, 2000

Thank you for providing us an assessment of the adequacy of the [REDACTED] information technology security program. GSFC agrees with the OIG concerning the importance of implementing and maintaining proper controls to reasonably assure system, program, and data security and integrity. The Center is committed to taking all appropriate actions in a timely manner toward that end.

The OIG audit brings additional focus to a major issue that the Center has been working and is in the process of resolving. The issue pertains to the need for the Center to assure that its information security systems are categorized appropriately within the revised NASA information system security guidelines. The revised NASA guidelines, NASA Procedures and Guidelines (NPG) 2810.1, "Security of Information Technology," were issued August 26, 1999, approximately 1 month after the OIG audit began in July 1999.

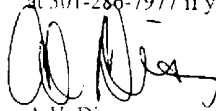
In the particular case of the [REDACTED], under the former security guidelines (June 1993 NASA Automated Information Security Handbook [NHB] 2410.9A), [REDACTED] was classified as a [REDACTED] operating under level 2 security requirements. When the new NPG was issued, the Center had to ensure that information systems were properly reclassified into one of five new information security categories. Management's mapping of the [REDACTED] original classification under the old NHB 2410.9A to the new NPG 2810.1 placed [REDACTED] within the new "Scientific, Engineering, and Research (SER)" information category. The OIG audit, however, audited the [REDACTED] information security procedures against the new "[REDACTED]" information category, which imposes a significant amount of additional security requirements above [REDACTED] original classification.

The Center is still in the process of reassessing whether certain [REDACTED] should be designated as [REDACTED] information systems or as [REDACTED] information systems. The Center is committed to making the appropriate information security system category determinations for [REDACTED] and other systems and to assure that the appropriate controls are in place as required by the designated category. Until the management reassessment is final, the Center will at least assure full implementation of security criteria to the [REDACTED] level for the [REDACTED]. If the Center elevates the [REDACTED] security category to [REDACTED], we will notify the OIG of implementation activities to assure full compliance at that level. We hope to complete our assessment and our response to you by June 15, 2000.

Key staff in the Goddard Chief Information Office, the Security Branch, and the [REDACTED] Program Office continue to work with your Auditor-in-Charge, Mr. James Geith, as part of this activity.

Thank you for recognizing in your draft report that Goddard personnel took prompt corrective actions on a number of issues identified during the audit. We will continue to work toward the proper closure of open actions to ensure the required level of security and integrity of our systems.

Due to the sensitivity of the information in the OIG draft report, we request that report distribution be limited. Please contact me or Ms. JoAnn Clark, GSFC Audit Liaison Officer, at 301-286-7977 if you need further information.



A.V. Diaz

Enclosure

cc:

HQ/AO/Mr. L. Holcomb  
HQ/HK/Mr. J. Horvath  
HQ/JM/Ms. M. Myles  
HQ/SD/Mr. M. Watkins  
HQ/Y/Dr. G. Asrar  
HQ/YB/Ms. D. Santa

## Appendix E. Report Distribution

---

### **National Aeronautics and Space Administration (NASA) Headquarters**

A/Administrator

AI/Associate Deputy Administrator

AO/Chief Information Officer

J/Associate Administrator for Management Systems

L/Associate Administrator for Legislative Affairs

Q/Associate Administrator for Safety and Mission Assurance

Y/Associate Administrator for Earth Science

### **NASA Center**

100/Director, Goddard Space Flight Center

## NASA Assistant Inspector General for Auditing Reader Survey

The NASA Office of Inspector General has a continuing interest in improving the usefulness of our reports. We wish to make our reports responsive to our customers' interests, consistent with our statutory responsibility. Could you help us by completing our reader survey? For your convenience, the questionnaire can be completed electronically through our homepage at <http://www.hq.nasa.gov/office/oig/hq/audits.html> or can be mailed to the Assistant Inspector General for Auditing; NASA Headquarters, Code W, Washington, DC 20546-0001.

**Report Title:** Unix Operating System Security and Integrity [withheld per exemption (b)(5)]  
at Goddard Space Flight Center

**Report Number:** \_\_\_\_\_ **Report Date:** \_\_\_\_\_

*Circle the appropriate rating for the following statements.*

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	N/A
1. The report was clear, readable, and logically organized.	5	4	3	2	1	N/A
2. The report was concise and to the point.	5	4	3	2	1	N/A
3. We effectively communicated the audit objectives, scope, and methodology.	5	4	3	2	1	N/A
4. The report contained sufficient information to support the finding(s) in a balanced and objective manner.	5	4	3	2	1	N/A

***Overall, how would you rate the report?***

Excellent	Fair
Very Good	Poor
Good	

***If you have any additional comments or wish to elaborate on any of the above responses, please write them here. Use additional paper if necessary.*** \_\_\_\_\_

---



---



---



---



---



**How did you use the report?** \_\_\_\_\_

---

---

---

---

---

---

---

---

**How could we improve our report?** \_\_\_\_\_

---

---

---

---

---

---

---

---

**How would you identify yourself? (Select one)**

Congressional Staff

Media

NASA Employee

Public Interest

Private Citizen

Other: \_\_\_\_\_

Government: \_\_\_\_\_ Federal: \_\_\_\_\_ State: \_\_\_\_\_ Local: \_\_\_\_\_

**May we contact you about your comments?**

**Yes:** \_\_\_\_\_

**No:** \_\_\_\_\_

**Name:** \_\_\_\_\_

**Telephone:** \_\_\_\_\_

Thank you for your cooperation in completing this survey.

## **Major Contributors to this Report**

Gregory B. Melson, Program Director for Information Assurance Audits

Ernest L. Willard, Audit Program Manager

James W. Geith, Auditor-in-Charge

Pat Reid, Program Assistant