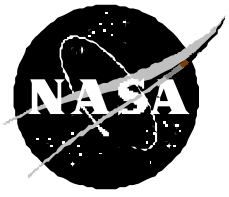
MAY 9, 2006

AUDIT REPORT

OFFICE OF AUDITS

NASA SHOULD IMPROVE EMPLOYEE AWARENESS OF REQUIREMENTS FOR IDENTIFYING AND HANDLING SENSITIVE BUT UNCLASSIFIED INFORMATION

OFFICE OF INSPECTOR GENERAL

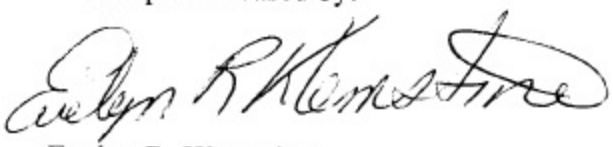


National Aeronautics and
Space Administration

REPORT NO. IG-06-010-REDACTED (ASSIGNMENT NO. A-04-013-00)

Note: This version of the report has been revised to omit NASA Information Technology/Internal Systems Data not routinely released under the Freedom of Information Act.

Final report released by:



Evelyn R. Klemstine
Assistant Inspector General for Auditing

Acronyms

FOIA	Freedom of Information Act
FRD	Federal Research Division
HQ	NASA Headquarters
IT	Information Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
OSPP	Office of Security and Program Protection
SBIR	Small Business Innovative Research
SBU	Sensitive But Unclassified
SETA	Security Education and Training, and Awareness

IN BRIEF

NASA SHOULD IMPROVE EMPLOYEE AWARENESS OF REQUIREMENTS FOR IDENTIFYING AND HANDLING SENSITIVE BUT UNCLASSIFIED INFORMATION

The Issue

The National Aeronautics and Space Act of 1958 (Space Act) requires NASA to "provide for the widest practicable and appropriate dissemination of information concerning its activities and the results thereof." This must be accomplished in a manner consistent with U.S. laws and regulations, Federal information policy, intellectual property rights, and technology transfer protection requirements. NASA faces many challenges in balancing its Space Act mandate with the requirements to protect certain classes of information that are not suitable for dissemination to the public. Crucial to the success of meeting those challenges is the need for NASA to (1) ensure that its policies and procedures for sensitive but unclassified (SBU)[1] information are complete and (2) create and maintain employee awareness of their responsibilities to safeguard SBU information.

Results

Overall, NASA's policies and procedures for handling SBU information are consistent with Federal laws and regulations. Prior to November 2005, the Agency's primary Security Program document did not cover all the types of SBU information that NASA uses, nor were SBU requirements in the Security Program document cross-referenced to other documents that contained additional requirements for specific types of SBU information. Revisions incorporated into the November 2005 version of NPR 1600.1, "NASA Security Program Procedural Requirements w/Change 1 (11/08/2005)," assuaged our concerns about the adequacy of the Agency's policies and procedures for SBU information. However, we found that NASA lacks a comprehensive SBU training program for civil servants and contractors on the requirements for protecting SBU information.

[1] Until November 2005, NASA used the term Administratively Controlled Information, or ACI, to identify official information of a sensitive but unclassified nature that needed to be protected against inappropriate disclosure. Such information officially became Sensitive But Unclassified on November 8, 2005, when NASA issued its revised NASA Procedural Requirements (NPR) 1600.1, "NASA Security Procedural Requirements w/Change 1."

Management Action

In November 2005, NASA revised the requirements for SBU information. Specifically, the new policies and procedures increased the number of SBU information types recognized by NASA and cross-referenced several types of SBU information to other documents that contained additional requirements. Although the new requirements emphasized the importance of establishing and maintaining an adequate level of education and awareness to safeguard and prevent unauthorized disclosure of SBU information, they did not detail a comprehensive SBU training program. Therefore, we are recommending that NASA establish an Agency-wide comprehensive training program that specifies the policies and procedures for identifying and handling SBU information.

In response to a draft of this report, the Assistant Administrator, OSPP, concurred with the recommendation and provided information on corrective actions planned (see Appendix D). We consider management's comments to be responsive and the recommendation resolved, although it will remain open until all actions have been completed and verified. No response to this final report is required.

Contents

INTRODUCTION

Background

NASA generates, receives, disseminates, and maintains an enormous amount of information, much of which is of an unclassified and nonsensitive nature with few restrictions on its use and dissemination. The security of this information is the direct, immediate, and inherent responsibility of all NASA personnel, contractors, and others granted access to it.

NASA must comply with several Federal laws and regulations that address disseminating information. These laws and regulations can be confusing, however, because their definitions of SBU information are not precise and some laws promote dissemination while other laws restrict or prohibit dissemination. For example, the Computer Security Act of 1987 defines sensitive information as any information for which the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled but has not been authorized to be kept secret. However, the Act does not specify the types of information that are included in sensitive information. Whereas the Computer Security Act requires protection of information such as personal and proprietary information from unauthorized disclosure, the Space Act promotes dissemination and requires the widest practicable and appropriate dissemination of information about NASA's activities.

Other laws restrict or prohibit dissemination of SBU information. For example, the Privacy Act prohibits dissemination of an individual's personal information without prior written consent of the individual. In addition, the Freedom of Information Act (FOIA) requires that agencies make information available to the public but exempts from disclosure internal personnel rules and practices, information specifically exempted by other statutes, trade secrets, personnel and medical files, and law enforcement records. The Homeland Security Act of 2002, which modifies FOIA, exempts from disclosure critical infrastructure information. Export control regulations restrict exportation of technical data relating to the Space Shuttle, satellites, and the International Space Station.

Objectives

The overall objective of our audit was to determine whether NASA established adequate controls that would protect SBU information. Specifically, we sought to determine whether NASA had (1) developed and issued policies and procedures that adequately define, identify, and protect all sensitive information with an emphasis on scientific and

technical sensitive information; (2) assigned accountability for the security of sensitive information; (3) established policies and procedures to properly screen sensitive information for possible inclusion in formal classification schemes;[2] and (4) established adequate policies and procedures for education and training to create user awareness of the need to recognize and properly safeguard sensitive information. See Appendix A for details of the audit's scope and methodology, our review of internal controls, and a list of prior coverage.

Meta-Data Report

As part of our review of NASA's policies and procedures to protect SBU information, we sampled NASA documents available on the Internet and found that they contained meta-data[3] that could be considered SBU information. In December 2005, we issued a report to the NASA Chief Information Officer and recommended that NASA (1) develop policies and procedures to define, recognize, and protect meta-data that may be contained in electronic documents, and (2) provide user awareness training on the meta-data policies and procedures developed pursuant to the preceding recommendation. See Appendix B for a copy of the report. [Appendix B has been redacted from this version.]

[2] During the course of the audit, we dropped objective 3 because it was beyond the scope of the planned work.

[3] Meta-data is data that describes other data. For information purposes, meta-data refers to the data generated when a Microsoft Word, Excel, or PowerPoint document is created or revised that describes how, when, and by whom a particular set of data was collected and how the data was formatted.

FINDING A: POLICIES AND PROCEDURES COVERING SBU INFORMATION

Although there are no Government-wide standards for defining what constitutes SBU information, NASA's policies and procedures are consistent with Federal laws and selected agencies' requirements for SBU information. The Agency has effectively assigned accountability for the security of sensitive information to OSPP. However, prior to November 2005, NASA's policies and procedures did not identify all the types of SBU information that NASA uses, and the various policies and procedures regulating security and management of SBU information Agency-wide were not cross-referenced to each other. On November 8, 2005, NASA revised its Agency Security Program, including the policies and procedures covering SBU information. The revisions assuaged our concerns about the adequacy of the Agency's policies and procedures for SBU information.

Federal Laws and Regulations and Selected Agencies' SBU Requirements

With the exception of certain types of information protected by statute, standard criteria and terminology defining the types of information warranting designation as SBU does not exist within the Federal government. To help us identify SBU-related laws, regulations, and other Federal agencies' directives that could apply to NASA, we contracted with the Federal Research Division (FRD) of the Library of Congress. FRD gave us a report that set forth the statutes, regulations, and Executive Branch directives that define and govern access to SBU information. We compared the SBU requirements identified in the FRD report with NASA's and found that the Agency has in place policies and procedures that are consistent with Federal laws and selected agencies' requirements. Appendix C shows the comparison.

Accountability for SBU Information

The Assistant Administrator for OSPP is responsible for overseeing Agency-wide implementation and integration of NPR 1600.1, "NASA Security Program Procedural Requirements w/Change 1," which establishes Agency-wide requirements for security program implementation. Further, the NPR designates that the Assistant Administrator for OSPP is to provide direction and oversight for an Agency-wide administrative security program that protects SBU information in NASA's custody. In addition to OSPP, the Office of the Chief Information Officer and other Headquarters offices also

have responsibility for specific types of SBU information. For example, export control information is considered SBU information, and NPR 2190.1, "NASA Export Control Program," designates the Assistant Administrator of the Office of External Relations as responsible for assessing and ensuring that all NASA programs, activities, and exports comply with U.S. export control laws and regulations.

Types of SBU Information NASA Uses

In its November 2005 revision of NPR 1600.1, the Agency provided extensive descriptions of the types of SBU information NASA uses. With no Government-wide standard criteria identifying SBU information and no terminology defining types of SBU information, each individual agency is left to designate the types of information it considers to be SBU information. Until November 2005, NASA had designated eight types of information as SBU in NPR 1600.1, but the list did not include all types of SBU information that NASA used. For example, it did not include

- source selection and bid and proposal information;
- Small Business Innovative Research (SBIR) data, limited-rights data, and Restricted computer software received in the performance of NASA contracts;
- information subject to the Privacy Act;
- systems security data revealing the security posture of a system; or
- information concerning or relating to private entity trade secrets or confidential commercial or financial information received by a NASA employee in the course of government employment or official duties.

The November 2005 revision not only listed all of these types of information as SBU, it further classified SBU information into three general categories:

- Information subject to FOIA: NASA designated as SBU any information originated within or furnished to NASA that falls under one or more of the exemption criteria of the Freedom of Information Act (5 U.S.C. §552).
- Information exempt or restricted from disclosure by statute, regulations, contract, or agreement: NASA provides eight examples of this category of SBU, such as, information subject to export control under International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR) and information disclosing a new invention in which the Federal Government owns or may own a right, title, or interest.

- Information that a designated NASA official determines to be unusually sensitive: NASA provides 13 examples of this category of SBU, such as sensitive scientific and technical information, and NASA information technology (IT) internal systems data revealing infrastructure used for servers, desktops, and networks.

With these changes, NASA has increased the types of SBU information described in NPR 1600.1 from 8 to 22.

Cross-Reference to Other Documents Containing Additional Requirements Related to SBU Information

Within NASA, management of SBU information is regulated through multiple Agency organizations and through multiple NASA regulations and directives. Although NPR 1600.1 is NASA's primary reference document for requirements covering SBU information, until November 2005, NPR 1600.1 did not cross-reference other Agency documents that contained additional SBU information requirements. The current NPR, however, notes that requirements for handling sensitive scientific and technical information are described in NASA Policy Directive (NPD) 2200.1, "Management of NASA Scientific and Technical Information (STI)," and NPR 2200.2, "Requirements for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information," and that requirements for disposing of IT systems that contain SBU information are described in NPR 2810.1, "Security of Information Technology." Further, NPR 1600.1 now notes that the requirements in NPR 2810.1, regarding the need to (1) certify and accredit IT systems that store SBU information and (2) store and control laptop computers and other media containing SBU information, must be met.

Corrective Action Taken

Revisions incorporated into the 2005 NPR 1600.1 adequately address the issues that we communicated to OSPP officials during our audit regarding (1) the incomplete listing of the types of SBU information that NASA uses and (2) the lack of cross-referencing to other documents that contain additional requirements for specific types of SBU information. Therefore, we are not making any recommendations in those areas.

FINDING B: COMPREHENSIVE SBU INFORMATION TRAINING IS NEEDED

While NASA expanded and clarified the Agency's requirements with regard to SBU information in November 2005, the Agency did not establish a comprehensive training program to educate civil servants and contractors about Agency requirements for identifying and handling SBU information. The November 2005 requirements state that the originators of information are required to identify it as SBU or not and protect it accordingly. Without a comprehensive training program, however, SBU information could be inadvertently disseminated, and that dissemination could result in harm to a person's privacy or welfare, have an adverse impact on economic or industrial institutions, or compromise programs or operations essential to safeguarding our national interests.

Federal Laws and NASA Requirements on SBU Information Training

Federal Laws. Two laws specifically require training for Federal employees and contractor personnel in securing SBU information. The first law, the Computer Security Act of 1987, requires that all persons—including contractors—involved in management, use, or operation of Federal computer systems that contain sensitive information receive periodic training in computer security awareness and accepted computer security practice. The second law, the Federal Information Security Management Act of 2002, requires that an agency's Chief Information Officer develop and maintain information security programs that include security awareness training to inform Federal personnel—including contractors—of information security risks associated with their activities as well as their responsibilities in complying with policies to reduce these risks.

In addition to the preceding Federal laws, the Federal Managers' Financial Integrity Act of 1982 (FMFIA) states that agencies must establish internal administrative controls in accordance with the standards prescribed by the Comptroller General, which are published in "Standards for Internal Control in the Federal Government" and set out management control standards for all aspects of an agency's operation. One of the standards of internal control— control activities—addresses appropriate policies, procedures, techniques, and mechanisms that should be in place to manage agency activities and identifies training is a necessary component of a good internal control program.

NASA Requirements. NPD 1600.2D, "NASA Security Policy," revalidated February 1, 2006, offers a generalized statement that NASA provides security and protection for, among other things, information. It further notes that securing and protecting is to be accomplished by methods including undertaking a security education and awareness program designed to solicit the support and involvement of all Agency personnel. Training offered by NASA falls into two categories:

- The Agency's annual IT security training, required at all Centers and NASA HQ, provides minimal details about SBU information. The training defines the term and reminds employees that SBU information, such as trade secrets, proprietary information, financial information, and personnel and medical records, must be properly marked and kept in a secured location when not under the supervision of an authorized person. However, the section devoted to SBU information lacks examples of proprietary information, fails to explain the types of financial information to consider as SBU, and does not address inventions, bid and proposal or source selection information, software, or SBIR data.

- NASA Centers' additional online security training includes guidance about managing SBU information. For example, NASA HQ and Kennedy Space Center both offer separate training modules that provide specific guidance on protections applicable to some of the subcategories of SBU information, such as export control, technical information exchange, and the document availability authorization process that determines whether scientific and technical information can be released. Marshall offers comprehensive training for each type of SBU information. The training module, "Safeguarding MSFC's Administratively Controlled Information," provides detailed explanations about information protected by export regulations and FOIA; inventions; source selection, proprietary, and privileged information; software; embargoed information; and SBIR data. The module also addresses marking and safeguarding and specifies consequences for not protecting SBU information.

Training Program for Protecting SBU Information

The revised NPR 1600.1 established the NASA Security Education and Training, and Awareness (SETA) Program. This program emphasizes that management and employee involvement are essential to an effective security program. Specifically, the SETA Program requires the following:

- The Center Director must ensure that adequate procedures are in place whereby all NASA employees and contractor personnel are briefed annually regarding Center security program responsibilities.

- Within 20 days of their arrival, a new NASA employee/contractor must receive an initial orientation briefing to acquaint them with local security procedures and employee responsibilities to protect personnel and Government property from theft, loss, or damage.

- The responsible supervisor must ensure that job-related, facility-oriented security education, and awareness instructions or training for newly assigned personnel are timely.

The November 2005 NPR 1600.1 recognizes that the effectiveness of an individual in meeting their security responsibilities is proportional to the degree to which the individual understands those responsibilities. It assigns the responsibility for providing training about SBU information to the Center Directors and an individual's manager and supervisor. However, the NPR does not ensure that the training being given must be comprehensive, in that it does not require that the training cover the policies and procedures for identifying, marking, safeguarding, storing, accessing, disclosing, protecting, transmitting, destroying, and imposing administrative violations and sanctions for all the types of SBU information that NASA handles. As written, the training requirements allow each manager, supervisor, and Center Director to determine which aspects of the Agency's SBU information requirements and the types of SBU information to include in its training. As a result, each Center's training will be different. For example, a Center Director could choose to only present the marking and safeguarding requirements for selected SBU types of information, such as export control, proprietary, FOIA, and SBIR data, while another could describe the types of SBU information that NASA uses and cover all the Agency's requirements with regard to SBU information, such as marking, storage, disclosure, protection, transmittal, and destruction.

Conclusion

By establishing the SETA Program, NASA has taken a positive step toward requiring that NASA employees and contractors be aware of the policies and procedures for managing and protecting SBU information. However, because originators of information are required to identify and protect SBU information, they must understand what SBU information is and how to prevent its inadvertent dissemination. If NASA employees and contractor personnel are unaware of what information needs protecting or are confused about how to protect it, SBU information could be inappropriately distributed, causing harm to the Agency as well as its projects and programs. Until NASA establishes a comprehensive, Agency-wide training program that covers SBU information, it has no assurance that the training provided to NASA employees and contractors covers a common baseline that incorporates an appropriate range of NASA policies and procedures for identifying and handling SBU information.

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

We recommend that the Assistant Administrator for the Office of Security Program Protection establish an Agency-wide comprehensive training program, to be implemented at each Center and HQ, that specifies the policies and procedures for identifying and handling SBU information.

Management's Response. Management concurred. The Office of Security Program Protection will add SBU information to their Web-site no later than May 12, 2006. The SBU information will provide employees and contractors access to the Awareness and Training information they need for identifying, marking, safeguarding, accessing, disclosing, and transmitting the information. In addition, OSPP will develop an Agency-wide comprehensive training program for SBU, which will outline the minimum policies and procedures that have to be covered by each Center in their SBU training and briefings. The training information will be placed on the System for Administration, Training, and Educational Resources for NASA (SATERN) by August 1, 2006.

Evaluation of Management's Response. Management's actions are responsive. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until all corrective actions have been completed and we have reviewed the supporting documentation.

APPENDIX A

Scope and Methodology

We performed work for this audit at Goddard Space Flight Center, HQ, Jet Propulsion Laboratory, Johnson Space Center, Kennedy Space Center, and Marshall Space Flight Center. Specifically, we interviewed personnel directly involved with export control, scientific and technical information, inventions, FOIA, Privacy Act, procurement, and security. In addition, we examined various SBU-related documentation generated by NASA Headquarters and the selected Centers.

To assess personnel awareness of SBU information, we analyzed various NASA requirements for identifying and protecting SBU information. The requirements reviewed included those for export control, scientific and technical information, inventions, FOIA, Privacy Act, procurement, security, counterintelligence, software, small business and innovative research, and information technology security.

To help us identify SBU-related laws, regulations, and agency directives that could apply to NASA, we contracted with the Federal Research Division (FRD) of the Library of Congress to give us a report that set forth the statutes, regulations, and Executive Branch directives that define and govern access to SBU information. We compared the SBU requirements identified in the FRD report with NASA's.

We reviewed the last two NASA Export Control Program Annual audits at the selected Centers and followed up on the status of open recommendations.

We evaluated SBU-related training, including training accessible online, available to NASA employees and interviewed employees involved with SBU-related training at HQ and selected Centers. In addition, we examined new employee orientation training given at HQ and the selected Centers.

As part of our review of NASA's policies and procedures to protect SBU information, we sampled NASA documents available on the Internet and found that they contained meta-data that could be considered SBU. In December 2005, we issued a report to the NASA Chief Information Officer and recommended that NASA develop policies and procedures to define, recognize, and protect meta-data that may be contained in electronic documents. Further, we recommended that NASA provide user awareness training on the meta-data policies and procedures developed pursuant to the preceding recommendation.

We performed the audit from July 2004 through March 2006. This audit was performed in accordance with generally accepted government auditing standards.

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Review of Internal Controls

We reviewed policies and procedures relating to SBU information and for training personnel to recognize and protect such information. NASA's policies and procedures with regard to SBU information are consistent with Federal laws and selected agencies' SBU requirements. The Agency has effectively assigned accountability for the security of sensitive information to OSPP. Revisions incorporated into NPR 1600.1, "NASA Security Procedural Requirements w/Change 1," issued on November 8, 2005, adequately addressed the issues that we had communicated to OSPP officials regarding (1) the incomplete listing of the types of SBU information that NASA uses and (2) the lack of cross-referencing to other documents that contain additional requirements for specific types of SBU information.

"Standards for Internal Control in the Federal Government" identifies training as an important element in creating a good internal control program. The lack of a comprehensive training program with regard to SBU information leaves NASA officials unable to assure that SBU information NASA controls is marked and handled in a manner consistent with NASA policies and procedures and may result in inconsistencies and errors regarding management of SBU information. We recommended that OSPP establish an Agency-wide comprehensive training program that specifies the policies and procedures for identifying and handling SBU information.

Prior Coverage

The Government Accountability Office (GAO) and the NASA Office of Inspector General (OIG) have issued 8 reports of particular relevance to the subject of this report. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted NASA OIG reports can be accessed at http://www.hq.nasa.gov/office/oig/hq/audits/reports/FY06/index.html

Government Accountability Office

> "Managing Sensitive Information: Departments of Energy and Defense Policies and Oversight Could Be Improved," GAO-06-369, March 7, 2006

"Managing Sensitive Information: DOE and DOD Could Improve Their Policies and Oversight," GAO-06-531T, March 14, 2006

"Export Controls: Post-Shipment Verification Provides Limited Assurance That Dual-Use Items Are Being Properly Used," GAO-04-357, January 12, 2004

NASA Office of Inspector General

"NASA's Policies for Protecting Technology Exported to Foreign Entities," IG-06-006, March 14, 2006

Letter to Congress on NASA's Export Controls, February 23, 2006

"NASA Lacks Procedures to Define, Recognize, and Protect Meta-Data," A-04-013, December 19, 2005

"Cyber Security: The Status of Information Security and the Effects of the Federal Information Security Management Act (FISMA) at NASA," Statement of the Honorable Robert W. Cobb, NASA Inspector General, June 24, 2003

"Goddard Space Flight Center's Compliance with Export Laws and Regulations," IG-02-016, May 14, 2002

Comparison of Federal and Selected Agencies' SBU Requirements with NASA's

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
Executive Orders (EO) • EO 12958 (April 17, 1995), "prescribes a uniform system for classifying, safeguarding, and declassifying national security information." • EO 13292 (March 25, 2003), "prescribe a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism."	• NPR 1600.1, Chapter 5, "Classified National Security and Sensitive But Unclassified (SBU) Information Management"
White House Memoranda • Memorandum (March 19, 2002), from the White House Chief of Staff to the heads of all executive departments and agencies regarding the safeguarding and protection of sensitive homeland security information directs recipients to "undertake an immediate reexamination of current measures for identifying and safeguarding" Government information "regarding weapons of mass destruction, as well as other information that could be misused to harm the security of our nation and the safety of our people." Further, they should carefully consider Freedom of Information Act (FOIA) exemptions. • Pursuant to the White House Memorandum, a joint memorandum from the Acting Director of the Information Security Oversight Office and the Co-Directors of the Justice Department's Office of Information and Privacy reiterates the above memorandum to control sensitive information by giving full and careful consideration to all FOIA exemptions.	• NPR 1600.1, Section 5.24.2.1(c).(2-12), clarifies FOIA exemptions to include information determined to be unusually sensitive by a designated NASA official such as Center maps, security measures for infrastructure, and information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security.

[4] Federal and selected agencies' SBU requirements were taken from a report prepared by the Federal Research Division of the Library of Congress for the NASA OIG. The report is dated August 2004.

[5] Information is current as of February 2006.

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
Presidential/National Security Directives (PD/NSC) and National Security Decision Directives (NSDD)	
• PD/NSC 24 (November 16, 1977) protects unclassified information that would be useful to an adversary as the information is transmitted by and between Government agencies and contractors. References the need for communications security (COMSEC). • NSDD-189 (September 21, 1985) states that "to the maximum extent possible, the products of fundamental research remain unrestricted." • NSDD-145 (September 17, 1984) establishes initial objectives of policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding systems which process or communicate sensitive information from hostile exploitation." • NSDD 42 (July 5, 1990) "establishes initial objectives, policies, and an organizational structure to guide the conduct of activities to secure national security systems from exploitation."	• NPR 2810.1, Section 4.11, provides detailed guidance for using encryption for classified and unclassified information. • NPR 2810.1, Section 4.12.1; provides guidance on National security information. • NPR 1600.1, Section 5.15, requires users of COMSEC material to follow the NASA Central Office of Record Standard Operating Procedures and the National Security Telecommunications Systems Security Instruction 4005. • NPR 2200.2B, Section 1.8, policy promotes release of scientific and technical data.
Federal Laws/Regulations	
• Freedom of Information Act (FOIA) of 1966, while promoting release of information, the Act provides 9 exemptions and 3 special law enforcement exclusions. In 2001, agencies were encouraged to carefully consider the values of safeguarding national security, enhancing the effectiveness of law enforcement, protecting sensitive business information, and preserving personal privacy when determining whether information could be released.	• NASA FOIA regulations and 14 CFR 1206, "Availability of Agency Records to Members of the Public," establish NASA policy for release of Agency records. • NPR 1600.1, Section 5.24.2.1(c).(2-12), clarifies FOIA exemptions to include information determined to be unusually sensitive by a designated NASA official, such as Center maps, security measures for infrastructure, and information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security.
• Computer Security Act of 1987 defines sensitive information and requires agencies to identify computer systems that contain	• NPR 2810.1: o Appendix C, "Glossary," provides a simpler definition of "sensitive

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
sensitive information and to plan security and privacy for each system identified. Protection means providing confidentiality, integrity, and/or availability.	information" than the one provided by the Computer Security Act. o P.1, "Purpose," and 1.1 "Objectives of NASA's IT Security Program," discuss confidentiality, integrity, and availability. o 1.2.6 says everyone who uses information technology resources bears responsibility for ensuring that integrity, availability, and confidentiality are not compromised.
• Homeland Security Act of 2002 mandates that Federal agencies share relevant and appropriate homeland security information with other Federal agencies, defines homeland security, and exempts critical infrastructure information from disclosure under FOIA.	• NPR 1600.1, 7.17.2.8, states that the Director, Security Management Division shall monitor the threat status in the Agency and maintain close liaison with the Department of Homeland Security (DHS) and National-level intelligence and security agencies for timely and accurate threat information.
• Arms Export Control/International Traffic in Arms Regulations (ITAR); defines the United States Munitions List	• NPR 1600.1, Appendix J, "NASA Foreign Visitor Security/Technology Control Plan Sample Template," contains the Security/Technology Transfer Control Plan (STTCP), which is used to ensure that technology is protected in accordance with NASA policy and procedure, and in accordance with EAR and ITAR. Section 3 contains materials that are to be used for a briefing on EAR and ITAR.
• Export Administration Act/Export Administration Regulations (EAR); specifies the Commerce Control List and the Missile Technology Control Regime	NPR 1600.1, Appendix J (3) -- see previous narrative.
Laws/Regulation/Agency Policy-Guidance • Nuclear Nonproliferation Act • Nuclear Proliferation Prevention Act • Iran Nonproliferation Act	• NPR 2190.1, Section 4.4.1; addresses nuclear, missile, and chemical biological proliferation. Foreign partners and end-users of NASA exports must be screened for nuclear proliferation concerns, missile proliferation concerns, and chemical-biological proliferation concerns. The section refers to 15 CFR Part 740 for missile and nuclear screens and 15 CFR Part 742.2 for destinations of chemical-biological weapons

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
• National Defense Authorization Act for FY 1991 - amends ITAR and EAR • National Defense Authorization Act for FY 1999 - limits missile exports to China	proliferation concern. • NPR 2190.1 o Chapter 4, "Export Administration Regulations (EAR) Procedures," describes license exceptions allowed and refer to 15 CFR 740, which provides detailed requirements for using the exceptions and warns that China has missile technology projects. o Chapter 5, International Traffic in Arms Regulations (ITAR) Procedures," Use of ITAR exemptions must be coordinated with the Center Export Administrator or the Headquarters Export Administrator.
Department of Defense • DoD 5200.1-R, Information Security Program, Apps. C (Classified) and 3 (Controlled Unclassified): marking "For Official Use Only" (FOUO) required at bottom of front cover, title page, first page, and outside of the back cover. In addition, pages that contain FOUO shall be marked at the bottom. Material other than paper documents shall bear markings that alert the holder or viewer. State Dept. designated Sensitive But Unclassified information - same requirements as FOUO. Drug Enforcement Administration (DEA) sensitive information requires marking the top and bottom of the front cover, title page, outside of back cover, and each page containing DEA sensitive information with "DEA Sensitive." Similar marking required for Unclassified Controlled Nuclear Information (UCNI).	• NPR 1600.1, Section 5.24.3, "Marking for SBU," states, "Information designated as SBU will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. The lack of SBU markings on information known by the holder to be SBU does not relieve the holder from safeguarding responsibilities. Where the SBU marking is not present on information known by the holder to be SBU, the holder of the information will protect it as SBU. Information protected by statute or regulation will be marked in accordance with the applicable guidance for that type of information. Information marked in accordance with such guidance need not be additionally marked SBU. If there is no specific guidance or marking requirements, information designated SBU will be marked as follows: a. Prominently mark the top and bottom of the front cover, first page, title page, back cover, and each individual page containing SBU information with the caveat "SENSITIVE BUT UNCLASSIFIED (SBU)." b. Materials containing specific types of SBU information may be further marked with the applicable caveat, e.g., "LAW ENFORCEMENT SENSITIVE," in order to alert the reader of the type of information conveyed. Where the

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
	sensitivity of the information warrants additional access and dissemination restrictions, the originator may cite additional access and dissemination restrictions. For example: *WARNING: This document is SENSITIVE BUT UNCLASSIFIED (SBU). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with NASA policy relating to SBU information. This information shall not be distributed beyond the original addressees without prior authorization* of *the originator.* c. SBU information being transmitted to recipients outside of NASA, for example, other federal agencies, state or local officials, NASA contractors, etc., shall include the following additional notice: *WARNING: This document is SENSITIVE BUT UNCLASSIFIED (SBU). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552) or other applicable laws or restricted from disclosure based on NASA policy. It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with NASA policy relating to SBU information and is not to be released to the public or other personnel who do not have* a *valid "need-to-know" without prior approval of an authorized NASA official (see NPR 1600.1).* d. Computer storage media, i.e., disks, tapes, removable drives, memory sticks, etc. containing SBU information will be marked "SENSITIVE BUT UNCLASSIFIED." e. Portions of a classified document, i.e., subjects, titles, paragraphs, and subparagraphs that contain only SBU information will be marked with the abbreviation (SBU). f. Individual portion markings on a document that contains no other designation are not required.

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
• DOD 5400.7R, DOD FOIA Program provides guidance on implementing FOIA, describes safeguards to protect sensitive information, DOD exemptions to FOIA, markings, and how to disseminate and transmit. • 03-CORR-017, FOIA Requests for Critical Infrastructure Information (March 2003) expands FOIA exemption 3 to cover critical infrastructure information (applies to DHS, not to DOD).	• 14 CFR 1206 NASA FOIA regulations, "Availability of Agency Records to Members of the Public," establishes the policies and procedures for release of NASA records. • NPR 1600.1, Section 5.24.6, "Storage, Access, Disclosure, Protection, Transmittal, and Destruction of SBU," provides minimum requirements for safeguarding SBU information.
Laws/Regulation/Agency Policy-Guidance • DOD Directive 5230.25, Withholding Unclassified Technical Data, states that the Secretary of Defense may withhold from public disclosure technical data with military or space applications unless regulations authorize the export of such data. _____ • 10 U.S.C. 130, Authority to Withhold from Public Disclosure Certain Technical Data _____ • 32 CFR 250, "Withholding of Unclassified Technical Data from Public Disclosure," implements 10 U.S.C. 130. _____ • 10 U.S.C. 128, Physical Protection of Special Nuclear Material: Limitation on Dissemination of Unclassified Information, states that the Secretary of Defense must prohibit the unauthorized dissemination of unclassified information pertaining to security measures, security plans, procedures, and equipment for the physical protection of special nuclear material.	• 14 CFR 1206, Subpart 5, authorizes the Associate Deputy Administrator or designee, after consulting with the General Counsel, to make final determinations about whether requested records will be made available or withheld from disclosure. _____ • No similar law that applies to NASA was identified. _____ • No similar law that applies to NASA identified. However, NPR 2200.2B, Section 4.2.2, "Protection of Certain STI Information," warns that certain types of information must be protected from public disclosure (national security-classified, export-controlled, personal information subject to the Privacy Act, copyrighted information, and documents disclosing inventions). Refer questions to NASA Headquarters or Center Patent or Intellectual Property Counsel and the Export Control Administrator. _____ • No similar law that applies to NASA was identified. However, NPR 7120.5C, Section 3.2.1.2.i, "Complete a Safety and Mission Success Plan," provides requirements for obtaining approval to launch radioactive materials. • NPR 2190.1, Section 4.4.1, requires foreign partners and end-users of NASA exports to be screened for nuclear, missile, and chemical biological proliferation concerns. Policy

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
	refers to 15 CFR 740 and 742.2.
• 32 CFR Part 223 implements 10 U.S.C. 128.	• No similar regulation that applies to NASA was identified.
Department of Energy	
• Safeguards & Security Glossary of Terms defines "Sensitive Unclassified Information" and "national security" and "governmental interests" as used in the definition.	• NPR 2810.1 Appendix C, provides a simpler definition of "sensitive information" than the definition provided by the Computer Security Act.
• Directives Management Document for Proposed DOE O471.X, Identifying Information as FOUO, directs DOE to establish a program to identify and mark sensitive unclassified information that may be exempt from FOIA disclosure as For Official Use Only (FOUO). [see DoE O 471.2A below.]	• NPR 1600.1 Chapter 10; "Glossary of Terms, Abbreviations, and Acronyms," defines Sensitive But Unclassified (SBU) information or material determined to have special protection requirements to preclude unauthorized disclosure to avoid compromises, risks to facilities, projects or programs, threat to the security and/or safety of the source of information, or to meet access restrictions established by laws, directives, or regulations: ITAR, EAR, Militarily Critical Technologies List, FAR, Privacy Act, Proprietary, FOIA, UCNI, NASA Developed Software, STI, source selection and bid and proposal information, and inventions.
• 42 U.S.C. 2168, Dissemination of Unclassified Information, provides a definition of Unclassified Controlled Nuclear Information (UCNI) and provides civil and criminal penalties.	• NPR 1600.1 Section 5.25, "Use, Protection and Accountability of Department of Energy (DOE) Unclassified Controlled Nuclear Information (UNCI)," defines UCNI, requires access only by personnel with a need-to-know, prohibits access to foreign nationals without approval of the DOE, requires storing to prevent unauthorized disclosure, and encryption for electronic transmission. • NPR 2190.1 Section 4.4.1 addresses nuclear, missile, and chemical biological proliferation. Foreign partners and end-users of NASA exports must be screened for nuclear proliferation concerns, missile proliferation concerns, and chemical-biological proliferation concerns. The section refers to 15 CFR Part 740 for missile and nuclear screens and to 15 CFR Part 742.2 for destinations of chemical-biological weapons proliferation concern.

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
• 10 CFR Part 1017, "Identification and Protection of Unclassified Controlled Nuclear Information," and DOE O 471.2A, "DOE Information Security Program Directive," state that documents containing UCNI must be marked conspicuously as "Not for Public Dissemination" prior to transmitting or upon retirement. Access is granted on a need-to-know basis. Documents must be physically protected. Provides civil and criminal penalties.	• No similar NASA regulations were identified. However, NPR 1600.1, Section 5.25.3.1, requires markings per DOE.
Nuclear Regulatory Commission • COMSECY-02-0015, Commission Action Memo: Withholding Sensitive Homeland Security Information from the Public - defines sensitive homeland security information based on draft DHS language not made public. Generally, information generated by the NCR, its licensees, or contractors will be withheld if its release could provide a clear and significant benefit to an adversary in a potential attack.	• NPR 1600.1 Section 5.25, "Use, Protection, and Accountability of Department of Energy (DOE) Unclassified Controlled Nuclear Information (UNCI)," defines UCNI, requires access only by personnel with a need-to-know, prohibits access to foreign nationals without approval of the DOE, requires storing to prevent unauthorized disclosure, and encryption for electronic transmission.
Department of State • Volume 12, Foreign Affairs Manual 540, "Scope," defines SBU.	• NPR 1600.1, Chapter 10; "Glossary of Terms, Abbreviations, and Acronyms," defines Sensitive But Unclassified (SBU) information or material determined to have special protection requirements to preclude unauthorized disclosure to avoid compromises, risks to facilities, projects or programs, threat to the security and/or safety of the source of information, or to meet access restrictions established by laws, directives, or regulations: ITAR, EAR, Militarily Critical Technologies List, FAR, Privacy Act, Proprietary, FOIA, UCNI, NASA Developed Software, STI, source selection and bid and proposal information, and inventions.
• Volume 12, Foreign Affairs Manual 542, "Implementation," changes "Limited Official Use" to SBU.	• NPR 1600.1 Section 5.24.1.2, SBU has previously been designated as For Official Use Only.
• Volume 12 Foreign Affairs Manual 543,	<u>Export Control</u> • NPR 2190.1, Section P.1, "Purpose,"

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
"Access, Dissemination and Release," addresses distribution restriction.	provides guidance, instructions, and responsibilities for all NASA employees and support contractors engaged in activities that involve the transfer of commodities, software, or technologies to foreign individuals or organizations. <u>Scientific and Technical Information (STI)</u> • NPR 2200.2B, Section P.1, "Purpose," identifies requirements for approving, publishing, and disseminating STI. <u>Inventions</u> • NPR 2200.2B, Section 4.2.2.2 states that information that is otherwise approved for public release may be withheld if it discloses an invention. <u>Privacy Act</u> • 14 CFR 1206, "Availability of Agency Records to Members of the Public," establishes NASA policy for release of Agency records. • NPD 1382.17G, Section 1.e.4, prohibits NASA employees and contractors from disclosing any information in identifiable form without the written consent of the person to whom it pertains. • NPR 1450.10C, Appendix C, "Privacy Act Correspondence," requires that Privacy Act correspondence be safeguarded according to NPR 1382.17. <u>Procurement</u> • FAR Section 15.207, "Handling proposals and information" states that proposals shall be safeguarded from unauthorized disclosure throughout the source selection process. Information received in response to a request for proposal shall be safeguarded adequately from unauthorized disclosure. • NASA FAR Supplement (NFS) Section 1803.104-4, "Disclosure, Protection, and Marking of Contractor Bid or Proposal Information and Source Selection

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
	Information" states that only Government employees serving in certain positions are authorized access to propriety or source selection information but only to the extent necessary to perform their official duties. • Procurement Information Circular (PIC) 03-03, "Scientific and Technical Information," provides guidance on treating STI produced under research and development contracts. <u>Security</u> • NPR 1600.1, Section 5.24.4, "Responsibilities," states that officers and employees designating information or materials as SBU and those receiving materials so marked shall be responsible for properly safeguarding the information contained therein. <u>Counterintelligence</u> • NPD 1660.1, "NASA Counterintelligence (CI) Policy," Section 1.3, "Responsibilities," makes the Assistant Administrator for Security and Program Protection responsible for the NASA CI Program. <u>Software</u> • NPR 7500.1, "NASA Technology Commercialization Process," Section 4.2, requires NASA employees and contractors to report new technologies and innovations (including software) as soon as possible after conception to determine whether intellectual property protection and patent application are appropriate. • NPD 7500.2, NASA Technology Commercialization Process," Section 5, "Responsibilities," makes the NASA General Counsel responsible for protecting intellectual property rights and for ensuring that transfer of NASA technology and intellectual property through licensing conforms with applicable laws, regulations, and NASA policies.

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
	Small Business and Innovative Research (SBIR) Data • NPR 2200.2B, Section 4.5.10.2, states that it is NASA policy to restrict all SBIR program reports from public disclosure for the period specified in the contract for SBIR data unless the contractor grants permission to publicly release the report sooner. Other • NPR 1450.10C, "NASA Correspondence Management and Communications Standards and Style," Chapter 6, "Electronic Communications," states that sensitive but unclassified information may be sent using e-mail if it is encrypted. • NPR 1450.10C, Appendix C, states that correspondence containing any item of information subject to the Privacy Act that is removed from a system of records not under the control of a system manager or an authorized representative, is to be prominently identified as a record protected y the Privacy Act. NASA Form 1534, "The Attached Material is Subject to the Privacy Act of 1974," should be used as a cover sheet for the correspondence. • NPR 7120.5B, "NASA Program and Project Management Processes and Requirements," makes program and project managers responsible for protecting information generated within their program. • NPR 2820.1C, "NASA Software Policies," states NASA's policy regarding intellectual protection of software and the release of software is to (a) manage and protect software created by or for NASA as valuable intellectual property during all phases of the life cycle; and (b) establish procedures and requirements concerning the release of software created by or for NASA that will maximize its benefit to NASA, the U.S. public, and the U.S.
• Volume 12, Foreign Affairs Manual 544,	• NPR 1450.10C, "NASA Correspondence

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
"SBU Handling Procedures" discusses possible encryption. • Volume 12 Foreign Affairs Manual 545, "Responsibilities" gives a general warning of consequences for disclosing SBU information. • Guidance for Drafting SBU Telegrams describes how documents containing SBU information should be labeled. • Volume 5 Foreign Affairs Manual 751.2, "Prohibitions When Using Email" states that unclassified SBU e-mail may be transmitted on the unclassified Intranet. SBU information marked NOFORN (Not for Release to Foreign Nationals) or with other restricted distribution must be transmitted on the classified Intranet. SBU e-mail may not be transmitted over the Internet. • Volume 12 Foreign Affairs Manual 660, "Communications Security (COMSEC) (SBU)." The Department of State would not release a copy of this document to the Federal Research Division of the Library of Congress. • Volume 3 Foreign Affairs Manual 4300, "Disciplinary Action" contains the following subsections that deal with various aspects of disciplinary action: 4310 Disciplinary Action-General; 4320 Disciplinary Action Common Practices; 4330 Admonishment; 4340 Reprimand; 4350 Suspension; 4360 Separation for Cause; 4370 List of Offenses	Management and Communications Standards and Style," Chapter 6, states that sensitive but unclassified information may be sent using e-mail if it is encrypted. • NPR 1600.1, Section 5.24.8.2, states that sanctions [for noncompliance with the NPR section on SBU information] include, but are not limited to, warning notice, admonition, reprimand, suspension without pay, forfeiture of pay, removal, and/or discharge. • NPR 1450.10C; Section 6.6.1.2, states that telegrams are delivered by telephone or printed copy in a few hours to any location within the United States (except Hawaii) and to Canada. • NPR 1450.10C, Section 6.2.3, states that e-mail systems are not secure. Never use them to transmit classified information even if it is encrypted. However, SBU may be sent using e-mail if it is encrypted. • NPR 2810.1, Section 4.11.2, provides detailed guidance for using encryption for classified and unclassified information. • NPR 1600.1, Section 5.15, requires users of COMSEC material to follow the NASA Central Office of Record Standard Operating Procedures (CSOP) and the National Security Telecommunications Systems Security Instruction (NSTSSI) 4005. Security • NPR 1600.1, Section 1.4, "Violations of Security Requirements," states that anyone who willfully violates, attempts to violate, or conspires to violate any regulation or order involving the NASA Security Program is subject to disciplinary action up to and including termination of employment and/or

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
Subject to Disciplinary Action Foreign Services. No one subsection details specific sanctions or procedures for responding to the improper or unauthorized release of SBU; however, all subsections are relevant since they describe the sanctions and procedures for responding to the improper or unauthorized release or handling of information generally.	possible prosecution under 18 U.S.C. 799 that provides for fines or imprisonment for not more than 1 year, or both.. • NPR 1600.1, Section 5.24.8.1, addresses administrative violations and sanctions for employees and non-employees if they disclose information designated as SBU without proper authorization. • NPR 1600.1 Section 5.24.8.2, states that sanctions [for noncompliance with the NPR section on SBU information] include, but are not limited to, warning notice, admonition, reprimand, suspension without pay, forfeiture of pay, removal, and/or discharge. • NPR 1600.1 Section 5.24.8.3, states: "Such sanctions may be imposed, as appropriate, upon any person determined to be responsible for a violation of disclosure restrictions in accordance with applicable law and regulations, regardless of office or level of employment." • NPR 1600.1 Section 5.22.2, states: "CNSI [classified national security information] and SBU are always the property of the United States Government. Individuals who remove SBU or CNSI may be subject to disciplinary action up to and including prosecution under Title 18 and Title 50 U.S.C. and other applicable laws." <u>Procurement</u> • FAR 3.101-3(a) states that agencies are required by Executive Order 11222 (May 8 1965) and 5 CFR 735 to prescribe "Standards of Conduct" that contain agency-authorized exceptions to 3.101-2, "Solicitation and Acceptance of Gratuities by Government Personnel," and disciplinary measures for persons violating the standards of conduct. • 14 CFR 1207, which refers to 5 CFR 2635, requires employees to comply with restrictions and prohibitions on disclosure of

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
	• certain sensitive Government information under the FOIA and Privacy Act, • proprietary and confidential information, and • certain procurement information. • FAR 3.104-8, "Criminal and civil penalties and further administrative remedies," states that criminal and civil penalties and administrative remedies, may apply to conduct that violates the Procurement Integrity Act. An official who knowingly fails to comply with the requirements of 3-104-3 is subject to the penalties and administrative action set forth in subsection 27(e) of the Act." • NFS 1852.235-73 requires contractors to review for publication or dissemination of the data for conformance with laws and regulations governing its distribution, including intellectual property rights, export control, national security, and other requirements, but does not stipulate consequences for inappropriate dissemination. <u>Proprietary</u> • NPR 1600.1 addresses proprietary information and consequences for noncompliance with the NPR (see above). In addition, 18 U.S.C. 1832 states that organization who steals trade secrets can be imprisoned not more than 10 years and/or fined up to $5,000,000. <u>Export Control</u> • NPR 2190.1, "NASA Export Control Program," Section 8.1, "General," explains that noncompliance with export control laws and regulations could result in criminal, civil, or administrative penalties. Section 8.3.1 refers to specific ITAR and EAR regulations in the Code of Federal Regulations that address penalties. • NPR 1600.1 provides for violating ITAR and EAR regulations, both criminal and civil penalties (criminal - fines up to $1 million

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
	and 10 years imprisonment; civil - fine up to $100 thousand). Scientific and Technical Information • NPR 2200.2B, "Requirements for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information (STI)" Section 4.2.2., "Protection of certain STI Information," states that certain types of information are required to be protected from public disclosure. FOIA provides guidance regarding categories of information that are exempt from mandatory release under FOIA. Dissemination of information may also be restricted under other laws, regulations, or policy. Restricted-access information includes export-controlled information, personal information subject to the Privacy Act, proprietary information of the Government or others, copyrighted information, and documents disclosing inventions. In addition, certain types of information are further restricted from dissemination via NAS public websites. With the exception of addressing the consequences for releasing STI information that is subject to export control requirements, NPR 2200.2B does not address the consequences for releasing STI that should be protected from public disclosure. Inventions • NPR 2200.2B, Section 4.5.16, "Documents Disclosing Inventions," says that information that is otherwise approved for public release may be withheld if it discloses an invention. (See STI above.) NPR 1600.1, Section 1.4.2, says that anyone who willfully violates, attempts to violate, or conspires to violate any regulation or order involving the NASA Security Program is subject to disciplinary action up to and including termination of employment and/or possible prosecution under 18 U.S.C. 799, that provides for fines or imprisonment for not more than 1 year, or both.

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
	Software • NPR 2210.1A, "External Release of NASA Software," Section 3.6.1, requires compliance with export control laws and regulations, which stipulate consequences SBIR Data • NASA Federal Acquisitions Regulation (FAR), Supplement (NFS) contract clause 1852.235-73, requires contractors to review publication or dissemination of the data for conformance with laws and regulations governing its distribution, including intellectual property rights, export control, national security, other requirements but does not stipulate consequences for inappropriate dissemination. FOIA and Privacy Act Information • 14 CFR 1212.800 states: "Failure to comply with the requirements of the Privacy Act and this part could subject NASA to civil suit under the provisions of 5 U.S.C. 552a(g)." • 14 CFR 1212.801 states: "(a) A NASA officer or employee may be subject to criminal penalties under the provisions of 5 U.S.C. 552a(i) (1) and (2). (1) Section 552a(i)(1). Any officer or employee of an agency, who by virtue of employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000. (2) Section 552a(i)(2). Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000. (3) These two provisions apply to

Federal and Selected Federal Agencies' SBU Requirements[4]	NASA SBU Requirements[5]
	NASA civil service employees as well as those employees of a NASA contractor with responsibilities for maintaining a Privacy Act system of records. (b) Section 552a(i)(3). Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

MANAGEMENT COMMENTS

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

April 27, 2006

Reply to Attn of: Office of Security and Program Protection

TO: Assistant Inspector General for Auditing

FROM: Assistant Administrator for Security and Program Protection

SUBJECT: Response to Draft Audit Report, "NASA Should Improve Employee Awareness of Requirements for Identifying and Handling Sensitive But Unclassified Information" (Assignment No. A-04-013-00)

In response to your memo dated April 11, 2006 on the subject Draft Audit Report, A-04-013-00, "NASA Should Improve Employee Awareness of Requirements for Identifying and Handling Sensitive But Unclassified Information", OSPP has reviewed the recommendation and comments.

Based on your recommendation, OSPP has developed an action plan to satisfy the findings in your report. Please see the OSPP response listed below.

OIG Recommendation for Corrective Action:

1. We recommend that the Assistant Administrator for the Office of Security and Program Protection establish an Agency-wide comprehensive training program, to be Implemented at each Center and HQ, that specifies the policies and procedures for Identifying and handling SBU information.

OSPP Response:

1. Concur. OSPP will add SBU information to the OSPP Web-site no later than May 12, 2006. The SBU information will provide employees and contractors access to the Awareness and Training information they need for identifying, marking, safeguarding, accessing, disclosing, and transmitting the information. It also makes reference to administrative violations and sanctions that can be imposed if SBU is not properly handled.

2. OSPP will also develop an Agency-wide comprehensive training program for SBU which will outline the minimum policies and procedures that have to be covered by each Center in their SBU training and briefings. The training information will be placed on the System for Administration, Training, and Educational Resources for NASA (SATERN) by August 1, 2006. Each Center can use the OSPP course until they update or create their own

If you have any questions or need additional information, please contact Steven L. Peyton at 202-358-0191.

David A. Saleeba

cc:
Mr. Clint Herbert
Mr. Phillip Bounds
Mr. Frank Martin
Mr. Steven Peyton

Report Distribution

National Aeronautics and Space Administration (NASA)

Administrator
Deputy Administrator
Chief of Staff
  Mission Support Offices
Chief Information Officer
Assistant Administrator, Institutions and Management, Security and Program Protection
Director, Institutions and Management, Infrastructure and Administration, Management Systems Division

NASA Centers

Director, Goddard Space Flight Center
Director, Jet Propulsion Laboratory
Director, Lyndon B. Johnson Space Center
Director, John F. Kennedy Space Center
  Chief Counsel, John F. Kennedy Space Center
Director, George C. Marshall Space Flight Center

Note: A redacted version of this report was distributed to non-NASA organizations and individuals and members of Congress. Recipients of the redacted version may request the full report from the NASA IG Counsel at 202-358-2575 of from the NASA IG Executive Officer at 202-358-0615.

Non-NASA Organizations and Individuals

Office of Management and Budget
  Deputy Associate Director, Energy and Science Division
    Branch Chief, Science and Space Programs Branch
Government Accountability Office
  Director, Defense, State, and NASA Financial Management, Office of Financial Management and Assurance
  Director, NASA Issues, Office of Acquisition and Sourcing Management

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
- Senate Subcommittee on Commerce, Justice, and Science

Senate Committee on Commerce, Science, and Transportation
- Senate Subcommittee on Science and Space

Senate Committee on Homeland Security and Governmental Affairs

House Committee on Appropriations
- House Subcommittee on Science, State, Justice, and Commerce

House Committee on Government Reform
- House Subcommittee on Government Management, Finance, and Accountability

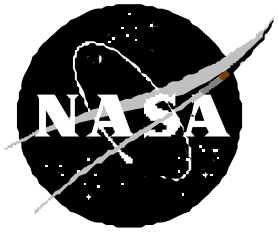
House Committee on Science
- House Subcommittee on Space and Aeronautics

Major Contributors to the Report:

Earl Baker, Attorney Advisor
Lamar Brickhouse, Auditor
Ari Elias-Bachrach, IT Specialist
Wesley Pippenger, Management Analyst
Carol St. Armand, Auditor
Janet Overton, Report Process Manager

MAY 9, 2006

REPORT NO. IG-06-010



OFFICE OF AUDITS

OFFICE OF INSPECTOR GENERAL

ADDITIONAL COPIES

Contact the Assistant Inspector General for Auditing at 202-358-1232 for additional copies of this report. Unrestricted audit reports by the NASA Inspector General's Office of Audits are available over the Internet at www.hq.nasa.gov/office/oig/hq/audits/reports/FY06/index.html.

COMMENTS ON THIS REPORT

In order to help us improve the quality of our products, if you wish to comment on the quality or usefulness of this report, please send your comments to Ms. Jacqueline White, Director of the Quality Control Division, at Jacqueline.White@nasa.gov or call 202-358-0203.

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
Washington, DC 20546-0001

NASA HOTLINE

To report fraud, waste, abuse, or mismanagement, contact the NASA OIG Hotline at 800-424-9183 or 800-535-8134 (TDD). You may also write to the NASA Inspector General, P.O. Box 23089, L'Enfant Plaza Station, Washington, DC 20026, or use http://www.hq.nasa.gov/office/oig/hq/hotline.html#form. The identity of each writer and caller can be kept confidential, upon request, to the extent permitted by law.