

Effective Date: October 16, 2007

## **Sensitive But Unclassified (SBU) Controlled Information**

The Computer Security Act of 1987, Public Law 100-235, defines "sensitive information" as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy." The purposes of the Computer Security Act included developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems and establishing security plans by all operators of Federal computer systems that contain sensitive information.

Within the Federal government, it is recognized more broadly that the failure to sufficiently identify sensitive information that must or should be subject to special handling procedures and protection from inappropriate disclosure, wherever it may reside in the Federal government, may result in increased risk to life or mission essential assets or monetary or other loss to individuals or firms.

This section 5.24 provides guidance and requirements for identifying and safeguarding sensitive but unclassified information at NASA. As used in this Chapter, the words "shall" and "must" identify mandatory requirements. The words "may," "should," "could," and "can" identify discretionary guidelines.

### **5.24.1. Background, Scope and Responsibilities**

5.24.1.1. NASA has determined that official information and material of a sensitive but unclassified (SBU) nature that does not contain national security information (and therefore cannot be classified) shall be protected against inappropriate access and disclosure by designating and handling such information as SBU in accordance with the procedures set forth in this NPR. Access to and disclosure of SBU information shall be to authorized individuals only. The identification of an authorized individual is based on a "need-to-know" analysis in accordance with paragraph 5.24.4.4 of this NPR.

5.24.1.2. With the exception of certain types of information required to be protected by statute or in accordance with an agreement with the information owner (e.g., Limited Rights Data obtained from a contractor), the designation of information as SBU is largely discretionary and must be made based on sound judgment and the criteria provided in section 5.24.2 of this NPR.

5.24.1.3. When information is designated as SBU in accordance with the requirements stipulated in section 5.24.2 of this NPR, it shall be marked in accordance with section 5.24.3, stored, accessed, disclosed and transmitted in accordance with section 5.24.4, and decontrolled or destroyed in accordance with section 5.24.5. The use of markings other than those described in section 5.24.3 shall not be used.

5.24.1.4. The SBU designation and procedures set forth herein do not apply to the information, reports, or analysis by members of other agencies or departments who are members of the National Intelligence Board (NIB), who are on loan to NASA, and whose authorities are derived

from other sources. However, SBU designation and procedures shall be applied when such information, or portions thereof, is copied for dissemination within NASA.

5.24.1.5. Each program or project office, or Center or Agency organization (e.g., a branch or division), may develop, publish, and maintain an organizational SBU "Designation Guide" to supplement the requirements and guidelines provided in this NPR. The Designation Guide should define additional requirements and guidelines for information developed or used by the program or project consistent with this Chapter and commensurate with a lower level organizational document, such as a System Level Procedure or Work Instruction. For example, a Designation Guide could document procedures where a program or project office has determined that a class of information, or information related to a specific aspect of the program/project, must be designated as SBU, or will not be designated as SBU but will be protected in a certain way. A Designation Guide shall be signed by the appropriate program or project manager with concurrence by the Office of Security and Program Protection at NASA Headquarters.

5.24.1.6. *Responsibilities*

a. Originators of information (hereinafter, "Originator"), individuals controlling information or recommending its dissemination (hereinafter, "Custodian"), officials authorized to designate information as SBU (hereinafter, "Designating Official"), and individuals handling or possessing information designated SBU or that is known or reasonably assumed to be SBU (hereinafter, "Holder") shall be responsible for properly safeguarding SBU information. These individuals shall:

- (1) Comply with the safeguarding requirements for SBU information as outlined herein. NASA Civil Servants are required to protect SBU information in accordance with the Trade Secrets Act (18 U.S.C. 1905), the Privacy Act (5 U.S.C. 552a) the Standards of Ethical Conduct for Employees of the Executive Branch (5 C.F.R. 2635), and all other applicable Federal and NASA Regulations.
- (2) Participate in formal classroom or computer based training sessions presented to communicate the requirements for safeguarding SBU information and the penalties that could result in unauthorized disclosure of SBU information.
- (3) Keep the number of copies of recorded SBU information to a minimum.
- (4) Ensure that contractors, consultants and other individuals not employed directly by NASA have proper protection obligations established through contract or agreement as a condition of access to SBU information. An obligation to protect SBU information shall be incorporated into a NASA contract through NASA FAR Supplement (NFS) clause 1852.237-72 Access to Sensitive Information. For additional information see paragraphs 5.24.4.4.1 and 5.24.4.4.2 of this NPR.

b. Supervisors and managers shall:

- (1) Ensure that an adequate level of education and awareness is established and maintained to emphasize safeguarding and preventing unauthorized disclosure of SBU information.
- (2) Ensure that an adequate level of education and awareness is established and maintained to emphasize that disclosing SBU information without proper authority could result in administrative or disciplinary action, fines and/or imprisonment.

(3) Take appropriate corrective actions, to include administrative or disciplinary action as appropriate, when unauthorized disclosures of SBU information occur.

#### 5.24.2. Identification and Designation of SBU Information

##### 5.24.2.1. *Designating Officials and Review of Information for Possible Designation as SBU*

a. Only a Designating Official may designate information as SBU. For the purpose of determining the appropriate Designating Official, a program or project office, or a Center or Agency organization (e.g., a branch or division) “owns” information if it originated or is responsible for the information. Depending on whether the information is “owned” by a program, a project, or an organization, the Designating Official shall be the program or project manager, or a high-level management/supervisory individual in the organization (e.g., a Branch or Division Chief), or their delegate(s). All delegations shall be in writing. The name of each Designating Official and a copy of each delegation shall be provided to the Center Security Office.

b. Originators and Custodians shall review information that may qualify as SBU under the guidelines described in paragraph 5.24.2.2 of this NPR for possible designation as SBU and provide a recommendation to the Designating Official prior to its dissemination. If an Originator or Custodian has questions regarding the sensitivity of information, they should err on the side of caution and provide the information to the Designation Officer for a determination. If information created by or in the possession of an Originator, Custodian, or Holder is not marked as SBU and he or she determines or believes that the information is required to be designated as SBU (see section 5.24.2.2.e of this NPR), he or she shall safeguard the information in accordance with section 5.24.4 of this NPR and shall notify the applicable Designating Official immediately so that an official SBU designation may be made.

c. Such information shall not be disseminated prior to the Designating Official making a determination whether to designate the information as SBU

##### 5.24.2.2. *Designation of Information as SBU*

a. Information required to be protected by statute or in accordance with an agreement with the information owner must be designated as SBU. In all other cases, that is where the SBU designation is discretionary, the Designating Official shall designate information as SBU based on guidance provided herein. The National and Aeronautics and Space Act of 1958 (the Space Act) requires NASA to “provide for the widest practicable and appropriate dissemination of information concerning its activities and the results thereof” (42 U.S.C. 2473 (a)(3)). Therefore, with the exception of information that must be designated as SBU (examples of which are provided in paragraph 5.24.2.2.(e)), Designating Officials should designate information as SBU based on sound judgment after evaluating: (i) the interests under the Space Act in disseminating the information; (ii) the risks and consequences of unauthorized dissemination; and (iii) the burden on the Agency of protecting information designated as SBU. Before designating information subject to discretionary withholding as SBU, the Designating Official must determine that the risks and consequences of unauthorized release or disclosure outweigh the interests of dissemination and the burden on the Agency resulting from an SBU designation. When evaluating the risks and consequences of unauthorized dissemination, the Designating Official should consider whether unauthorized release or disclosure of the information has the potential to: (i) damage a person's privacy interests or economic or physical welfare; (ii) adversely impact non-governmental firms or institutions (e.g., cause monetary or other economic loss to firms or institutions); or (iii) compromise programs or operations essential to NASA's missions or to the safeguarding of our national interests.

b. Information originating within or furnished to NASA that may be designated as SBU includes: (i) information that qualifies for withholding under one or more of the applicable exemption criteria of the Freedom of Information Act (5 U.S.C. §552) (hereinafter, "FOIA") as described in paragraphs 5.24.2.2.d and 5.24.2.2.e of this NPR, and (ii) information that does not qualify for withholding under the FOIA but where a determination is made under the guidelines described in paragraph 5.24.2.2.f of this NPR that the information should be designated as SBU based on the risks and consequences of an unauthorized release.

c. Designating information as SBU does not necessarily represent that the information has been determined by NASA to be exempt from disclosure under the FOIA. Requests under the FOIA, for information designated as SBU, shall be reviewed and processed in the same manner as any other FOIA request.

d. The FOIA establishes a legal right of access to identifiable, existing federal agency records, subject to statutory exemptions. In most cases, the application of FOIA exemptions by an Agency is discretionary. That is, a FOIA exemption allows an Agency to withhold applicable information from disclosure to the public, but if the information is not required to be withheld under some other statutory authority the Agency has the discretion to voluntarily release the information. In accordance with paragraph 5.24.2.2.a of this NPR, before designating information subject to discretionary withholding under a FOIA exemption as SBU, the Designating Official must determine that the risks and consequences of unauthorized disclosure justify an SBU designation. FOIA exemptions are set forth in 5 U.S.C. §552(b).

- (1) FOIA exemption 1 applies to classified national security information. Because SBU is inherently unclassified information, FOIA exemption 1 is not applicable to SBU designations (see 5.24.2.2.e (1) for additional guidance);
- (2) FOIA exemption 2 applies to information related solely to internal personnel rules and practices of an agency (see 5.24.2.2.e (2) for additional guidance);
- (3) FOIA exemption 3 applies to information specifically exempted from disclosure by statute (see 5.24.2.2.e (3) for additional guidance);
- (4) FOIA exemption 4 applies to trade secret and commercial or financial information which is privileged or confidential (see 5.24.2.2.e (4) for additional guidance);
- (5) FOIA exemption 5 applies to inter-agency or intra-agency memorandum or letters which are not available by law to a party except in litigation with the agency (see 5.24.2.2.e (5) for additional guidance);
- (6) FOIA exemption 6 applies to personnel, medical, or similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy (see 5.24.2.2.e (6) for additional guidance);
- (7) FOIA exemption 7 applies to records or information compiled by or for law enforcement purposes (Note: generally, this exemption does not apply to information originated or handled by NASA);
- (8) FOIA exemption 8 is related to records relating to examination or operation of a financial institution (Note: generally, this exemption does not apply to information originated or handled by NASA);

(9) FOIA exemption 9 is related to geological and geophysical information, including maps, concerning wells (Note: generally, this exemption does not apply to information originated or handled by NASA).

e. The following examples are provided for guidance purposes. Additional examples or detail, that are specific or common to a particular program or project office, should be documented in an appropriate organizational Designation Guide as described in paragraph 5.24.1.5 of this NPR. Examples of information that could be categorized as SBU under particular FOIA exemptions include:

(1) Since SBU information does not include classified national security information (CNSI), FOIA exemption 1 does not apply to SBU information. For procedures related to CNSI see sections 5.1 – 5.23 of this NPR.

(2) FOIA exemption 2 information includes information related to internal personnel rules or practices if disclosure of such information would risk circumvention of a statute or lawful agency regulation. Information of this type generally relates to information that reasonably could be expected to enable someone to succeed in causing a feared harm. Designation of this type of information as SBU is generally discretionary and should be determined in accordance with paragraph 5.24.2.2.a of this NPR. Examples of such information could include:

(a) Center maps and/or documents describing locations/directions (e.g., latitude, longitude, depth, etc.) of underground utility conduits (e.g., sewers, gas, data, communications, etc.);

(b) Drawings and specifications that identify existing or proposed security measures for mission essential infrastructure designated assets or other key resources;

(c) Mission specific security plans that identify protective measures and procedures for assets that are sensitive in nature but are not classified. (Example: Payloads that utilize special nuclear materials, payloads that contain certain animal experiments, and STS missions, as determined by the CCS, etc.);

(d) Emergency contingency or continuity of operations plans that provide detailed information regarding emergency response processes and procedures that, if publicized, could give a potential adversary vital information with which to thwart or compromise emergency response efforts;

(e) NASA information technology (IT) internal systems data that could allow unauthorized access, infiltration, or damage to NASA IT systems. Such data may include: data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models.

(f) Systems security data revealing the security posture of the system. For example, threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, and Certification and Accreditation documentation; and

(g) Reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities, whether to persons, systems, or facilities, not otherwise eligible for classification under Executive Order 12958, as amended.

(3) Examples of FOIA exemption 3 information include:

(a) Certain information subject to export control under the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR). If information is determined to be export controlled (i.e., export is restricted or prohibited) under the ITAR or EAR, it must be protected from inappropriate disclosure to foreign entities. However, whether to designate such information as SBU is discretionary and shall be determined in accordance with paragraph 5.24.2.2.a of this NPR. For additional guidance see the Center Export Administrator and NPR 2190.1.

(b) Information developed by NASA under a Space Act Agreement and subject to section 303(b) of the Space Act (42 U.S.C. 2454(b)) or under a Cooperative Research and Development Agreement (CRADA) and subject to 15 U.S.C. §3710(c)(7)(B). These statutes cover information developed by NASA under a Space Act agreement or CRADA that would be a trade secret or commercial or financial information that is privileged or confidential if the information had been obtained from a non-Federal party participating in such an agreement. Such information must be protected in accordance with the terms of the Space Act agreement or CRADA under which it was developed. However, whether to designate such information as SBU is discretionary and shall be determined in accordance with paragraph 5.24.2.2.a of this NPR. For additional guidance see the Center Office of Chief Counsel and NAII 1050-1, Space Act Agreement Guide.

(c) Information disclosing a new invention in which the Federal Government owns or may own a right, title, or interest and subject to 35 U.S.C. §205. Designation of such information as SBU is discretionary and must be approved by the Center Patent/Intellectual Property Counsel.

(d) Plans for development or marketing of a government invention submitted under a license application and subject to 35 U.S.C. §209(f), and periodic reports on utilization of a government invention submitted under a license and subject to 35 U.S.C. §209(d)(2). For additional guidance see the Center Patent/Intellectual Property Counsel.

(e) Information subject to the Privacy Act of 1974 (5 U.S.C. §552a), which qualifies for withholding under FOIA exemptions 3 and 6. For additional guidance see paragraph 5.24.2.2.e.(6) related to FOIA exemption 6.

(4) Information exempt from disclosure under FOIA exemption 4 shall always be designated as SBU. Examples of FOIA exemption 4 information include:

(a) Proprietary information of others provided to NASA. Proprietary information of others is information developed at private expense embodying trade secrets or comprising commercial or financial information that is privileged or confidential. Under the Trade Secrets Act (18 U.S.C. 1905) NASA employees are subject to criminal prosecution and removal from office for wrongful disclosure of proprietary information received in the course of government employment or official duties. Proprietary information may be received by NASA with or without a nondisclosure agreement. However, proprietary information should always be marked by the owner with an appropriate notice indicating that the information is proprietary before it is accepted by NASA.

(b) Source selection information (SSI). The Procurement Integrity Act prohibits the release of source selection and contractor bid or proposal information (41 U.S.C. 423, implemented at Federal Acquisition Regulations (FAR) 3.104; see also FAR 2.101 for the definition of SSI).

(c) Small Business Innovative Research Data, Limited Rights Data, and Restricted Computer Software delivered under NASA contracts and marked by the contractor with appropriate notices (see FAR clauses 52.227-14 Alternates II and III and 52.227-20). In accordance with paragraph 5.24.3.3., no additional SBU markings need be added to such information received with pre-existing restrictive markings. However, an SBU coversheet (NF 1686) should be added to the source document or materials derived from the source document in accordance with paragraph 5.24.3.4.

[Note: Information/data marked by a contractor with restrictive notices and delivered under a NASA contract should always be reviewed by the Contracting Officer or the Contracting Officer's Technical Representative (COTR) prior to acceptance to ensure that the restrictive markings are authorized by the clause and are justified. In accordance with paragraph (e) of the Rights in Data – General clauses, 52.227-14(e), the Contracting Officer is authorized to challenge any data delivered under a contract if: (1) such data is marked with the notices specified in Alternates II and III (notices indicating the data is either Limited Rights Data or Restricted Computer Software) and use of such notices is not justified, or (2) such data bears any other restrictive or limiting markings not authorized by the contract (e.g., Proprietary). Only the Contracting Officer may authorize the removal of such restrictive notices.]

(5) FOIA exemption 5 information that is most often found at NASA includes predecisional information such as a national space policy not yet publicly released, budgetary data not yet publicly released, pending reorganization plans, and information related to other substantive predecisional policy matters. Information related to the deliberative process, i.e., NASA's internal decision making process used to develop exemption 5 information, is also protectable under FOIA exemption 5. Whether to designate such information as SBU is discretionary and shall be determined in accordance with paragraph 5.24.2.2.a of this NPR.

(6) Information exempt from disclosure under FOIA exemption 6 includes Privacy Act records (5 U.S.C. 552a) and other Personally Identifiable Information (PII), which is addressed in OMB memoranda and guidance. PII is described by OMB as information about an individual maintained by an agency, including education, financial transactions, medical history and criminal or employment history; it also includes information which can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name or biometric records. PII shall always be designated as SBU. Specific requirements and responsibilities for protecting PII are discussed in NASA's Privacy Act Regulations (14 C.F.R. Part 1212), NPD 1382.17G and NPR 1382.1.

f. In addition, certain types of information that do not fall within a particular FOIA exemption may still be sensitive based on the risks and consequences of an unauthorized release. In accordance with paragraph 5.24.2.2.a of this NPR, before designating such information as SBU, the Designating Official should determine that the risks and consequences of unauthorized disclosure outweigh the interest of dissemination and the burden on the Agency of an SBU designation. For information that does not fit within an applicable FOIA exemption as defined above, a program or project office, or Center or Agency organization, may define additional SBU categories of information in its Designation Guide, consistent with the guidelines in this paragraph and paragraph 5.24.2.2.a of this NPR.

#### 5.24.3. Marking Recorded SBU Information

Recorded information in any form (e.g., physical or electronic) that is designated as SBU by the Designating Official, shall be marked by the Originator or Custodian according to the guidelines

of this section so that individuals having access to the SBU information are aware of its sensitivity and protection requirements. The lack of SBU markings on information known by the Holder of such information to be SBU does not relieve the Holder from safeguarding responsibilities. Where an SBU marking is not present on information known or reasonably assumed by the Holder to be SBU, the Holder shall contact the Originator or Custodian (if such Holder is not also the Originator or Custodian) such that a formal SBU determination is made according to the guidelines in section 5.24.2 of this NPR.

#### 5.24.3.1 *SBU Information Covered By Other Protocols*

Wherein marking criteria are established by other statutes, regulations, contractual provisions, NASA directives, etc. (hereinafter, collectively referred to as "Other Directive(s)"), the Originator or Custodian shall mark information, after appropriate analysis and designation protocols as described in section 5.24.2 of this NPR, in accordance with the applicable Other Directive. In other words, where marking criteria/protocols exist in an Other Directive, the marking requirements in this Chapter are not controlling. Markings required by the Other Directive shall be used and no additional SBU markings need be added. However, an SBU coversheet (NF 1686) shall be added in accordance with paragraph 5.24.3.4 of this NPR. Examples of SBU information that may be covered by an Other Directive include the following:

- a. Limited Rights Data, Restricted Computer Software, and SBIR Data received from a contractor (see FAR clauses 52.227-14, Alternates II and II, for marking of Limited Rights Data and Restricted Computer Software, and 52.227-20 for marking of SBIR Data, and NFS clauses 1852.237-72 and 1852.237-73 for marking of other restricted information).
- b. NASA Scientific and Technical Information (STI) (see NPR 2200.2B and NASA Form (NF) 1676).
- c. Information exempted from disclosure by treaty, statute (e.g., Export Administration Regulations (EAR) and International Traffic in Arms Regulation (ITAR)), or other agreements (e.g., a Space Act Agreement).
- d. Privacy Act records and other PII (see NPR 1382.1 for marking requirements and use of NF 1534, Privacy Act Cover Sheet).

#### 5.24.3.2 *SBU Information Not Covered By Other Protocols*

If there is no specific guidance or marking protocol, the Originator or Custodian shall mark the information previously designated as SBU by the Designating Official as described in this section.

- a. SBU information shall be marked, using a minimum of 10 point font, as follows:
  - (1) Mark the bottom of the front cover or first page, as applicable, and each individual page containing SBU information with a notice that includes: the caveat "SENSITIVE BUT UNCLASSIFIED (SBU);" the Designating Official (by name and/or position); the Designating Official's organization, project or program; and date of SBU designation.
  - (2) Mark the top of each individual page containing SBU information with the caveat "SENSITIVE BUT UNCLASSIFIED (SBU)."
  - (3) Materials containing specific types of SBU information (if known) shall be further marked with an applicable caveat (e.g., "SENSITIVE BUT UNCLASSIFIED (SBU) -- SOURCE

SELECTION INFORMATION (SII)," "SENSITIVE BUT UNCLASSIFIED (SBU) – PERSONALLY IDENTIFIABLE INFORMATION (PII)," or "SENSITIVE BUT UNCLASSIFIED (SBU) -- PREDECISIONAL INFORMATION") in order to alert the reader of the type of information conveyed.

b. The following is an example SBU marking for the bottom of the front cover or first page, as applicable, and each individual page containing SBU information:

SENSITIVE BUT UNCLASSIFIED (SBU) -- SOURCE SELECTION INFORMATION (SII)

SBU designation made by John G Doe/Director, NASA HQ Procurement Branch, on Jan 10, 2007.

c. If applicable, identify any automatic decontrol provisions on the front cover or first page, e.g., "Contents may be decontrolled on (date)," or "Content may be decontrolled upon (specific occurrence such as publication of embargoed materials)," or "Content may be decontrolled only by the Designating Official or successor."

d. Where the sensitivity of the information warrants additional access and dissemination restrictions, the Originator or Custodian may cite additional access and dissemination restrictions on the front cover or first page, as applicable. 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.*

e. Computer storage media, i.e., disks, tapes, removable drives, memory sticks, etc. containing SBU information shall be marked "SENSITIVE BUT UNCLASSIFIED (SBU) INFORMATION." Marking of computer storage media is in addition to, not as a substitute for, SBU marking requirements for individual document stored therein.

#### 5.24.3.3. *Information Received with Pre-Existing Markings*

Where information is received from sources external to NASA with pre-existing restrictive markings, the pre-existing restrictive markings shall be maintained (see paragraph 5.24.2.2.e.(4) for information on the NASA's right to challenge restrictive markings on data delivered under a NASA contract). Such information shall be designated SBU and the Originator or Custodian shall carry forward pre-existing restrictive markings from the source documents to any copies or new material derived from the source documents. No additional SBU markings need be added. However, an SBU coversheet (NF 1686) shall be added to the source document or materials derived from the source document in accordance with paragraph 5.24.3.4. See paragraph 5.24.2.2.e.(4) for additional guidance.

#### 5.24.3.4. *Use of SBU Coversheet*

The Holder of SBU information shall use the SBU coversheet, NASA Form (NF) 1686, printed on yellow paper, with SBU information recorded in a physical form in accordance with the following procedures and guidelines:

a. The appropriate box indicating the applicable category of SBU must be checked and the Designating Official's name and organization and the date of the designation must be entered where indicated at the bottom of the form. Use of the form without this information is unauthorized. Documents received without this information on the form should be returned to the originator for proper processing.

- b. When removed from an authorized storage location and individuals without a need-to-know are present, or where casual observation would reveal SBU information to unauthorized individuals, a SBU coversheet shall be used to prevent unauthorized or inadvertent disclosure.
- c. When disclosing, disseminating, or transmitting SBU information in a physical form, a SBU coversheet shall be placed on top of the subject material. The Holder shall populate the NF 1686 and if applicable, may seek counsel from the appropriate Designating Official.
- d. When receiving SBU equivalent information from another government agency, handle the subject material in accordance with the guidance provided by the other government agency. Where no guidance is provided, handle the subject material in accordance with the requirements of this section 5.24.3. If applicable, the Holder may seek counsel from the appropriate Designating Official.
- e. When information is transmitted in an electronic format (e.g., by email attachment) a SBU coversheet may be added by scanning the material and the coversheet into a single document. SBU information transmitted in the body of an email need not include a SBU coversheet, but shall include SBU markings in accordance with paragraph 5.24.3.2 of this NPR and be transmitted in accordance with paragraph 5.24.4.5 of this NPR.

#### 5.24.4. Storage, Access, Disclosure, and Transmittal of SBU Information

The minimum requirements for storage, access, disclosure, and transmittal of SBU information is provided in paragraphs 5.24.4.1 through 5.24.4.5 of this NPR. It is recognized that some types of SBU information may be more sensitive than others and thus warrant additional safeguarding measures above the minimum requirements established in this Chapter. For example, certain types of information may be considered extremely sensitive based on the consequences of an unauthorized release. Such consequences could be increased risk to life or mission essential assets. The Designating Official may add additional control requirements as necessary to afford appropriate protection to such information in an organization's Designation Guide. NASA Civil Servant employees must use sound judgment coupled with an evaluation of the risks, vulnerabilities, and the potential damage to personnel or property as the basis for determining the need for safeguards in excess of the minimum requirements and protect the information accordingly.

##### 5.24.4.1 *SBU Information Covered By Other Protocols*

The protection criteria/protocols in this Chapter are the minimum protections required for SBU information. However, where more stringent protection criteria are established by Other Directives (e.g., NPR 1382.1 for Privacy Act records and other PII and NPR 2190.1 for export controlled information), the information shall be protected in accordance with the applicable Other Directive. In other words, where more stringent protection criteria/protocols exist in an Other Directive, the protection requirements in this Chapter are not controlling. Should there be no such criteria/protocols in the Other Directive, information shall be safeguarded in accordance with requirements for SBU provided in section 5.24.4 of this NPR.

##### 5.24.4.2. *Information from Other Government Agencies with Pre-existing Markings*

Information may be received by NASA employees from other government agencies or international organizations with pre-existing restrictive markings. Other government agencies and international organizations may use different terminology to identify sensitive information, such as "Limited Official Use (LOU)," and "For Official Use Only (FOUO)." In most instances the safeguarding requirements for this type of information are equivalent to SBU requirements

identified herein. However, other agencies and international organizations may have additional requirements concerning the safeguarding of sensitive information. The safeguarding guidance from the other agency or organization should be followed. Should there be no such guidance, the information shall be safeguarded in accordance with the requirements for SBU provided in section 5.24.4 of this NPR.

#### 5.24.4.3. *Storage.*

Holders of information designated SBU shall ensure the proper safeguarding of such information by limiting its access to authorized individuals only and by storing it according to the storage protocols defined below. The identification of an authorized individual is based on a "need to know" analysis in accordance with paragraph 5.24.4.4 of this NPR. The Holder of the subject SBU information shall comply with the following procedures:

a. **SBU Information Recorded in a Physical Form.** A physical form typically includes, but is not limited to, printed paper. SBU information, whether located at a NASA or Contractor facility or removed from the facility (taken off-site), shall either be in the direct control of an authorized individual or, if unattended, stored as described below.

(1) When unattended, SBU information recorded in a physical form shall at a minimum be stored:

(a) in a locked file cabinet,

(b) in a locked desk drawer, a locked overhead storage compartment such as a systems furniture credenza or similar locked compartment, or

(c) in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other individuals without a need-to-know, such as a locked room or an area where access is controlled by a guard, cipher lock, or card reader.

(2) SBU information recorded in physical form shall not be stored in the same container used for the storage of classified information unless there is a correlation between the information. When SBU information is stored in the same container used for the storage of classified materials, the SBU information shall be segregated from the classified materials to the maximum extent possible, i.e. separate folders, separate drawers, etc.

b. **SBU Information Recorded in Electronic Form**

(1). Information Technology (IT) systems that store SBU information shall be categorized at a minimum as FIPS 199 Security Category Moderate and certified and accredited for operation in accordance with federal and NASA standards. Consult NPR 2810.1, Security Information Technology, for detailed information.

(2). SBU information that is stored on laptop computer hard drives and other removable media devices (e.g., memory sticks, CDs) shall be encrypted and such devices shall be stored and protected to prevent loss, theft, unauthorized access and unauthorized disclosure. Storage and control shall be in accordance with NPR 2810.1.

#### 5.24.4.4. *Access and Disclosure*

5.24.4.4.1. *Internal Access and Disclosure.* Access to and disclosure of SBU information shall be to authorized individuals only. An "authorized individual" is one that has both a "need-to-know" in connection with official duties as determined by the Designating Official or designee and an obligation to protect the SBU information. A security clearance is not required for access to SBU information. Whenever SBU information is disclosed, the Holder must be made aware of the following restrictions on access and disclosure:

a. When discussing with or transferring SBU information to another individual, the Holder of the information shall ensure that the individual with whom the discussion is to be held or the information is to be transferred has a valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, or from observing or otherwise obtaining the information. Where there is uncertainty as to a individual's need-to-know, the Holder of the information shall request dissemination instructions from his/her next-level supervisor or his/her appropriate Designating Official.

b. When a "need-to-know" in connection with official duties has been demonstrated, SBU information of which NASA or a NASA contractor is the Originator may be disclosed to any Federal Government employee or current contractor when an obligation to protect SBU information has been incorporated into the contract. Protection obligations shall be incorporated into a NASA contract through NFS clause 1852.237-72 Access to Sensitive Information. Where contractor employees require access to SBU information and the clause is not in a contract, it should be added to the contract or a nondisclosure or confidentiality agreement must be executed in accordance with NASA or Center protocols. NASA employees should consult with the Office of the General Counsel at Headquarters or appropriate Center Office of Chief Counsel in regards to executing nondisclosure or confidentiality agreements.

c. If SBU information will be discussed or disseminated at meetings, the Holder or Custodian of the SBU must ensure that the SBU information is not disclosed to unauthorized individuals and that all copies of materials containing SBU information are accounted for at the end of the meeting. NASA employees should contact the Center Protective Service Office to ensure that meeting rooms provide adequate protection for SBU information.

d. When NASA is not the originating agency, further dissemination of SBU information by the Holder of the information shall be made only with authorization from the originating or designated custodial agency. When information requested or to be discussed originated with another agency, the Holder of the information must comply with that originating agency's policy concerning third party discussion and dissemination.

e. The Holder of the SBU information shall comply with any access and dissemination restrictions cited on the material, provided with the material, or verbally communicated by the Originator, Custodian, or Designating Official. As provided at 5.24.4.1 of this NPR, sensitive information protected by statute or regulation, i.e., Privacy Act, Critical Infrastructure Information, EAR, ITAR, etc., shall be controlled and disseminated in accordance with applicable guidance for that type of information. Where no guidance is provided, the Holder shall handle SBU information in accordance with the requirements of this Chapter.

f. NASA IT Systems containing SBU shall be appropriately protected from unauthorized access. Access shall be granted only after the requisite security investigation, as outlined in chapters 3 or 4 of this NPR, has been accomplished. In addition, security controls shall at a minimum comply with FIPS 199 Security Category Moderate.

g. When discussing SBU information over a telephone, care should be taken to ensure that the conversation is secure from “eavesdropping” by unauthorized individuals, e.g., by using a phone in a private office or non-public area. The use of a STU III (Secure Telephone Unit), or Secure Telephone Equipment (STE), is encouraged, but not required. SBU information shall not be discussed over cell phones.

5.24.4.4.2. *External Access and Disclosure.* Generally, disclosure of SBU information to external recipients (i.e., non-U.S. Federal Government employees and non-U.S. Federal Government contractor employees) is prohibited. However, if a nondisclosure or confidentiality agreement has been executed in accordance to NASA or Center protocols or if a duty of confidentiality has been established (e.g., as per provisions in a grant, cooperative agreement, or Space Act Agreement), SBU information may be disclosed to external recipients. NASA employees should consult with the Office of the General Counsel at Headquarters or appropriate Center Office of Chief Counsel in regards to executing nondisclosure or confidentiality agreements. Further, if none of the above scenarios apply and an ad hoc request for SBU information is made to a NASA employee, the NASA employee shall forward such a request to his/her appropriate FOIA Public Liaison Officer.

5.24.4.5. *Transmittal*

Transmission of SBU information may be made via a variety of transmission methods. Such transmissions shall be made in accordance with the safeguards in this section and only to known recipients. Additionally, the Holder of the SBU information shall comply with any access, dissemination, and transmittal restrictions cited on the material or provided with the material.

a. Transmission of SBU information recorded in a physical form within the U.S. and its Territories. NASA Form 1686, SBU Coversheet, must be attached to SBU information prior to transmission and transmission shall comply with the following procedures:

(1) Material containing SBU information shall be placed in a single opaque envelope or container and sufficiently sealed to prevent inadvertent opening and to show evidence of tampering. The envelope or container shall bear the complete name and address of the sender and addressee, to include program office and the name of the intended recipient (if known).

(2) Material containing SBU information may be mailed by U.S. Postal Service First Class Mail or an accountable commercial delivery service such as Federal Express or United Parcel Service.

(3) Material containing SBU information may be entered into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access, e.g., sealed envelope.

b. Transmission of SBU information recorded in a physical form to Overseas Offices. NASA Form 1686, SBU Coversheet, must be attached to SBU information prior to transmission. When an overseas office is serviced by a military postal facility, i.e., APO/FPO, the Holder of the information may transmit the subject SBU information directly to the office. Where the overseas office is not serviced by a military postal facility, the Holder shall send the subject SBU information through the Department of State, Diplomatic Courier.

c. Transmission of SBU information recorded in electronic form. The Holder of the information shall comply with the following procedures:

(1) Transmittal via fax. The use of a secure fax machine is highly encouraged. However, unless otherwise restricted in accordance with an organization's Designation Guide, SBU information may be sent via nonsecure fax. Where a nonsecure fax is used, the sender shall coordinate with the recipient to ensure that the SBU information faxed shall not be left unattended or subjected to possible unauthorized disclosure on the receiving end.

(2) Transmittal via E-Mail, FTP, and HTTP (Web). Encryption or secure communications systems shall be used when transmitting SBU information via email, FTP, web, etc., to locations outside the Center's firewall, with the following exception. If it is not possible to transmit SBU via appropriately encrypted channels, an explanation of how SBU will be protected during transmission must be addressed in the Master or Subordinate IT Security plan as described in NPR 2810.1, e.g., the information can be included as a password protected attachment with the password provided in a separate transmission. Holders of SBU information shall comply with any email or other electronic transmission restrictions imposed by an organization's Designation Guide. SBU information shall not be transmitted to personal email accounts, due to inherent vulnerabilities.

(3) NASA Internet/Intranet

(a) SBU information shall not be posted on a public NASA website or any other public website.

(b) SBU information may be posted on the NASA Intranet or other government controlled or sponsored protected encrypted data networks. However, the official authorized to post the information should be aware that access to the information is open to all personnel who have been granted access to that particular Intranet site. The official must determine the nature of the information is such that need-to-know applies to all such personnel; the benefits of posting the information outweigh the risk of potential compromise; the information posted is prominently marked as SENSITIVE BUT UNCLASSIFIED; and information posted does not violate any provisions of the Privacy Act or other applicable laws.

(4) Transmittal to network printers. Unencrypted transmission of documents containing SBU information to network printers is only permitted if the network printer and the originating computer are on an internal NASA network behind a NASA firewall. SBU information shall be picked up from printers immediately after sending.

#### 5.24.5. Decontrol and Destruction of SBU

The Designating Official who initially designated the material as SBU, or a successor or designee(s), are the only individuals who can decontrol SBU material.

##### 5.24.5.1. *Continual Decontrol Review*

The Designating Official shall be held responsible for continued review and the prompt removal of SBU designations and restrictive markings when the necessity no longer exists. The establishment of specific protocols (i.e., duration between reviews, authority to decontrol SBU information, etc.) for said review is the responsibility of the Designating Official's organization and may be documented in its Designation Guide. Such decontrol protocols should be reasonably commensurate with the sensitivity of the subject information and the dynamics of the factors used to designate the information as SBU.

##### 5.24.5.2. *Ad Hoc Decontrol Review*

The control status of any information designated as SBU shall be reviewed by the Designating Official upon an ad hoc request by a NASA civil servant employee to whom disclosure has been restricted. A NASA civil servant may make a request for a NASA contractor employee team member if the contractor employee has a need-to-know. Such material shall be decontrolled and disclosed to the requesting NASA civil servant employee unless the Designating Official determines, within a reasonable period of time after the request, that the subject information must remain designated as SBU or a contractor employee does not have a need-to-know. A determination that information containing pre-existing markings must be safeguarded in accordance with SBU protection requirements must be based on the guidelines established in section 5.24.2 of this NPR. If there is a need for a legal interpretation, the Designating Official is highly encouraged to consult with the Office of the General Counsel at Headquarters or appropriate Center Office of Chief Counsel.

#### 5.24.5.3. *Decontrol Markings*

When SBU information is decontrolled, the Designating Official shall do the following:

- a. Redact or order the redaction of any restrictive marking on information designated as SBU by striking out the restrictive markings.
- b. Remove or order the removal of any SBU coversheets attached to the materials,
- c. Include or order the inclusion of a decontrol mark such as, "Decontrolled by the Designating Official, [name or organizational position], on [date]," on the front cover or equivalent of the recorded material.

#### 5.24.5.4. *Destruction*

SBU information must be maintained in accordance with the NASA Records Retention Schedule (NPR 1441.1D). If SBU information or material cannot be decontrolled, excess copies that are no longer needed shall be removed from IT systems, shredded, burned, or destroyed in other similar methods that preclude unauthorized disclosure. Destruction of excess copies may be accomplished by:

- a. "Hard Copy" materials shall be destroyed by shredding, burning, pulping, pulverizing, such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.
- b. Electronic storage media shall be sanitized appropriately by overwriting or degaussing, or non-recoverable encrypted deletion. Contact local IT security personnel for additional guidance.
- c. Paper products containing SBU information shall not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

#### 5.24.5.5. *Disposal of IT Systems Containing SBU*

Refer to NPR 2810.1 for procedural requirements regarding clearing of hard drives, blackberries, personal digital assistant (PDA's), and other storage mediums, prior to disposal or recycling.

#### 5.24.6. *Incident Reporting*

All NASA employees and contractors shall report, without delay, the loss, compromise, suspected compromise, or unauthorized disclosure of SBU information to his/her immediate

supervisor or applicable Designating Official. Incidents involving SBU in NASA IT systems shall be reported to the center IT Security Manager in accordance with IT incident reporting requirements in NPR 2810.1.

5.24.6.1. All NASA employees and contractors shall report, without delay, suspicious or inappropriate requests for information by any means, e.g., email or verbal, to the NASA Center Chief of Security.

5.24.6.2. NASA employees or contractors who observe or become aware of the loss, compromise, suspected compromise, or unauthorized disclosure of SBU information shall report it as soon as possible, but not later than the end of the next duty day, to his/her appropriate Designating Official and the Center Chief of Security.

5.24.6.3. Additional notifications to appropriate NASA management personnel shall be made without delay when the disclosure or compromise could result in physical harm to an individual(s) or the compromise of a planned or on-going operation.

5.24.6.4. At the request of an appropriate Designating Official, an inquiry shall be conducted by the center security official or other designee to determine the cause and affect of the incident and the appropriateness of administrative or disciplinary action against the offender

5.24.7. Administrative Violations and Sanctions.

5.24.7.1. All NASA employees and contractors (when required under their contracts), who have access to SBU, are responsible individually for complying with the provisions of this NPR and may be subject to administrative sanctions if they disclose information designated SBU without proper authorization.

5.24.7.2. Sanctions include, but are not limited to: warning notice, admonition, reprimand, suspension without pay, forfeiture of pay, removal, discharge, or any combination.

5.24.7.3. 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.