



Goddard Procedural Requirements (GPR)

DIRECTIVE NO. GPR 1600.1 **APPROVED BY Signature:** Original signed by
EFFECTIVE DATE: April 3, 2008 **NAME:** Edward J. Weiler
EXPIRATION DATE: April 3, 2013 **TITLE:** Director

COMPLIANCE IS MANDATORY

Responsible Office: Code 240/GSFC Security Division

Title: Goddard Security Requirements

PREFACE

P.1 PURPOSE

This directive establishes security policies and procedures for the Goddard Space Flight Center (GSFC) and its component facilities as required in NPD 1600.2 and NPR 1600.1. It establishes security program standards and requirements necessary to achieve Center-wide security program consistency and uniformity, while allowing reasonable flexibility in implementing risk management principles, where appropriate, at all GSFC facilities. It also describes management security responsibilities.

To ensure that all security requirements are met with minimum disruption to normal activities, this document defines the responsibilities, coordination, and controls to be followed. It describes both routine and emergency operations.

This directive implements the requirements of NPR 1600.1 at GSFC, and is organized such that it follows, chapter-by-chapter, the organization of the first nine chapters of the NPR. Chapter 10 implements NPR 1620.3. Chapter 11 implements NPR 1660.1. Chapters 12 and 13 describe GSFC requirements not currently covered in Agency directives.

P.2 APPLICABILITY

This directive applies to all GSFC personnel, facilities, and activities, including all permanent and temporary sites, and to all GSFC contractors, tenant organizations, tenant contractors, grantees, clubs, visitors, vendors, guests, and/or anyone else doing business or physically on the GSFC or its component facilities, in accordance with applicable law and as directed by contractual, grant, and agreement documents.

GSFC, in the context of this directive, includes the Greenbelt site, the Wallops Flight Facility (WFF), the Goddard Institute for Space Studies (GISS), and the Independent Verification and Validation (IV&V) Facility. Exceptions or special provisions for specific sites are identified in the body of the document.

P.3 AUTHORITY

NPD 1600.2, NASA Security Policy

NPR 1600.1, NASA Security Program Procedural Requirements

P.4 REFERENCES

- a. 5 U.S.C. 552, The Freedom of Information Act
- b. 5 U.S.C. 552a, The Privacy Act of 1974
- c. 49 U.S.C. Chapter 51, Transportation of Hazardous Material
- d. 49 C.F.R. 172.101, Purpose and Use of Hazardous Materials Table
- e. NPD 2530.1, Monitoring Or Recording Of Telephone Or Other Conversations
- f. NPD 9800.1, NASA Office of Inspector General Programs
- g. NPR 1371.2, Procedural Requirements for Processing Requests for Access to NASA Installations or Facilities by Foreign Nationals or U.S. Citizens Who are Reps of Foreign Entities
- h. NPR 1620.2, Physical Security Vulnerability Risk Assessments
- i. NPR 1620.3, Physical Security Requirements for NASA Facilities and Property
- j. NPR 1660.1, Counterintelligence (CI)/Counterterrorism (CT) Procedural Requirements
- k. NPR 7120.5, NASA Program and Project Management Processes and Requirements
- l. GPR 2810.1, Security of Information Technology
- m. GPR 6500.1, Helicopter Landing/Takeoff
- n. GPR 8621.1, Reporting of Mishaps and Close Calls
- o. Standard Form (SF) 86, Questionnaire for National Security Positions
- p. Standard Form (SF) 86C, Standard Form 86 Certification
- q. Standard Form (SF) 312, Classified Information Nondisclosure Agreement
- r. Standard Form (SF) 702, Security Container Check Sheet
- s. NASA Form 699A, Certificate Of Authority To Carry Concealed Firearms
- t. NASA Form 699B, Certificate Of Authority To Carry Unconcealed Firearms
- u. NASA Form 1684, Authorization for Release of Credit Reports
- v. GSFC Form 24-10D, Lost/Missing/Stolen Property Report
- w. GSFC Form 24-12, Key Request/Receipt Form
- x. GSFC Form 24-12A, Keycard Request/Receipt Form
- y. GSFC Form 24-26, Security Work Request
- z. GSFC Form 24-27, Locator and Information Services Tracking System (LISTS) Data
- aa. GSFC Form 24-53, Request for Temporary Badge for U.S. Citizens (Unescorted Access)
- bb. GSFC Form 24-54, Security Technology Transfer Control Plan
- cc. Foreign Travel Debriefing Questionnaire (controlled by CISA; see Chapter 11).

P.5 CANCELLATION

GHB 1600.1A, GSFC Security Manual, dated November 30, 1990

P.6 SAFETY

None

P.7 TRAINING

DIRECTIVE NO. GPR 1600.1
EFFECTIVE DATE: April 3, 2008
EXPIRATION DATE: April 3, 2013

- a. All GSFC civil service employees and contractors shall take the Annual Security Awareness Training, available from the [System for Administration, Training, and Educational Resources for NASA \(SATERN\)](#); and
- b. The Goddard Security Division (GSD) shall administer annual Federal Arrest Authority and Use of Force training to security personnel as described in Section 9.1.

P.8 RECORDS

The table below lists both the records required by this GPR and those required by NPR 1600.1. See P.11 for identification of acronyms. The term “appropriate” in the Record Custodian column means the location appropriate for a given site, e.g., the Greenbelt Security Office as opposed to the Wallops Security Office.

No.	Record Title	Record Custodian	Retention
1	Foreign National (FN) Visitors Files (i.e., copies of passports, visas, permanent resident cards, visit requests, etc.)	Appropriate International Visits Coordinator	* NRRS 1/35 Destroy 2 years after termination of visit.
2	Key Accountability Files – Under Maximum Security	Appropriate GSD key control office	* NRRS 1/99A Destroy 3 years after turn in of key.
3	Key Accountability Files – All Other Areas	Appropriate GSD key control office	* NRRS 1/99B Destroy 6 months after turn in of key.
4	Guard Service Assignment Files	Appropriate security office	* NRRS 1/100A Destroy 3 years after final entry.
5	Guard Service Control Files	Appropriate security office	* NRRS 1/100B Destroy when superseded or obsolete.
6	Classified Documents Inventory Reporting Files	Appropriate Classified Material Control Office	* NRRS 1/101 Destroy when 2 years old.
7	Classified Information Nondisclosure Agreements (SF-312)	Appropriate Personnel Security Office	* NRRS 1/102 Destroy when 70 years old.
8	Personnel Security Clearance Files documenting processing of investigations on Federal employees or applicants, or others who perform work on a Federal agency under contract that requires access to Government facilities or sensitive data.	GSD Personnel Security Office	* NRRS 1/103A Destroy upon notification of death or not later than 5 years after separation or transfer of employee or no later than 5 years after contract relationship expires, whichever is applicable.

DIRECTIVE NO. GPR 1600.1
EFFECTIVE DATE: April 3, 2008
EXPIRATION DATE: April 3, 2013

9	Personnel Security Clearance Files of investigative reports and related papers furnished to agencies by investigative organizations for use in making security/suitability determinations.	GSD Personnel Security Office	* <u>NRRS 1/103B</u> Destroy in accordance with the investigating agency instructions.
10	Personnel Security Clearance Files Index to the Personnel Security Case Files.	GSD Personnel Security Office	* <u>NRRS 1/103C</u> Destroy with related case file.
11	Personnel Security Clearance Status Files Lists, or Rosters maintained in security units showing the current security clearance status of individuals.	GSD Personnel Security Office	* <u>NRRS 1/103D</u> Destroy when superseded or obsolete.
12	GSFC LISTS database – NASA 51 LIST (GSFC Form 24-27)	GSD LISTS Manager	* <u>NRRS 1/104</u> Records are retained for varying periods of time, in compliance with NPR 1441.1 and the Privacy Act System Notice. Contact the Center Records Manager.
13	Identification Credentials Files, including cards, badges, parking permits, photographs, agency permits to operate motor vehicles, and property, dining room, and visitor passes, and any other similar identification credentials.	Appropriate GSD Identification Office	* <u>NRRS 1/105A</u> Destroy credentials 3 months after return to issuing office.
14	Identification Credentials Files Receipts, Indices, Listings, and Accountable Records.	Appropriate GSD Identification Office	* <u>NRRS 1/105B</u> Destroy after all listed credentials are accounted for.
15	Records of Acquisition of Firearms	Appropriate GSD Security Contract Program Manager	* <u>NPRS 1/106A</u> Destroy 1 year after firearm is destroyed or transferred.
16	Certificate to carry firearms (NASA Form 699A and 699B)	Center Chief of Security	* <u>NPRS 1/106B</u> Destroy 1 year after termination of certificate.
17	Firearms data relating to individual qualifications, training, and maintenance of proficiency in the use of firearms.	Appropriate security office	* <u>NRRS 1/106C</u> Destroy 1 year after termination of individual.
18	Facilities Checks (By Guard Force) data sheets, door slip summaries, check sheets, and guard reports on security violations (except copies in files of agency security offices covered elsewhere).	Appropriate security office	* <u>NRRS 1/107A</u> Destroy when 1 year old.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov/gdmsnew/home.jsp> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

DIRECTIVE NO. GPR 1600.1
EFFECTIVE DATE: April 3, 2008
EXPIRATION DATE: April 3, 2013

19	Facilities Checks (By Guard Force) Reports of routine after-hour security checks which either do not reflect security violations, or for which the information contained therein is documented in the files defined elsewhere.	Appropriate security office	* <u>NRRS 1/107B</u> Destroy when 1 month old.
20	Security Violation Files relating to alleged violation of a sufficiently serious nature that are referred to the Department of Justice or Department of Defense for prospective determination, exclusive of files held by those Departments responsible for making such determinations.	Appropriate security office	* <u>NRRS 1/108A</u> Destroy 5 years after close of case.
21	Security Violation Files – All other offices and files, exclusive of papers placed in official personnel folders.	Appropriate security office	* <u>NRRS 1/108B</u> Destroy 2 years after completion of final action.
22	Container Files – Classified Document Security	Appropriate Classified Material Control Office	* <u>NRRS 1/109A</u> Destroy when superseded by a new form or list, or upon turn-in of containers.
23	Container Files – Returnable	Appropriate Classified Material Control Office	* <u>NRRS 1/109B</u> Destroy 3 years after return of container or purchase of container, whichever is applicable.
24	Documents, Accountability/ Inventory Files – Top Secret Documents	Appropriate Classified Material Control Office	* <u>NRRS 1/111A</u> Destroy 5 years after documents shown on forms are downgraded, transferred, or destroyed.
25	Documents, Accountability/ Inventory Files – Classified Documents	Appropriate Classified Material Control Office	* <u>NRRS 1/111B</u> Destroy when 2 years old.
26	Industrial Security Files – Precedent and unusual cases selected by pertinent NASA officials	Appropriate Industrial Security Office	* <u>NRRS 1/113A</u> Destroy after the document to which the classification action applies has been downgraded or declassified by suitable markings
27	Industrial Security Files – All other offices/case files	Appropriate Industrial Security Office	* <u>NRRS 1/113B</u> Destroy when no longer needed, or not later than 3 years after contract is closed/completed.
28	Logs, Registers, and Control Files – Visitors	Appropriate security office	* <u>NRRS 1/114A</u> Destroy 5 years after final entry or date of document, as appropriate.
29	Logs, Registers, and Control Files – Guards	Appropriate security office	* <u>NRRS 1/114B</u> Destroy 2 years after final entry.

DIRECTIVE NO. GPR 1600.1
EFFECTIVE DATE: April 3, 2008
EXPIRATION DATE: April 3, 2013

30	US Citizen Passport Files – Personal Identification or passport photographs	Code 274	* <u>NRRS 1/115</u> Return original to requester, destroy when 5 years old or when superseded or obsolete, whichever is later.
31	Foreign National Files – Personal Identification or passport photographs	Appropriate International Visits Coordinator	* <u>NRRS 1/115</u> Return original to requester, destroy when 5 years old or when superseded or obsolete, whichever is later.
32	Surveys and Inspections of Government-Owned Facilities	Appropriate security office	* <u>NRRS 1/116A</u> Destroy when 3 years old, or upon discontinuance of the facility, whichever is sooner.
33	Surveys and Inspections of Privately-Owned Facilities	Appropriate security office	* <u>NRRS 1/116B</u> Destroy when 4 years old or when security cognizance is terminated, whichever is sooner.
34	Fire, Explosion, and Accident Investigative Files – Precedent or Unusual Cases	Appropriate security office	* <u>NRRS 1/119A</u> Permanent – Retire to FRC when 5 years old. Transfer to NARA when 30 years old.
35	Fire, Explosion, and Accident Investigative Files – Routine Cases	Appropriate security office	* <u>NRRS 1/119B</u> Destroy when 2 years old.

*NRRS – NASA Records Retention Schedules (NPR 1441.1)

P.9 METRICS

The Center Chief of Security (CCS) shall:

- a. Assess physical security, loss prevention, and antiterrorism activities;
- b. Assess and report on the metrics identified in NPR 1600.2;
- c. Assess and report on annual Federal Arrest Authority and annual Security Awareness Training as required by NPR 1600.1; and
- d. Continuously evaluate Center and program-level criticality and vulnerabilities, local threats, and other factors identified in NPR 1600.1, and report changes to the Director of Management Operations.

The above metrics shall be the responsibility of the Goddard Security Division (GSD) and shall be reported annually, in November, at the Director’s Status Review.

P.10 DEFINITIONS

- a. Contractor – A person or entity performing work for or with NASA pursuant to a formal written agreement authorizing personnel and/or equipment to be housed on GSFC premises.
- b. Derivative Classification – The incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov/gdmsnew/home.jsp> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

- c. Employee – an individual working at GSFC as described below:
 - (1) NASA Employee – any civil servant employed by a NASA center or organization, or
 - (2) GSFC Employee – a NASA employee based at GSFC, or any other civil servant employed by a tenant federal organization which has civil servants housed on GSFC property.
- d. Escort – A GSFC employee who has accepted the responsibility for and is required to be with a visitor, guest, vendor, or other non-employee at all times during their visit to the GSFC. With proper notification and coordination, escort duties may be “passed” from one employee to another.
- e. Foreign National (FN) – Any person who is not a citizen of the United States.
- f. GSFC Security Division (GSD) – All civil service employees and contractors assigned to GSFC Code 240, with responsibility for all security-related functions and activities at Greenbelt, WFF, IV&V, and GISS.
- g. GSFC Security Force – Any of the uniformed or plainclothes security officers of the security operations contractor at GSFC.
- h. HAZMAT – Hazardous material, i.e., any substance or material that the Secretary of Transportation has determined is capable of posing an unreasonable risk to health, safety, and property when transported in commerce, and is designated as hazardous under 49 U.S.C. Chapter 51, Transportation of Hazardous Material. It includes hazardous substances, hazardous wastes, marine pollutants, elevated temperature materials, and materials designated as hazardous in the Hazardous Materials Table (see 49 C.F.R. 172.101).
- i. Original Classification – An initial determination that information requires protection, in the interest of national security, against unauthorized disclosure; to ensure such protection, a security classification designation is assigned to signify the level of protection required. Security classification guides are provided by an original classification authority (NASA or other agency) to convey classification guidance.
- j. Physical Security Barrier – Any physical structure, either natural or man-made, which impedes, prohibits, directs, or controls the normal movement or access of personnel or vehicles.
- k. Temporary Badge – An identification pass, which may or may not have a photo of the holder on the face/front of it, issued to any non-employee visiting, working on, delivering to, or otherwise having or conducting official business with the GSFC and/or its employees. Employees, tenants, and contractors may be issued one-day temporary badges when they forget to bring their badges.
- l. Tenant – An organization, or employee thereof, having a formal agreement with NASA to house personnel on GSFC premises.
- m. Vendor – Any company or person who routinely services the GSFC on a regular basis.

- n. Visitor – Any person who is not defined as an employee or contractor, e.g., visiting personnel, guests, vendors, etc.

P.11 ACRONYMS

CCS	Center Chief of Security	ID	Identification
CI	Counterintelligence	IT	Information Technology
CISA	Counterintelligence Special Agent	IVC	International Visits Coordinator
CNSI	Classified National Security Information	IV&V	Independent Verification and Validation Facility
CT	Counterterrorism	LASS	Limited Access Security System
DHS	Department of Homeland Security	LISTS	Locator and Information Services Tracking System
E-PACS	Electronic Physical Access Control System	MOU	Memorandum of Understanding
FMD	Facilities Management Division	NAC	National Agency Check
FN	Foreign National	NASA	National Aeronautics and Space Administration
FOIA	Freedom of Information Act	OIG	Office of the Inspector General
FOM	Facility Operations Manager	PAO	Public Affairs Office
GDMS	Goddard Directives Management System	RVI	Random Vehicle Inspection
GISS	Goddard Institute for Space Studies	SATERN	System for Administration, Training, and Educational Resources for NASA (SATERN)
GSA	General Services Administration	SF	Standard Form
GSD	GSFC Security Division, including security components at WFF, IV&V, and GISS	STTCP	Security/Technology Transfer Control Plan
GSFC	Goddard Space Flight Center, including WFF, IV&V, and GISS	USPP	U.S. Park Police
HAZMAT	Hazardous Materials	WFF	Wallops Flight Facility

PROCEDURES

In this document, a requirement is identified by “shall,” a good practice by “should,” permission by “may” or “can,” expectation by “will,” and descriptive material by “is.”

CHAPTER 1. Introduction and Responsibilities

1.1 Introduction

Chapters 1-9 in this directive correspond to the same chapter numbers in NPR 1600.1. NPR 1600.1 also describes best practices, the processes for requesting waivers and exceptions, and the penalties for security violations.

Chapter 10 of this directive addresses the key, lock, and electronic security controls at GSFC, in accordance with NPR 1620.3. Chapter 11 addresses counterintelligence and counterterrorism at GSFC, in accordance with NPR 1660.1. Responsibilities for chapters 10 and 11 are described in those chapters

of this directive and in their respective NPRs. Chapter 12 addresses the reporting and investigation of security incidents and violations, and describes the associated responsibilities. Chapter 13 describes activities which are unauthorized or restricted at GSFC.

1.2 Responsibilities

Certain individuals and organizations have specific responsibilities for security at GSFC. For chapters 1-9 of this directive, NPR 1600.1 identifies these responsibilities for the following:

- a. Center Director
- b. Center Chief of Security (CCS)
- c. Chief Information Officer
- d. Program Managers, Line Managers, and Supervisors
- e. Individual Employees and Contractors

GSFC employees and contractors shall comply with the requirements of NPR 1600.1, Chapter 1. The following additional responsibility applies:

The Chief Counsel or designee advises the CCS and staff on all legal matters, to include search and seizure, use of force, jurisdiction, constitutional law, evidentiary standards, due process, release of information, and other subjects.

1.3 Waivers and Exceptions

The process for obtaining waivers or exceptions to GSFC's security requirements is as follows:

1.3.1 The program manager, project manager, branch head, or division chief shall submit a waiver request memorandum through the appropriate GSFC directorate office to the appropriate GSD security office. The request shall include:

- a. The reason(s) the waiver is necessary;
- b. A security risk analysis: e.g., cost of implementation; effects of potential loss of capability to the Center; compromise of national security information; injury or loss of life; loss of one-of-a-kind capability; inability of the CCS to perform its missions and goals, etc.; and
- c. An explanation of compensatory security measures implemented in lieu of the requirements to be waived.

1.3.2 The appropriate GSD security office shall either recommend approval or denial to the CCS (or designated local representative). The CCS (or designee) will return the waiver request to the appropriate GSD security office indicating one of the following:

- a. approval,
- b. need for further information, or
- c. denial and closure.

The appropriate GSD security office shall return the waiver request to the initiator.

1.3.3 In the event the waiver is denied, the waiver may be appealed to the Center Director.

CHAPTER 2. Personnel Security Program Requirements and Investigations for Positions Requiring Access to Classified National Security Information (CNSI)

GSFC employees and contractors shall comply with the requirements of NPR 1600.1, Chapter 2. The following additional requirements apply:

2.1 Acceptance of Prior Investigations and Favorable Personnel Security Clearance Determinations From Other Government Agencies and Organizations

An individual seeking GSFC's acceptance of another governmental entity's investigation and/or favorable personnel security clearance determination shall present a completed Questionnaire for National Security Positions ([SF-86](#)) or Standard Form 86 Certification ([SF-86C](#)) and an Authorization for Release of Credit Reports ([NASA Form 1684](#)).

2.2 Suspension of Personnel Security Clearances

The CCS shall suspend an individual's security clearance for 30 days if the security forms for reinvestigation are not returned within 30 days of notification. If after 30 days the forms still have not been completed, the individual's security clearance shall be administratively withdrawn.

CHAPTER 3. NASA Employment Suitability Investigations and Determinations for NASA Employees (No CNSI Access or Security Clearance Required)

GSFC employees and contractors shall comply with the requirements of NPR 1600.1, Chapter 3.

CHAPTER 4. Chapter 4: NASA Personnel Security Program: Risk Designation Process, Background Investigations, and Access Determinations for NASA Contractor Employees

GSFC employees and contractors shall comply with the requirements of NPR 1600.1, Chapter 4.

CHAPTER 5. Classified National Security and Sensitive But Unclassified (SBU) Information Management

GSFC employees and contractors shall comply with the requirements of NPR 1600.1, Chapter 5. The following additional requirements apply:

5.1 Original Classification

When preparing material (e.g., text, graphs, artwork, etc.) based on original research, analysis, data collection, or test results, the author shall review the material for possible classified information. If the content is thought to be classified, an Original Classification Determination is required. Only the CCS and other personnel designated in writing by the Assistant Administrator, Office of Security Programs and Protection, are authorized to make an Original Classification Determination up to the SECRET level. Until this determination is made, the material shall be protected at the classification level thought to be applicable by the author(s). The CCS shall be contacted for questions concerning original classification determinations and procedures.

5.2 Derivative Classification

Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority. Where possible, they should determine whether the paraphrasing, restating, or summarizing of classified information has removed the basis for classification. If checks with the original classification authority, security classification guide, or other inquiries disclose that no classification or a lower classification is appropriate, the derivative document shall be issued as unclassified or classified according to the new level of classification. Where there is disagreement as to the appropriate level of classification required, the CCS shall make the final determination.

5.3 Access to Classified National Security Information (CNSI)

5.3.1 Rank, position, and security clearance of an individual do not, by themselves, entitle an individual access to classified information.

5.3.2 This procedure does not apply to cryptographic information or classified information from a foreign government or international pact organization. Questions about access to cryptographic information shall be referred to the GSD.

5.3.3 Classified information shall never be discussed on unsecured telephones. Classified information shall never be discussed in public places, conveyances, or anywhere within the hearing of an unauthorized person.

5.3.4 Access to classified information from a foreign government or international pact organization shall conform to specialized security requirements established by national policies. Questions about access to classified information from a foreign government or international pact organization shall be referred to the GSD.

5.4 Protecting, Controlling, and Changing Classified Information

- a. Protecting Classified Material During Use – When classified material is in actual use, the material shall be kept under the immediate and continuing control of an authorized person. Personnel shall exercise caution when visitors are present in their area and enforce security clearance, need-to-know, and information requirements related to the work that will be performed. Whenever an unauthorized

person is present, documents shall be covered or turned face down while outside the security container, or placed in a container. Proper storage shall consist of placing the material in a General Services Administration (GSA)-authorized vault or security container with a three-position dial combination lock, and locking the vault or container.

- b. Controlling Access to Security Containers and Their Contents – The custodian of a security safe or container shall define and implement procedures in which the first person opening the security container each day initials the Security Container Check Sheet (SF-702) and annotates the time the safe was opened. Throughout the day, each time the container is opened or closed, the SF-702 shall be initialed and annotated with the time. At close of business, the custodian or the last person having access to the container shall check the container to verify that all materials have been returned to the container and that it is locked. All security containers containing classified material shall be checked daily by the GSFC Security Force, and the SF-702 shall be signed by the security officer making the security patrols.
- c. Security Container Combination Changes – The custodian shall contact the GSD when a combination needs to be changed. Container combinations are changed:
 - (1) At least annually, at the completion of the annual inventory;
 - (2) When a security container account is established;
 - (3) When the list of authorized users changes; and
 - (4) When compromise is suspected.
- d. Changes in Classified Material Custodians – When a change in custodian occurs for any reason, the incoming and outgoing custodians shall conduct a physical inventory of all classified materials. If requested, the GSD may assist with the inventory. After the inventory has been completed and documented, the supervisor of the outgoing custodian shall advise the GSD of the inventory results. All discrepancies shall be resolved promptly. The outgoing custodian may request a copy of any correspondence relating to the inventory and the resolution of discrepancies for his/her records. The GSD shall brief the new custodian about custody control procedures before he/she assumes responsibilities. The list of classified materials shall then be maintained by the new custodian.

CHAPTER 6. Industrial Security Program

GSFC employees and contractors shall comply with the requirements of NPR 1600.1, Chapter 6.

CHAPTER 7. Physical Security Program

GSFC employees and contractors shall comply with the requirements of NPR 1600.1, Chapter 7. The following additional requirements apply:

7.1 Security Controls at GSFC

DIRECTIVE NO.	<u>GPR 1600.1</u>
EFFECTIVE DATE:	<u>April 3, 2008</u>
EXPIRATION DATE:	<u>April 3, 2013</u>

7.1.1 Physical security controls and other measures used for the protection of persons and property shall be the responsibility of and administered by the GSD.

7.1.2 Uniformed Security Force officers shall staff all entrances and gates to the GSFC. Some access entrances and gates have deployable physical security barriers which are controlled by the security officers at that entrance. GSFC facilities, buildings, and projects designated as critical areas or having critical information or personnel shall be controlled by an electronic physical access control system (E-PACS) or a security officer.

7.1.3 All personnel accessing the GSFC shall have and display a valid NASA or GSFC identification badge while on the Center or any of its component facilities.

7.1.4 All vehicles accessing GSFC shall be properly registered and insured in a state of the United States or in a diplomatic entity which is recognized and/or has reciprocity with the state in which the GSFC facility is located.

7.1.5 It is recommended that personnel contact the GSFC Security Operations Center at 6-8661 or the WFF Security Office at 1111 in the event they are going to leave their vehicle on center overnight or for an extended time while on travel or for other reasons.

7.2 NASA/GSFC Photo Identification (Photo-ID) Badge Program

7.2.1 GSD shall use the NASA photo-ID Badge Program as its primary identification system, which will be implemented in phases. At the time of this writing, the NASA photo-ID badges are issued to GSFC civil service employees and contractors, while GSFC-specific badges are used for some functions that will eventually be served by badges in the NASA photo-ID program. When this phase is reached, the use of GSFC-specific badges will be limited to certain events, facilities, functions, or other situations where the NASA photo-ID Badge Program does not apply.

7.2.2 The NASA photo-ID Badge Program is defined in Section 7 of NPR 1600.1. Each NASA photo-ID badge has an indicator showing the center where the holder is employed.

7.2.3 Identification badges issued at the GSFC shall be issued only by the GSD. Non-NASA badges or forms of identification not issued by the GSD are not acceptable identification for access to the Center. If other forms of temporary identification are requested or needed by any GSFC organization, that identification shall be acceptable only if reviewed and approved by the GSD.

7.2.4 GSFC-specific identification badges may designate whether the badge holder has a valid security clearance, or may display a visual access code indicator or authorization.

7.2.5 A GSFC-specific identification badge may but does not always have the badge holder's photograph.

7.2.6 GSFC-specific identification badges are valid and honored only at GSFC, unless other NASA locations or government facilities, at their discretion, choose to recognize them.

7.2.7 Prior to the issuance of a temporary GSFC-specific identification badge to a visitor, one or more of the following criteria shall be met. The notification process, procedures, and names and positions of approving management officials are defined at <http://securitydivision.gsfc.nasa.gov> .

- a. Unannounced/unexpected (i.e., less than 48 hours (two business days) notice) U.S. Citizen visitors shall be escorted by a NASA or GSFC employee or contractor.
- b. U.S. Citizen visitors (for 1 day or longer, up to 6 months) shall be “vouched for” (sponsored) by a valid NASA or GSFC employee or contractor. The Request for Temporary Badge (GSFC Form 24-53) shall be submitted at least 48 hours (2 business days) prior to the visit and approved by the appropriate management official for the length of the visit. Authorized approving officials are defined at <http://internalquicklinks.gsfc.nasa.gov/geninfo/SponsorRespon1007.doc> .

Exceptions to this rule may be allowed by the CCS. If any NASA or GSFC employee or contractor authorized to sponsor a visitor is unable to meet the 48-hour requirement, they may call the GSD to request an exception. Exceptions will only be granted on a case-by-case basis. The following are several examples where the CCS may grant an exception:

- (1) Anything that a Director Of defines as an emergency;
- (2) Parents or others authorized to pick up children, when the employee is unable to pick up their child at the GSFC Daycare Center;
- (3) Authorized employee or contractor is unable to drive due to illness or injury; or
- (4) Unannounced HQ NASA or press meeting.

FN Visitors shall have a NASA or GSFC employee sponsor who completes and submits all appropriate forms and documentation per the NASA Foreign National Management System located at <http://ivan.esportals.com> . The sponsor shall also complete the GSFC Form 24-54, NASA FN Visitor Security/Technology Transfer Control Plan (STTCP), an electronically fillable form which is available on the Goddard Directives Management System (GDMS). All required documentation shall be submitted to the facility International Visits Coordinator (IVC) in sufficient time to comply with NASA FN Visit Requirements (see NPR 1371.2). In addition, each sponsor shall contact their respective IVC, prior to submission of forms, to determine if any additional paperwork is required.

7.2.8 All badges shall be worn and visibly displayed at all times while the badge holder is on GSFC property. Badges shall be worn photo-side visible and above the waist.

7.2.9 No symbol, pin, decal, sticker, or other device may be affixed to any identification badge.

7.2.10 All NASA and GSFC badges are the property of the U.S. Government.

7.2.11 The badge holder shall:

- a. Ensure that the badge is safeguarded at all times;

- b. Ensure that the badge is not defaced or damaged;
- c. Immediately report the loss, theft, duplication, or forgery of any NASA or GSFC-specific identification badge to the GSD;
- d. Challenge anyone seen on the GSFC without a proper, valid NASA or GSFC-specific identification badge, or immediately report that fact to the GSD;
- e. Notify the GSD of any name change;
- f. Surrender the identification badge as described in section 7.3.3.1.

7.2.12 The GSD shall only issue NASA Retiree ID Badges/Cards to civil service employees retiring from the GSFC.

7.2.13 The GSFC-specific identification badges shall be reviewed, redesigned, and reissued at intervals of not more than 5 years.

7.3 NASA Photo-ID and GSFC-Specific Badge Issuance Criteria

7.3.1 GSFC employees and contractors shall be issued a NASA photo-ID and/or GSFC-specific badge. A NASA photo-ID identifies the holder as an official NASA civil servant or contractor. A GSFC-specific badge is not accepted at NASA Headquarters or any other NASA Center.

7.3.2 All FN employees and visitors to the GSFC are issued NASA photo-ID and/or GSFC-specific FN badges by the GSD. GSFC-specific FN badges shall be one of the following:

- a. **ESCORT REQUIRED** – valid for access only with an authorized NASA or GSFC US citizen employee acting as escort, whose attendance to the visitor is mandatory at all times while on Center;
- b. **LIMITED ACCESS** – valid only for access during normal weekday duty hours (6:00 a.m. to 6:00 p.m., Monday-Friday). No weekend or holiday access is authorized, except with prior approval and an escort;
- c. **UNESCORTED/UNLIMITED ACCESS FN VISITOR** – valid for access to the GSFC and its facilities during normal duty hours, after hours, weekends, and holidays. It indicates that the individual has successfully met the security requirements;
- d. **UNESCORTED/UNLIMITED ACCESS FN EMPLOYEE OR CONTRACTOR** – valid for GSFC FN employees or contractors, providing access to the GSFC and its facilities during normal duty hours, after hours, weekends, and holidays. It indicates that the individual has successfully met the security requirements. The individual must be a valid GSFC employee, contractor, tenant employee, grantee, etc.

7.3.3 Badge Confiscation/Recovery Criteria

7.3.3.1 Badges, passes, cards, etc. shall be surrendered:

- a. When no longer authorized or needed, e.g., at the termination of employment at the GSFC;
- b. At the end of a contract or authorized access period;
- c. Upon request by recognized authority, e.g., a member of the GSD staff, a uniformed Security Force officer, or an individual's supervisor or company;
- d. Upon refusal to submit to a Random Vehicle Inspection (RVI) or inspection of personal package(s), briefcase(s), suitcase(s), etc. on Center, except when the inspection requirement or the badge surrender is waived by the CCS;
- e. When it is discovered that an individual has made false statements to obtain access to the GSFC; or
- f. At any other time or situation deemed appropriate by the Center Director or designee, or the CCS.

7.3.3.2. Individuals who surrender their badges may be granted limited access to the Center at the discretion of the CCS. They may be issued a Visitor's Badge and/or may require an escort. If the badge was confiscated for refusal to submit to an RVI, the individual shall consent to a vehicle inspection prior to bringing a vehicle onto GSFC property.

7.3.3.3. In the event an individual's badge is confiscated, the individual shall submit a letter to the CCS requesting the badge be returned and describing the action taken to ensure the event does not reoccur. The request requires concurrence by the individual's Director Of.

7.3.4 Exceptions to NASA photo-ID and/or GSFC-Specific Badging

The following cases do not warrant issuance of a NASA photo-ID or GSFC-specific badge:

- a. Children under the age of 13 are not required to be issued a GSFC-specific identification badge, but may be permitted on GSFC as long as they are sponsored and accompanied by a parent, legal guardian, or other authorized holder of a NASA photo-ID or GSFC-specific badge who has valid access to the Center. Actions of all children granted access under this provision shall be the responsibility of the adult sponsoring the visit.
- b. Vendors (e.g., deliverers of fuel, laundry, vending machine foods, bulk liquid gases like liquid nitrogen, etc.) who do not meet the contract requirements for badge issuance may be permitted access to the GSFC if a specific written request is submitted to the GSD by the requesting organization. The request shall include appropriate justification for "frequent" access, the vendor's name, verification of U.S. citizenship of the "typical" driver(s), frequency of access, and impact if the particular vendor is not permitted "routine" access to the Center. The request will be reviewed and approved, or disapproved with explanation, by the CCS or designee.

Any vendor who routinely services the GSFC on a regular basis, i.e., more than three (3) days a week (e.g., oil deliveries, liquid nitrogen deliveries, UPS, FedEx, vending services, etc.), may be issued a NASA photo-ID and/or GSFC specific badge if they meet the Center's eligibility requirements. Any vendor that does not qualify for a GSFC-specific badge will be badged as a visitor.

- c. Construction contractors and their subcontractors are authorized access by virtue of their contract and the specific authorization of the contracting officer and contracting officer's technical

representative. Only those contractors/subcontractors who will be physically located on the GSFC for the duration of the contract may be issued NASA photo-ID or GSFC-specific badges. All other contractors/subcontractors shall be issued appropriate access badges valid for the duration of the particular function or construction project they are working on. Construction contractors may receive temporary badges valid for up to six months, if they meet the Center's eligibility requirements, and these badges may be renewed with proper authorization.

- d. All service of papers/process shall be coordinated through the GSD with guidance from the Office of Chief Counsel. The GSFC Security Force is not authorized or permitted to accept process service for individuals, companies, or the U.S. Government.
- e. Special Agents and Investigators with valid credentials from other federal agencies conducting non-emergency official business or inquiries on the GSFC may be allowed access to the Center based on their credentials. At the discretion of the GSD, they may be issued a valid GSFC-specific identification badge.
- f. Attendees of special activities, conferences, or other special functions shall obtain and display a "Special Events" badge approved by the GSD, which has the date(s) of activity duration, name or acronym of the activity, and a place for the attendee's or holder's name. The attendee or badge holder shall complete the "name" section and display the badge conspicuously throughout the duration of the event or activity.

7.4 GSFC-Specific Badge Color Coding

7.4.1 The GSFC-specific badge may visually indicate, by color stripe(s) at the top of the badge, the badge holder's suitability standing (see NPR 1600.1, Chapter 3), e.g., whether the individual has completed a favorable National Agency Check (NAC), whether the individual holds a valid security clearance, etc.

- a. **RED** – indicates a security clearance;
- b. **WHITE** – indicates that a favorable NAC or NAC With Inquiries has been completed;
- c. **GREEN** – indicates that NAC paperwork has been submitted to the GSD, but the investigation has not been completed.

7.4.2 A GSFC-specific badge may have a local Access Authorization Code, e.g., EMTG for the Emergency Management Task Group, or WIAD for the Wallops Island Access Designation. These visually indicate an individual's authorization to enter special limited-access areas such as closed, restricted, or controlled areas (see NPR 1600.1), facilities, or buildings.

7.4.3 All GSFC-specific FN badges shall be color-coded as follows:

- a. **RED** – escort required
- b. **YELLOW** – limited access
- c. **GREEN** – unescorted/unlimited access (visitor, employee, or contractor)

In this case, instead of a color stripe, the whole badge is colored.

7.5 Inspection of Persons and Property

7.5.1 All persons, packages, vehicles, deliveries, etc., shall be subject to inspection as a condition of entry to GSFC. Inspections are in accordance with NPR 1600.1.

7.5.2 At Greenbelt, deliveries, packages, containers, etc., shall be processed through Central Receiving prior to being granted access to the Center. No delivery vehicle will be permitted on Center until it has been processed through Greenbelt Central Receiving. **EXCEPTION:** Deliveries that arrive during hours when Greenbelt Central Receiving is not in operation may be pre-approved by the GSD. Contact the GSD for approval procedures.

- a. Deliveries, packages, containers, etc., that meet size requirement for processing through x-ray equipment shall be scanned prior to delivery on Center.
- b. Deliveries, packages, containers, etc., that are too large to fit through x-ray equipment shall be visually scanned and may be checked by Security Force canine detection teams prior to delivery on Center.

7.5.3 At WFF, all deliveries shall report to the WFF Main Gate for inspection during the hours of 8:00 a.m. to 4:30 p.m. They are then processed per a. and b. above.

7.5.4 At GISS and IV&V, all deliveries are processed through security personnel located at the front or rear entrances of the facility.

7.5.5 All deliveries by outside vendors, companies, organizations, etc., who do not have a valid GSFC visitor's badge, shall be met at the GSFC point of entry and escorted by a GSFC employee or contractor.

7.6 Security Areas

Security Areas are described in NPR 1600.1. All requests and requirements for designation of security areas on the GSFC shall be processed through the GSD.

7.7 Facility Security

7.7.1 GSD shall conduct a Physical Security Vulnerability Risk Assessment on each major building at GSFC annually, as a minimum, or if the building usage requirements change. Requirements are specified in NPR 1620.2.

7.7.2 A representative from GSD shall be part of and involved in all new construction projects, major renovations of facilities or buildings, and/or organizational renovations, moves, or reorganizations. New construction and renovations shall comply with security requirements as defined by GSD for locks and locking devices, master key systems, E-PACS devices, and other security requirements as defined or developed for the construction or renovation project.

DIRECTIVE NO.	<u>GPR 1600.1</u>
EFFECTIVE DATE:	<u>April 3, 2008</u>
EXPIRATION DATE:	<u>April 3, 2013</u>

7.7.3 GSFC facility construction projects, renovations, repairs, or other facilities projects shall meet the physical security standards and requirements as defined by GSD for fences, locking devices, key systems, E-PACS devices, security alarms, building-to-parking lot or roadway setbacks, etc., for protection of personnel, property, equipment, resources, etc.

7.7.4 GSFC key control procedures implement the requirements of NPR 1620.3, and are described in Chapter 10 herein.

7.8 Flight and Launch Site Security

7.8.1 All GSFC aircraft and other flight operations (balloons, unmanned aerial vehicles, rockets, etc.) shall comply with the requirements of NPR 1600.1, NPR 1620.2, and NPR 1620.3.

7.8.2 All GSFC directorates involved in suborbital flight and rocket launch operations shall coordinate with the appropriate security office to ensure that documented procedures are in place to meet the requirements of NPR 1600.1, NPR 1620.2 and NPR 1620.3 for all flight missions.

7.8.3 All GSFC sites shall have appropriate plans and procedures for landing and takeoff of emergency assistance aircraft, e.g., helicopters, at or near the facility, for emergency medical evacuations or other emergency situations. At Greenbelt, the requirements are specified in GPR 6500.1.

Other GSFC facilities shall have their own arrangements or established procedures with local emergency officials for landing and takeoff of emergency assistance aircraft. WFF has an established airfield onsite. The WFF Security Office shall be responsible for all airfield and aircraft security matters on the WFF airfield.

7.9 Control and Issuance of Arms, Ammunition, and Explosives

7.9.1 No one may possess firearms (e.g., handguns, rifles, machine guns, shotguns, and ammunition) or other intermediate levels of force devices (e.g., Oleoresin Capsicum spray (pepper spray), tear gas and batons) on GSFC property except as follows:

- a. NASA employees or contractors who hold NASA Headquarters certifications to possess firearms;
- b. Employees of other federal agencies who are authorized and required by their agency to carry firearms in the performance of their duties; and
- c. State and local law enforcement officers required to be armed in the performance of their duties.

7.9.2 At Greenbelt and WFF, the Security Force may use detection devices and/or canine detection teams to perform routine inspections, RVIs, delivery inspections, and package inspections. In addition, the Security Force may respond to all incidents, threats, or reports of firearms, ammunition, or explosives violations on those facilities.

DIRECTIVE NO.	<u>GPR 1600.1</u>
EFFECTIVE DATE:	<u>April 3, 2008</u>
EXPIRATION DATE:	<u>April 3, 2013</u>

7.9.3 Certain GSFC organizations may be required to store, maintain, and handle explosives in the performance of their duties. Organizations at GSFC who deal with arms, ammunition and/or explosives, electroexplosive devices, pyrotechnic devices, and propellants, including rocket fuel and motors, shall provide the GSD a list of the types of these explosives, locations where stored, and a list of all personnel who use or transport them in the performance of their duties. The list will include individuals' names, organization codes, phone numbers, types of explosives to be used, location, name of mission(s) supported, and storage locations of explosives. Applicable organizations at both Greenbelt and WFF shall update this list quarterly and submit to their respective security offices.

7.10 Standards for Secure Conference Rooms

At Greenbelt, there is a certified secure conference room as required in NPR 1600.1. It is under the control of the HQ NASA/OSPP Counterintelligence (CI) Section.

7.11 Threat and Incident Reporting

All incidents of threats, thefts, crimes or suspected criminal activities, emergencies, serious injuries, fires, etc. on GSFC or NASA facilities, except IT Security incidents, shall be reported to the GSD. This is in addition to the mishap reporting requirements of GPR 8621.1. Refer to GPR 2810.1 for Information Technology Security incident-handling procedures.

Examples of reportable incidents are:

- possible espionage,
- possible sabotage,
- suspected terrorist activities,
- bombing incidents (including bomb threats),
- shootings or other violent acts,
- destruction of NASA facilities, property, or equipment,
- death or serious bodily harm requiring hospitalization,
- threats against NASA property, missions, or personnel,
- information regarding concealment of firearms, explosives, or implements of war,
- information regarding individuals appearing to act irrationally in efforts to contact NASA or other high officials in the U.S. Government.

Any GSFC employee or contractor who observes any incident involving fraud, waste and/or abuse shall report it to the Office of the Inspector General (OIG), as required by NPD 9800.1.

7.12 NASA Security Office Special Agent Badges and Credentials

- a. At GSFC, NASA Security Office Special Agent badges and credentials shall be issued only to individuals in the GSD identified by the CCS.

DIRECTIVE NO.	<u>GPR 1600.1</u>
EFFECTIVE DATE:	<u>April 3, 2008</u>
EXPIRATION DATE:	<u>April 3, 2013</u>

- b. NASA Security Office Special Agent badges and credentials issued by NASA Headquarters to individuals from other NASA Centers are valid and carry the same authorizations while on GSFC property.

7.13 Technical Surveillance Countermeasures

Technical Surveillance Countermeasures support shall be provided by the GSD Counterintelligence Section and coordinated through NASA Headquarters' Director, Security Management Division.

7.14 Dealing with Demonstrations

All planned or impromptu demonstrations or strikes/informational labor picketing at any GSFC location, that affect NASA interests, shall be reported to the GSFC Security Force as soon as they become known.

The GSFC Security Force will respond to all such incidents, and set up an incident command post, establish perimeter access control at the point of the incident, and notify the GSFC Office of Public Affairs (PAO) and/or the GSFC Industrial Security Officer.

7.15 Threat Condition (THREATCONS)

7.15.1 GSFC shall use the Department of Homeland Security (DHS) color codes to identify Threat Conditions at GSFC. Threat Conditions are:

- a. **THREATCON GREEN** – applies when there is no or an unspecified threat of possible terrorist activity against personnel and facilities.
- b. **THREATCON BLUE** – applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable.
- c. **THREATCON YELLOW** – applies when an increased and more predictable threat of terrorist activity exists.
- d. **THREATCON ORANGE** – applies when an incident occurs or intelligence is received, indicating that some form of terrorist action against personnel and facilities is imminent.
- e. **THREATCON RED** – applies in the immediate area where a terrorist attack has occurred, or when intelligence has been received that terrorist action against a specific location or person is likely.

7.15.2 GSFC will generally follow and protect to the Threatcon level established by NASA Headquarters. In the event of an increase in the level by the DHS, GSFC shall protect at the level designated by DHS, absent further or additional guidance from NASA Headquarters. The GSD, with approval of the Center Director, may decide to protect at a level higher than that published nationally, but shall not protect at a level less than that determined by NASA Headquarters.

7.16 Hazardous Material (HAZMAT) Security

7.16.1 All HAZMAT brought to or transported on the Greenbelt facility shall be processed through Central Receiving and the security checkpoint for deliveries in the Building 16W Warehouse. HAZMAT deliveries made to the Greenbelt Facility after Central Receiving is closed may, with prior

DIRECTIVE NO.	<u>GPR 1600.1</u>
EFFECTIVE DATE:	<u>April 3, 2008</u>
EXPIRATION DATE:	<u>April 3, 2013</u>

approval, be processed by GSFC Security Force personnel upon arrival. Contact the GSD for approval procedures.

HAZMAT deliveries to WFF shall report to the WFF Main Gate for inspection Monday through Friday only, excluding holidays, during the hours of 8:00 a.m. to 4:00 p.m.; others will be turned away unless other arrangements are made in advance. IV&V and GISS do not receive HAZMAT.

7.16.2 All HAZMAT carrier vehicles shall be inspected by a member of the GSFC Security Force.

7.16.3 All HAZMAT deliveries made directly to the Greenbelt facility or WFF shall be escorted by a NASA or GSFC employee or contractor of the organization receiving the shipment, or shall have prearranged for a Security escort.

7.16.4 HAZMAT shall be stored, maintained, and used in such a manner as to prohibit access and/or use by unauthorized personnel. Storage containers and facilities housing HAZMAT shall be protected with appropriate access control devices (e.g., E-PACS or restricted locks and keys), blast- or explosive-resistant barriers, fences, etc., to ensure that only authorized personnel have access and that accidental explosion, disbursement, and/or contamination is contained.

CHAPTER 8. Program Security

GSFC employees and contractors shall comply with the requirements of NPR 1600.1, Chapter 8. The following additional requirements apply.

8.1 Major functional organizations within Code 100 and directorates shall each designate a Security Program Manager to coordinate the implementation of the requirements of this GPR within their organizations. Similarly, GSD may require organizations owning or responsible for certain special facilities to designate a Facility Security Manager with similar responsibilities. Names and contact information for Security Program Managers and Facility Security Managers shall be provided to GSD by the responsible organizations and shall be maintained up to date.

8.2 Program and project managers shall coordinate with the appropriate GSFC Security Office, prior to the implementation of the program or project, to ensure that the security requirements of NPR 7120.5 are met. This should ensure that security requirements and provisions are identified as early as possible and reflected in program and project plans. Older programs and projects having program/project plans approved before these security requirements were defined in NPR 7120.5 shall coordinate with the appropriate GSFC Security Office and document the security requirements in a program- or project-level directive.

8.3 No information system can process classified information until a System Security Authorization Agreement is in place. A requestor acquires this approval through their management and the Center Director. The Center Director's approval then allows Security to proceed and provide the necessary Certification and Accreditation (see NPR 1600.1) of the information system.

The procedure is described below:

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov/gdmsnew/home.jsp> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

DIRECTIVE NO.	<u>GPR 1600.1</u>
EFFECTIVE DATE:	<u>April 3, 2008</u>
EXPIRATION DATE:	<u>April 3, 2013</u>

- a. The program, project, or other requesting organization submits a request memo to the CCS describing what kind of classified information they need to process, why they need to process it, and the computer system or network proposed for the activity.
 - The requesting organization should not purchase/acquire computer equipment prior to receiving CCS's recommendations.
 - The request memo requires Division-level approval.
- b. If the CCS approves the request, he/she routes it to the Center Director for approval.
- c. If approved by the Center Director, the CCS performs the Certification & Accreditation Process.
- d. This results in a System Security Authorization Agreement.

CHAPTER 9. Federal Arrest Authority and Use of Force Training and Certification

GSFC employees and contractors shall comply with the requirements of NPR 1600.1, Chapter 9. The following additional requirements apply.

9.1 Responsibilities

Federal Arrest Authority and Use of Force training and certification shall be administered and controlled by the GSD. The CCS shall be responsible for compliance of the program with the requirements of NPR 1600.1.

9.2 Law Enforcement Jurisdiction, Response, and Support

9.2.1 With the exception of one small tract of land to the west of the Baltimore-Washington Parkway, the Greenbelt facility has exclusive federal jurisdiction; therefore, State and local law enforcement agencies have no law enforcement jurisdiction on the vast majority of the facility. GSFC shall seek to maintain a Memorandum of Understanding (MOU) with the U.S. Park Police (USPP) to provide law enforcement support at/on the Greenbelt facility when requested. When called, USPP has law enforcement authority as stated in the MOU and will work with GSD representatives and the GSFC Security Force to the successful conclusion of the incident or situation.

9.2.2 The WFF facility, depending on the specific location, has either exclusive federal jurisdiction or concurrent jurisdiction with local and state law enforcement agencies. GSFC shall seek to maintain an MOU similar to that described in 9.2.1 with local and state law enforcement agencies to define authority and responsibility for responding to incidents, situations, demonstrations, etc..

9.2.3 The IV&V facility is part of the University of West Virginia and is located on state land. GSFC shall seek contractual arrangements with UWV to define authority and responsibility for responding to incidents, situations, demonstrations, etc.

9.2.4 The GISS facility is located in a GSA facility. GSFC shall seek to maintain an MOU similar to that described in 9.2.1 with GSA to define authority and responsibility for responding to incidents, situations, demonstrations, etc..

CHAPTER 10. LOCKS, KEYS, AND ELECTRONIC SECURITY SYSTEMS

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov/gdmsnew/home.jsp> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

This chapter implements the lock and key control requirements of NPR 1620.3.

10.1. GENERAL

Lock, key and electronic security systems requirements have been established at each GSFC site to protect areas, safeguard pilferable materials and supplies from unauthorized access, and prevent unauthorized disclosure of sensitive, restricted, or classified information.

All areas and materials that require protection as described above shall be secured through the application of security measures such as locking mechanisms, electronic security systems, or other “industry standard” locking devices. Keys, keycards, and access control devices shall be issued only to authorized individuals who require access to the controlled areas. Keys and combinations to locking mechanisms shall be limited to the minimum number of individuals necessary.

10.2. RESPONSIBILITIES

In addition to the responsibilities identified in NPR 1620.3, the following additional responsibilities are identified for key, lock, and electronic security systems.

10.2.1 GSD

The GSD shall be responsible for establishing and maintaining the program for keys, locks, and electronic access controls and ensuring uniform implementation throughout the GSFC.

10.2.2 Supervisors

Supervisors shall be responsible for approvals and ensuring that only authorized personnel are issued access control devices, e.g., keys and keycards. See 10.3 for other approval requirements.

10.3. KEY, LOCK, AND ELECTRONIC SECURITY SYSTEM CONTROLS

10.3.1. Key and Lock Systems

The GSFC Key and Lock System consists of two components:

- a. Limited Access Security System (LASS) – Used to protect special areas and functions designated by the GSD. Keys to areas protected by a LASS are absolutely restricted to the individual user(s) and the GSD staff.
- b. Building System – Used to protect general offices, suites, laboratories, and areas not designated or protected under a LASS. Keys to areas protected by the Building System are issued to those needing access in the course of their daily duties and only to the level required for the conduct of their assigned responsibilities.

Only locking mechanisms approved by the GSD will be authorized for these purposes. The number of individuals authorized to receive or retain keys and lock combinations shall be kept to the minimum necessary.

10.3.2 Master Keys

Master Keys shall be strictly controlled. Master Keys include Building Grand Masters, Building Sub-Masters, Area and Suite Masters, LASS Masters, and Special Area Masters. The following apply at Greenbelt and WFF, but not at IV&V or GISS.

- a. Building Grand Masters – Building grand master keys shall be issued only to personnel with a direct need for Center-wide access in the performance of official duties. Requests for issuance shall come from the appropriate directorate through the Director of Management Operations to the GSD, and shall include a complete justification of the need.
- b. Building Sub-Masters – Sub-masters are for individual buildings and will be issued to the respective Facility Operations Manager (FOM). Other persons requiring sub-masters in the performance of official duties shall forward a written request, through the appropriate directorate and FOM, to the CCS for approval. The request shall include a complete justification of the need for the key.
- c. Area and Suite Masters – Requests for these keys shall be submitted to the GSD through the appropriate Division Chief or Branch Head responsible for the suite or area.
- d. LASS Masters – LASS masters shall be issued only to security personnel with approval of the CCS.
- e. Special Area Masters – Janitorial storage areas and mechanical or electrical equipment room keys shall be requested through the Chief, Facilities Management Division (FMD). Telephone closet keys shall be requested through the Information Technology and Communications Directorate.

10.3.3 Obtaining Keys and Locks

- a. Acquisition – The GSD controls locks, security containers (i.e., safes), combinations, and keys. All requests for the purchase of locks, locking devices, locking security containers (i.e., safes), electronic security controls, alarms, etc., through small purchases, store stock purchases, or "mass" purchases, require approval by the GSD to ensure compatibility with existing control systems and locking procedures.

(1) Padlocks and Keys – All requests to purchase padlocks and keys require approval by GSD. Equipment and materials shall be secured in accordance with NPR 1600.1 and NPR 1620.3. Individuals responsible for areas with a need for padlocks and keys shall contact the GSD for more specific guidelines and requirements.

(2) Cipher Locks – Cipher locks are not generally used at GSFC. However, the GSD may approve the use of cipher locks for areas or rooms with special security needs, or which meet unique security circumstances and cannot feasibly be secured in any other manner. Individuals responsible for areas with a need for a cipher lock shall contact the GSD for more specific guidelines and requirements.

- b. Issuance – Keys and keycards shall be issued only to authorized individuals with a valid need for access into a room, facility, or area. All locks, keys, keycards, locking devices, and other such items intended to control access on the Center or its facilities shall be issued through the GSD. Requests for keys or keycards shall be made using the Key Request/Receipt Form (GSFC Form 24-12) or Keycard Request/Receipt Form (GSFC Form 24-12A), and routed to the appropriate GSD key control office through the appropriate Branch Head or approving official. After a 24-hour delay for the key control office to verify the information, the key control office will notify the requestor(s) that the key(s) or keycard(s) is (are) ready for pick up.

At WFF, the GSFC 24-12 or 24-12A shall be routed to the Wallops Security Office through the appropriate FOM, Facility Security Manager, or other approving official. In order to receive a key or keycard at WFF, personnel must have a NASA or GSFC-specific badge.

Requests not submitted to the key control office within 30 days of the authorizing signature date will be canceled. Inquiries regarding specific requirements for obtaining keys and keycards shall be directed to the key control office.

IV&V and GISS will develop their own procedures, and provide a copy of those procedures to the GSD.

- c. Installation or Replacement – All requests for the installation or replacement of locks, locking devices, or access control systems (whether for new construction, renovations, or other reasons) shall be processed through the GSD using a Security Work Request (GSFC Form 24-26), to ensure compatibility with existing control systems and locking procedures.

(1) Desks and File Cabinets: The GSD will provide replacement locks and keys for desks, file cabinets, and other similar containers on a limited basis, as available.

(2) Doors: The GSD will provide or replace locks and keys for doors as available on rooms or areas requiring access controls, except for new construction or renovations contracted through the FMD, for which the GSD will only provide keys.

(3) Repair of Defective Locks/Knobs: The GSD coordinates locksmith repairs of defective locks and knobs.

10.3.4 Electronic Security Systems

Several types of electronic security systems are used on the GSFC. These systems are monitored at Greenbelt by the GSD on a 24-hour basis to protect classified information or material, IT resources,

DIRECTIVE NO.	<u>GPR 1600.1</u>
EFFECTIVE DATE:	<u>April 3, 2008</u>
EXPIRATION DATE:	<u>April 3, 2013</u>

Mission Control Centers, valuable property, or other sensitive areas requiring controlled and/or monitored access. At WFF, they are similarly monitored by the Emergency Operations Center. These systems are available through the GSD to all GSFC organizations with security needs requiring this level of protection.

- a. Reports of access requested by organizations for areas under their control will be reviewed and approved by the GSD prior to being released to the requesting organization.
- b. Specific questions regarding alarms and activations should be directed to the GSD.

10.3.5 Installation and Maintenance of Security Systems

All installations and repairs of security systems shall be requested through the GSD using a Security Work Request (GSFC Form 24-26). The GSD will determine if the system is required and coordinate authorized installation and maintenance of the equipment. Such systems shall comply with the National Fire Protection Association code and the International Building Code.

10.3.6 Security of Locking Mechanisms

- a. All controlled keys and keycards shall be requested using the GSFC Forms 24-12 and 24-12A, respectively. No markings or special codes will be placed on GSFC keys by users or others, except as issued by the GSD. Keys, keycards, and locking mechanisms may be transferred or duplicated only by the GSD. Keys which are no longer needed or no longer in use shall be returned to the GSD immediately upon removal of need or use.
- b. Padlocks shall not be left in an open position while on a hasp or in storage. Padlocks shall be relocked after opening to prevent lock substitution.

10.3.7 Reporting Loss/Theft of Keys and Keycards

Employees and contractors shall be responsible for protecting keys, keycards, and locks entrusted to them from damage, loss, or theft. When keys, keycards, and/or locks are discovered missing as a result of theft, negligence, or other loss, the missing item shall be reported immediately to the GSD.

The reporting individual shall then complete a Lost/Missing/Stolen Property Report (GSFC Form 24-10D), which can be obtained on GDMS. The individual shall obtain authorization for replacement on the GSFC Form 24-10D and submit it to the GSD. The authorizing official for civil servants is the appropriate Division Chief or the authorizing official of the location or facility they are assigned to, and for contractors it is the COTR.

There may be a waiting period before keycard replacement to allow for possible return by mail.

10.3.8 Requesting Security Work

DIRECTIVE NO.	<u>GPR 1600.1</u>
EFFECTIVE DATE:	<u>April 3, 2008</u>
EXPIRATION DATE:	<u>April 3, 2013</u>

Security work (e.g., lock and alarm installations, rekeying, lock and safe repairs, keycard installations, or other security work) shall be requested on a Security Work Request (GSFC Form 24-26). Inquiries regarding specific requirements for completing security work requests shall be directed to the GSD.

10.3.9 Locking Security Containers

The GSD shall be responsible for the accountability, placement, and maintenance of all locking security containers, safes, vaults, media storage containers, and areas or doors secured with combination locks. All requests for locking security containers for the storage of classified or sensitive material, the movement or placement of containers, maintenance of or combination changes for containers or locks, or procurements of locking security containers shall be coordinated with and approved by the GSD. The GSD can, on a limited basis, provide a locking heavy-duty security container or vault with a 3-position dial combination lock approved for the storage of classified material. When this type of container is used for storage of classified material, the combination shall be changed at least annually.

CHAPTER 11. Counterintelligence and Counterterrorism

11.1 General

GSFC employees and contractors shall comply with the requirements of NPR 1660.1. The following additional requirements apply.

11.2 Responsibilities

11.2.1 The GSFC Counterintelligence Special Agent (CISA, described in NPR 1660.1) shall:

- a. Establish and conduct annual counterintelligence/counterterrorism (CI/CT) awareness briefings to employees and contractors;
- b. Provide updated threat assessments, as appropriate;
- c. Prepare or coordinate and provide CI and CT threat analysis products for GSFC technologies, facilities, and programs;
- d. Coordinate Intelligence Information Reports developed by GSFC CI/CT resources with the CI/CT and intelligence communities; and
- e. Maintain a Foreign Travel Debriefing Questionnaire form and provide it per 11.2.3.

11.2.2 Program and project managers shall, in addition to the responsibilities listed in NPR 1600.1, be responsible for coordinating with the CI/CT Office to schedule annual CI/CT awareness training for employees and contractors.

11.2.3 Employees and contractors shall:

- a. Report to the CISA all suspicious unsolicited requests from FNs via any means (electronic mail, postal mail, telephone, fax, in-person, etc.) wherein the FN is soliciting government or other sensitive information;
- b. Report any individual who may exhibit any of the behavior(s) listed in Appendix A, Espionage and Terrorism Indicators, which the employee or contractor deems suspicious and worthy of reporting;
- c. Obtain a Foreign Travel Debriefing Questionnaire from the Center CISA, and, upon return from overseas travel, complete it and return it to the CISA; and
- d. Receive annual CI/CT awareness training.

CHAPTER 12. Security Investigations

12.1 General

The GSD is authorized to conduct security investigations into any reported or observed security incident or security violation that involves the personal security or welfare of any individual at GSFC, the loss or theft of any government or privately owned property, or the security of any NASA asset, building, or property at any GSFC facility or geographically separated location(s).

12.2 Scope

The GSD shall review each reported security incident or security violation and determine the need for further investigation. Decisions to investigate security incidents or violations will be made after consideration of applicable Federal and state laws and consistent with designated GSD and OIG investigative responsibilities.

12.3 Responsibilities

- a. GSD – The GSD shall be responsible for conducting investigations of security violations and security incidents, which includes investigating, evaluating, recommending administrative action, and taking appropriate law enforcement action. The GSD shall also be responsible for maintaining the security and confidentiality of all reported or obtained investigative information.
- b. Supervisors – All supervisors shall advise their employees and contractors of their duty to cooperate with GSD investigative efforts.
- c. Employees and contractors – Employees and contractors shall be responsible for immediately reporting all security incidents (see Section 7.11) to the GSD. Employees and contractors shall cooperate with all GSD investigations into security incidents, and provide any requested assistance and relevant information to authorized investigators.

12.4 Reporting

Information received and documented in a GSD investigative report often involves personal data and law enforcement information that is sensitive in nature, the release of which may be limited or prohibited by Federal laws, such as the Privacy Act and Freedom of Information Act (FOIA). Privacy Act requests for documents by personnel with an official need to know the information, as well as

requests by employees seeking information about themselves, shall be submitted to the CCS. Other requests for GSD documents under the FOIA shall be submitted to the Center FOIA Office.

Once an investigative report is released to an individual, that person shall not share it with others, even those with a legitimate need to know, unless specifically approved by the CCS.

CHAPTER 13. Unauthorized or Restrictive Activities

The following are unauthorized or restricted activities at GSFC or any of its locations:

13.1 Possession of Firearms or Weapons

Firearms and other dangerous weapons (including, but not limited to saps, numchucks, knives over 3 inches, explosives) are prohibited on the GSFC with the following exceptions:

- a. Firearms in the possession of GSD personnel in the performance of their official duties;
- b. Knives solely used for culinary purposes or for purposes required in the performance of official duties;
- c. Weapons in the possession of state or local law enforcement officers or other authorized officials as required by the GSD and as described in section 7.9.1; and
- d. Explosive items as described in section 7.9.3.

The sale or transfer of weapons on the Center is prohibited.

13.2 Possession of Contraband and Drugs and Consumption of Alcoholic Beverages

The possession of contraband, i.e., goods or materials that are illegal to possess, is prohibited on the GSFC. Illegal drugs (as defined by the Drug Enforcement Administration) are prohibited on any GSFC location. Persons prescribed narcotic-type medical drugs shall carry them in approved containers with a valid prescription label affixed to the container. Alcoholic beverages may be served by and consumed at the Greenbelt Recreation Center and WFF Rocket Club, and at other Greenbelt and WFF locations upon approval of the appropriate Division Chief during non-duty hours with notification to GSD for safety and security purposes. Driving under the influence of alcohol or illegal drugs is prohibited. Transportation of open containers of alcoholic beverages shall comply with the laws of the surrounding local jurisdiction.

13.3 Intoxicated Individuals

Entering the GSFC or operating a motor vehicle on GSFC property at any GSFC facility, while under the influence of intoxicating beverages or drugs, is prohibited. Individuals determined to be intoxicated will be denied entrance or removed/escorted from the GSFC, as the situation warrants. If already on

DIRECTIVE NO.	<u>GPR 1600.1</u>
EFFECTIVE DATE:	<u>April 3, 2008</u>
EXPIRATION DATE:	<u>April 3, 2013</u>

GSFC, their keys and badges may be confiscated, law enforcement officials may be called, and they may be removed or escorted from the GSFC, as the situation warrants. Keys will be returned when the individual meets the legal requirements to drive.

13.4 Hunting and Fishing

There is NO hunting allowed at GSFC.

At Greenbelt, fishing is restricted to members of the GEWA Fishing Club and only under approved club rules. At WFF, fishing is prohibited on Wallops Island during WFF launch operations and on the Main Base at all times. Fishing is permitted on Wallops Island at other times by individuals with a NASA photo-ID or GSFC-specific badge. No fishing permit is required to fish on Wallops Island; State of Virginia laws apply.

13.5 Ice Skating

There is no ice skating allowed at GSFC.

13.6 Photographic and Recording Equipment

The possession and use of photographic, video, and/or recording equipment on GSFC is controlled within Restricted, Limited or Closed Areas (as defined in NPR 1600.1). Employees, contractors, visitors, and others desiring to record or photograph within these areas shall coordinate with and obtain approval from the appropriate Division Chief or person in charge of the area where the recording or photographing activity is to take place before the activity can be permitted.

Use of photographic, video, and/or recording equipment shall comply with NPD 2530.1. Operation of photographic, video, and/or recording equipment shall be in an open, public manner so that all personnel involved are aware of its use and function. Approval of the Chief Counsel or his designee shall be obtained prior to use of any video or audio recording device whose use is not open and known and clearly disclosed to personnel being recorded (e.g., surveillance activities). Custodians of classified material and technical monitors of classified tests and operations are responsible for ensuring that classified materials and/or information are protected from unauthorized disclosure through recording or photographic activities.

Official news media personnel may carry photographic, video, and/or recording equipment on the GSFC, except in areas where prohibited, provided they are escorted by an authorized representative of the PAO. It is the responsibility of the PAO escort and/or the person visited, interviewed, or photographed to ensure that no unauthorized photographs or recordings are made and that there is no compromise of classified information.

13.7 Gambling

DIRECTIVE NO.	<u>GPR 1600.1</u>
EFFECTIVE DATE:	<u>April 3, 2008</u>
EXPIRATION DATE:	<u>April 3, 2013</u>

Employees shall not conduct, or participate in, any gambling activity including the operation of a gambling device, conducting a lottery or pool, a game for money or property, or selling or purchasing a numbers slip or ticket.

13.8 Solicitation

Except as authorized by the Center Director, GEWA or WEMA, individuals shall not engage in commercial solicitation at GSFC, such as distribution of commercial advertising material or product samples, or collecting debts. Fundraising, except for the Combined Federal Campaign, is prohibited. Approved activities and the collection of commercial debts by authorized financial institutions (e.g., NASA Federal Credit Union) are permitted. Sales and marketing representatives on official business with NASA will be permitted to call on clients at the GSFC on an appointment-only basis.

13.9 Animals

No domesticated animals, except trained assistance dogs and dogs brought in for official purposes, are permitted on the GSFC or its facilities. Employees, contractors, and guests on the GSFC will not feed or attempt to domesticate any of the wild animals inhabiting the Greenbelt or WFF facilities. Employees, contractors, or guests who discover dangerous, annoying, dead or dying animals on the GSFC should immediately report the event or situation to the GSD. At Greenbelt, call the GSD Security Operations Center at 6-8661. At WFF, report the event to the Emergency Operations Center at 911 from an on-Center phone, or 757-824-1333 from a cell phone.

13.10 Offensive Communications

Abusive communications, such as threatening, intimidating, or harassing language and telephone calls, are prohibited on or at any GSFC location. Victims of such abuse should immediately report the communications to the GSD with as much information as possible. At Greenbelt, call the GSD Security Operations Center at 6-8661. At WFF, report the event to the Emergency Operations Center at 911 from an on-Center phone, or 757-824-1333 from a cell phone.

13.11 Children

Children of GSFC employees and contractors may be permitted on GSFC facilities if they are escorted by their parent(s). Children may be left at the Child Development Center for day care purposes.

Except as provided above, children shall be accompanied and controlled by their parent(s) at all times. Children are considered to be visitors and may not be taken into Restricted, Limited or Closed Areas (see NPR 1600.1) without prior written approval and authorization by the area owner. Similarly, local managers may impose further restrictions on children visiting their areas.

Appendix A

Espionage and Terrorism Indicators

An increasing number of studies and reports have indicated that specific behaviors or characteristics are frequently exhibited by individuals engaged in espionage and/or terrorist activities. Some of these reports are:

- a. NASA Counterintelligence Program Operating Instruction, May 2007
- b. Department of Homeland Security/Federal Bureau of Investigation Memo dated August 3, 2004, Suspicious Activity Reporting Criteria for Infrastructure Owners and Operators
- c. Department of Homeland Security/Federal Bureau of Investigation Joint Intelligence Bulletin No. 148 dated September 14, 2004, subject: Al-Qaida Surveillance Tactics Similar to Those in Recovered Al-Qaida Training Manual
- d. Ohio Homeland Security brochure HLS 0005, dated 08/2005, It's the Little Things That Count: Seven Signs of Terrorism, found at:
http://www.homelandsecurity.ohio.gov/PDF_files/Seven_Signs_Brochure.pdf
- e. Central Intelligence Agency Counterintelligence Indicators: <http://intelligencesearch.com/ia097.html>

An Internet search for "Joint Terrorism Task Force" will provide numerous additional sources. The following lists of indicators have been developed:

Espionage Indicators

While common features abound, it is important to note that these factors are descriptive and not predictive. That is, certain behaviors and personality characteristics have been found to be associated with persons who have engaged in espionage, but they are by no means exclusive to that set of people. The important lesson here is that managers and coworkers should be sensitive to the following types of indicators, and report behaviors that suggest possible espionage activity. The letter in parentheses after each indicator shows which of the above five reports was the source.

- a. Removing classified or sensitive information from the workplace without authorization. (e)
- b. Visiting foreign diplomatic establishments in the United States or abroad without any logical reason or permission. (e)
- c. Maintaining close associations with officials from designated countries. (e)
- d. Engaging in personal business dealings/private ventures with individuals from foreign governments or corporations. (e)
- e. Maintaining bank accounts in foreign countries. (e)
- f. Frequently working alone and after scheduled work hours without any logical reason or explanation. (e)
- g. Unauthorized/unexplained continuous contact with foreign governments or foreign corporations. (e)
- h. Violating or circumventing established security practices. (e)
- i. Frequent security violations. (e)
- j. Exhibiting undue curiosity in projects/programs without logical explanation or "need-to-know." (e)
- k. Loitering in areas where sensitive/classified projects are being conducted when the individual is not involved in the project. (e)

- l. Displaying a reluctance to submit paperwork for a security clearance when requested/needed for work. (e)
- m. Exhibiting signs of having more money/valuables than salary or family circumstances would allow. (e)
- n. Experiencing a sudden unexplained reversal of a financial situation. (e)
- o. Bringing unauthorized/unexplained cameras, recording devices, or other similar unauthorized equipment into work areas. (e)
- p. Attempting to entice other employees or contractors into questionable/illegal activities. (e)
- q. Expressing disaffection with NASA programs/projects/employees/contractors and seeking to get revenge. (e)
- r. Demonstrating unusual travel patterns such as last-minute personal trips of short duration and attempting to conceal trips from supervisors/co-workers. (e)
- s. Attempting to gain unauthorized access to computer systems/networks. (b)

Terrorism Indicators:

Prior to every terrorist attack, someone has to “check out” the target to gather needed intelligence. This action is normally performed through: Surveillance; Elicitation; Theft; Tests of Security; and Rehearsals. You should report the following:

- a. Sketching, mapping, photographing, or conducting surveillance of GSFC facilities. (b,d)
- b. Suspicious persons or vehicles. (d)
- c. Individuals asking suspicious questions about GSFC facilities, activities or personnel. (b,d)
- d. Unauthorized individuals attempting to gain access to GSFC facilities. (d)
- e. Theft of or attempts to obtain security uniforms, identification cards, or equipment. (b)
- f. Lost or stolen official identification which could be used or altered to gain access to GSFC. (b)
- g. Stolen official government vehicles, which may be used to access GSFC facilities. (b)
- h. Lost, stolen or any suspicious attempts to obtain blueprints, floor plans, alarm schematics, detailed maps, or other information which could be used to plan a terrorist attack. (b)
- i. Any discovery of documents, particularly in foreign languages, which appear to contain pictures or drawings of GSFC facilities or other key infrastructure. (b)
- j. Information overheard about any planned international or domestic terrorist activity. (d)
- k. Incidents where terrorist organizations offer employment or training to US persons or ask for assistance in the design, manufacture, maintenance, or employment of terrorist weapons. (b)

