Kennedy NASA Procedural Requirements

Effective Date: **October 22, 2004**

Expiration Date: **October 22, 2009**

Responsible Office: **Director of Spaceport Services**

KSC SECURITY PROCEDURAL REQUIREMENTS

National Aeronautics and Space Administration

John F. Kennedy Space Center

KDP-KSC-F-10 Rev. Basic

RELEASED - Printed documents may be obsolete; validate prior to use.

TABLE OF CONTENTS

Preface
P.1 Purpose
P.2 Applicability
P.3 Authority
P.4 Appendices
P.5 Cancellation/Supersession

CHAPTER 1. RESPONSIBILITY FOR SAFEGUARDING

1.1 General
1.2 Kennedy Space Center Chief of Security
1.3 NASA KSC Employees
1.4 Incorporation Into Contracts
1.5 Heads of Primary Organizations

CHAPTER 2 . SECURITY INSPECTIONS AND AUDITS

2.1 Purpose
2.2 Responsibilities
2.3 General Provisions
2.4 Audits
2.5 Security Inspections
2.6 Violations

CHAPTER 3. SECURITY AWARENESS AND TRAINING

3.1 General
3.2 Organizational Requirements
3.3 Briefings
3.4 Security Awareness Library
3.5 Required Documentation

CHAPTER 4. CLASSIFYING AND MARKING

4.1 Classified Information
4.2 Classifying Information
4.3 Declassifying and

CHAPTER 5. SAFEGUARDING CLASSIFIED MATERIAL

5.1 General
5.2 Access to Classified Material

RELEASED - Printed documents may be obsolete; validate prior to use.

5.3 Storage
5.4 Storage Provisions
5.5 Storage Containers
5.6 Combinations
5.7 Opening, Locking, and Checking Storage Containers
5.8 Accounts
5.9 Account Custodians
5.11 Accountability
5.12 Inventories
5.13 Assistance Visits
5.14 Transmission
5.16 Reproduction
5.17 Foreign Government Information
5.18 Secure Conference Rooms

CHAPTER 6. CLASSIFIED INFORMATION INCIDENT REPORTING

6.1 General
6.2 Security Violation and Compromise of Classified Information
6.3 Other Reportable Incidents
6.4 Training
6.5 Penalties

CHAPTER 7. FOREIGN CONTACTS, REQUESTS FOR INFORMATION AND FOREIGN TRAVEL

7.1 General
7.2 Responsibilities
7.3 Reporting Contacts with Foreign Nationals and Representatives of a Designated Country or Area
7.4 Reporting Requests for Information
7.5 Foreign Travel
7.6 Designated Countries and Areas

CHAPTER 8. TECHNICAL SECURITY SAFEGUARD SYSTEMS

8.1 General
8.2 Concept
8.3 System Descriptions
8.4 Requirements
8.5 Intrusion Detection Systems
8.6 Close Circuit Television (CCTV)
8.7 Access Control Systems (ACS)
8.8 System Upgrade

RELEASED - Printed documents may be obsolete; validate prior to use.

CHAPTER 9. COMMUNICATIONS SECURITY

9.1 General
9.2 Responsibilities
9.3 Objectives
9.4 COMSEC Program
9.5 COMSEC Equipment Maintenance
9.6 COMSEC Material Control System
9.7 Emergency Planning and Actions
9.8 COMSEC Evaluations
9.9 COMSEC Awareness
9.10 COMSEC Training

CHAPTER 10. TEMPEST--CONTROL OF COMPROMISING EMANATIONS

10.1 General
10.2 Responsibilities
10.3 Tempest

CHAPTER 11. TECHNICAL SURVEILLANCE COUNTERMEASURES

11.1 General
11.2 Responsibilities
11.3 Requirements
11.4 Procedures
11.5 Discovery of Devices/Suspect Devices

CHAPTER 12. LAW ENFORCEMENT

1.1 General
1.2 Law Enforcement Duties
1.3 Jurisdiction
1.4 NASA and J-BOSC Points of Contact

CHAPTER 13. PROTECTIVE FORCES

13.1 General
13.2 Management of Protective Forces
13.3 Protective Forces Duties
13.4 Protective Forces Training
13.5 Protective Forces Equipment

RELEASED - Printed documents may be obsolete; validate prior to use.

CHAPTER 14. INCIDENT MANAGEMENT SYSTEM

14.1 General
14.2 Responsibilities4
14.3 Security Incident Management Team4
14.4 Preparation and Planning4
14.5 Natural Disasters4
14.6 Bombs and Bomb Threats4
14.7 Hostage/Terrorist Incidents4
14.8 Criminal Acts4

CHAPTER 15. BADGES AND PASSES

15.1 General
15.2 Responsibilities1
15.3 Access to KSC/Cape Canaveral Air Force Station (CCAFS)
15.4 Badge Receipting
15.5 Display and Control of the Badge
15.6 Lost Badge/Area Permit Reporting
15.7 Termination, Leave of Absence, Vacation, and Foreign Travel
15.8 Violations
15.9 Pass Requests by Telephone
15.10 Adverse Information Reporting
15.11 Resident Badges
15.12 Nonresident Badges
15.13 Temporary Passes
15.14 Official Visitor Pass (Escort Required)
15.15 Exit Pass
15.16 Special Badges and Placards

CHAPTER 16. PERSONNEL CONTROL AND AREA PERMITS

16.1 General
16.2 Responsibilities
16.3 Display and Safeguarding of KSCAP and TAA
16.4 Access Provisions
16.5 Safety Familiarization Requirements
16.6 Temporary Area Authorizations
16.7 Requesting Area Permits, PACAS Cards, TAA's
16.8 Lost Area Permit, TAA, or PACAS Card

CHAPTER 17. FOREIGN VISITORS

17.1 General
17.2 Responsibilities

RELEASED - Printed documents may be obsolete; validate prior to use.

17.3 Visitor Identification/Program Definitions
17.4 Visit Types and Definition
17.5 Visit Request Procedures
17.6 Access Authorizations
17.7 Tours
17.8 Foreign Public Information Media
17.9 Discussions and Requests for Information
17.10 Extending Invitations to Visit NASA/KSC
17.11 Visits to MILA STDN Station, Florida

CHAPTER 18. PROTECTIVE BARRIERS AND OPENINGS

18.1 Protective Barriers
18.2 Barricade Classification and Specifications

CHAPTER 19. TRAFFIC AND PARKING CONTROL

19.1 Purpose
19.2 General
19.3 Moving/Nonmoving Traffic Regulations
19.4 Overweight/Overdimension Equipment/Vehicles/Authority/Escort
19.5 Crash Reporting Procedure
19.6 KSC Traffic Citation Point Assessment System
19.7 KSC Traffic Appeals System
19.8 Assignment of Reserved Parking Spaces
19.9 Assignment Responsibilities for Reserved Parking
19.10 Procedures for Requesting Reserved Parking
19.11 Traffic Management Review Board

CHAPTER2 0. VIOLATIONS OF LAW INCIDENT REPORTING

20.1 General
20.2 Behavior of Cleared Persons
20.3 Other Reportable Incidents
20.4 Penalties

CHAPTER 21. TRANSPORTATION AND MATERIAL SECURITY

21.1 General1
21.2 Types of Cargo/Material
21.3 Responsibilities
21.4 Minimum Standards
21.5 Nonofficial Deliveries

RELEASED - Printed documents may be obsolete; validate prior to use.

CHAPTER 22 . REGISTERED KEY AND LOCK SYSTEM (RKLS), LOCKSMITH SERVICES

22.1 Purpose
22.2 Responsibilities
22.3 General
22.4 Key Control Custodians and Alternates
22.5 Key and Lock Accountability/Control
22.6 J-BOSC Locksmith Services
22.7 Key Security/Control
22.8 Audits/Accountability
22.9 KSC Key Accountability System (KKAS)
22.10 Training
22.11 Key Audit Agent

CHAPTER 23. CONTROL OF WEAPONS
23.1 General
23.2 Applicability
23.3 Policy
23.4 Definitions
23.5 Authority to Carry Firearms
23.6 Responsibilities
23.7 Control, Issuance, and Carrying of Firearms by KSC Personnel
23.8 Possession of Weapons by KSC Employees and Requests for Waivers
23.9 Prohibited Weapons and Items

CHAPTER 24. KSC FLAG POLICY

24.1 General
24.2 Scope
24.3 Authority
24.4 Responsibilities
24.5 Procedures

CHAPTER 25. KSC CHILD CARE DEVELOPMENT CENTER PROGRAM

25.1 General
25.2 Responsibilities
25.3 Adverse Information
25.4 Periodic Reinvestigations

CHAPTER 6. FEDERAL EMPLOYEE SECURITY PROGRAM (FESP)

26.1 General
26.2 Position Sensitivity Levels

RELEASED - Printed documents may be obsolete; validate prior to use.

26.3 Responsibilities
26.4 NASA Pre-Employment Screening
26.5 Periodic Reinvestigations
26.6 Security Clearances
26.7 Security Clearances for Civil Servants
26.8 Certifying Security Clearances from KSC
26.9 Certifying Security Clearances to KSC
26.10 Co-operative (Co-op) Education Students

CHAPTER 27. PERSONNEL RELIABILITY PROGRAM (PRP)

27.1 General
27.2 Responsibilities
27.3 Mission Critical Space Systems Areas (MCSSA)
27.4 Other Area Designation Personnel Screening Requirements
27.5 Authorized Requestors
27.6 Acceptance of Other Programs
27.7 Verifying PRP Certification to Other Installations
27.8 Forms and Procedures
27.9 Specific Criteria
27.10 Disposition of Cases with Adverse Information
27.11 Employment Status
27.12 Interim PRP
27.13 Personnel Reliability Board

CHAPTER 28. AUTOMATED INFORMATION PERSONNEL SECURITY PROGRAM

28.1 General
28.2 Responsibilities

APPENDIX

A. Miscellaneous Controlled Activities

Preface

P.1 Purpose

This directive is to ensure that security policies, regulations, and procedural requirements for security matters on NASA, Kennedy Space Center (KSC) are fully addressed. This KNPR prescribes the minimum standards, procedures, specifications, and requirements to be followed at KSC to ensure uniformity and effectiveness.

P. 2 Applicability

RELEASED - Printed documents may be obsolete; validate prior to use.

This KNPR is applicable to all personnel, facilities, property, and classified material at KSC, regardless of custody. The information detailed shall provide the level of detail necessary to apply the security standards as identified to support the Resource Protection Program for KSC. This applies to all KSC organizational elements and to their associated contractors to the extent specified in their respective contracts. It also applies to other Government agencies, visitors to KSC, and sites under KSC's operational jurisdiction. Modifications to existing facilities and systems, required for full compliance with NASA Resource Protection requirements, shall be made as funds are available.

P.3 Authority

a. NPD 1600.2, “NASA Security Policy”
b. NPR 1600.1, “NASA Security Program Procedural Requirements”

P.4 Appendix

Miscellaneous Controlled Activities

P.5 Cancellation/Supersession

This document supersedes KHB 1610.1, Basic, KSC Security Procedural Requirements.

Scott Kerr
Director of Spaceport Services

Distribution: TechDoc Library

CHAPTER 1. RESPONSIBILITY FOR SAFEGUARDING

1.1 GENERAL

Directors of field organizations are levied the responsibility for ensuring proper safeguarding of facilities, property, information, and/or material under their jurisdiction to include component activities geographically located apart from the parent installation.

1.2 KENNEDY SPACE CENTER CHIEF OF SECURITY

The Director of Spaceport Services appoints the Center Chief of Security (CCS) of KSC who is responsible for:

RELEASED - Printed documents may be obsolete; validate prior to use.

a. Ensuring that Protective Services & Safeguards Office personnel are immediately and fully responsive to any request for assistance received from an individual relating to security, as set forth in this requirement.

b. Establishing and maintaining the standards and implementing the procedures, specifications, and requirements stated in NASA HQS directives and in this requirements document.

c. Personally approving the modification or substitution of any provision set forth in this requirement after a specific determination that such modification or substitution provides protection for classified material or installation property at least equal to that prescribed within.

d. Promptly and fully determining the circumstances of any loss or subjection to possible compromise of classified information or material at the installation and taking such action as may be necessary to formally notify the originating office or agency.

e. Establishing more rigid standards, procedures, or specifications than prescribed in this KNPR whenever conditions or circumstances arise which indicate that increased security needs are necessary in the interest of National Security.

f. Ensuring that points of contact within the Protective Services & Safeguards Office for each chapter of this KNPR are identified.

1.3 NASA KSC EMPLOYEES

a. NASA and contractor supervisors, at all levels, are responsible for ensuring that they and the personnel under their jurisdiction, to whom classified material is entrusted, are fully knowledgeable of and comply with the provisions set forth in this procedural requirement and installation security regulations where applicable.

b. All NASA employees generating, having possession of, or otherwise handling classified information or material are responsible for:

(1) Familiarizing themselves with and complying with the requirements of this KNPR.

(2) Verifying that a prospective recipient of classified information or material has both:

RELEASED - Printed documents may be obsolete; validate prior to use.

(a) A security clearance equal to the degree of classification involved.

(b) An official "need-to-know" for the information or material involved.

(3) Immediately reporting to Protective Services & Safeguards Office, any loss or suspected compromise of classified information or material.

(4) Bringing to the attention of their supervisor any known or suspected practice or condition which does not constitute compliance with this procedural requirement.

c. NASA supervisors at all levels are responsible for ensuring that they, and the personnel under their jurisdiction, who occupy KSC facilities, are knowledgeable of the security requirements for the protection and safeguarding of those facilities and shall bring to the attention of The Protective Services & Safeguards Office, any condition or practice not commensurate with established security procedures or requirements.

1.4 INCORPORATION INTO CONTRACTS

The Director, Procurement Office, shall incorporate this KNPR into all contracts consistent with its applicability and scope.

1.5 HEADS OF PRIMARY ORGANIZATIONS

Heads of primary organizations shall ensure that personnel under their control adhere to the requirements and concepts of this KNPR.

CHAPTER 2. SECURITY INSPECTIONS AND AUDITS

2.1 PURPOSE

This chapter provides for the establishment and conduct of a security inspection and audit program to ensure KSC's compliance with this KNPR, Executive Order, federal regulations, Protective Services & Safeguards Office procedural requirements, and laws applicable to KSC and areas under its jurisdictional control.

. RESPONSIBILITIES

a. The Chief, Protective Services & Safeguards Office, is responsible for:

RELEASED - Printed documents may be obsolete; validate prior to use.

(1) Security inspections and audits of KSC organizations for their adherence to the security requirements with which they are lawfully obligated to comply.

(2) Reporting the results of security inspections and audits to the Director of Spaceport Services, the organizations audited, and if appropriate, to other Government agencies.

b. Heads of primary organizations are responsible for:

(1) Complying with the provisions of this chapter.

(2) At the request of the Chief, Protective Services & Safeguards Office, providing points of contact within their organization to accommodate audit teams or inspectors.

2.3 GENERAL PROVISIONS

a. Scheduled and unscheduled audits may be conducted by The Protective Services & Safeguards Office personnel, or their designees, to assess the effectiveness of KSC's adherence to security regulations, directives and policy.

b. Inspections and audits shall be performed to provide a method of informing organizations of problems, or potential problems, in their security program.

c. Results of inspections and audits shall be documented and provided to top management. Follow-up reviews may be performed to ensure corrections have been implemented.

d. Security Inspection and Audit Teams shall:

(1) Coordinate with the organization to be inspected/audited to ensure that the scheduled inspections/audits are conducted on a noninterference basis.

(2) Provide, in advance, a written "Notification of Inspection" to the organization being audited and request they complete the attached audit information survey.

e. Each organization shall:

RELEASED - Printed documents may be obsolete; validate prior to use.

(1) Provide an organizational point of contact for scheduled or unscheduled inspections or audits.

(2) Complete the pre-inspection/audit information survey and return it to The Protective Services & Safeguards Office at least 5 working days prior to the scheduled inspection.

2.4 AUDITS

a. Audits shall focus on the information security aspects of KSC activities and shall be designed to effectively assess the proper application of security measures concerning the marking, handling, storage, transmission, and destruction of classified material.

b. Periodic information security audits shall consist of, but not necessarily be limited to, the following:

(1) Classified account inventory

(2) Storage containers/combination change

(3) Classified account custodian training

(4) Administrative procedures

(5) General security training attendance

c. In conjunction with the periodic information security audit, an inventory of Guest Badges shall be conducted if the organization being inspected has guest badges issued to them.

d. Prior to the start of the audit, security teams/inspectors shall provide an initial briefing to an organizational point of contact and an outbriefing upon completion.

2.5 SECURITY INSPECTIONS

a. The Chief, Protective Services & Safeguards Office, in fulfilling the role of the Center Chief of Security, has the overall responsibility to ensure a secure working environment for all KSC employees. To accomplish this, The Protective Services & Safeguards Office shall perform scheduled and unscheduled security inspections of KSC organizations to ensure compliance with all aspects of this KNPR and other applicable security regulations.

RELEASED - Printed documents may be obsolete; validate prior to use.

b. In addition to security inspections conducted by representatives of The Protective Services & Safeguards Office, the Joint-Base Operations Support Contractor, under the auspices of Chief, Protective Services & Safeguards Office, conducts periodic Resource Protection Surveys.

c. Security inspections shall focus on, but not necessarily be limited to, the following:

(1) Physical security.

(2) Technical security.

(3) Operations security.

(4) Administrative security (exclusive of classified accounts).

(5) Mission specific security when classified requirements are identified.

(6) General security training attendance.

2.6 VIOLATIONS

If evidence that a suspected or actual violation of a security regulation or breech of law is found, the provisions of Chapter 04, "Classified Information Incident Reporting," or Chapter 409, "Violations of Law Incident Reporting," shall be followed.

CHAPTER 3. SECURITY AWARENESS AND TRAINING

3.1 GENERAL

Security awareness is achieved through a continuing process of information and motivation. At KSC this shall be accomplished through a series of formal briefings arranged by The Protective Services & Safeguards Office and through the respective efforts of each organization. In addition to security awareness, employees must be trained in the materials and methodology of security. Each organization shall develop and undertake a program of security training.

3.2 ORGANIZATIONAL REQUIREMENTS

a. Each organization shall provide its employees with a program of security awareness and training commensurate with the employees'

RELEASED - Printed documents may be obsolete; validate prior to use.

involvement with sensitive or classified information, material, or operations. To a reasonable extent, security awareness and training shall be tailored to the employees' duties, functions, or situations. For example, employees who are not cleared for access to classified information need not be instructed in the procedures for classified document control. On the other hand, a group of employees who work in a closed area (access to which is considered equivalent to access to classified information) shall be informed of their security responsibilities and instructed in security procedures for working in that area. The intent is to motivate employees and ensure that they have the requisite knowledge to fulfill their security responsibilities.

b. Security Awareness. Each organization shall implement security awareness measures to supplement the required briefings identified below. Since each organization is responsible for various and sundry protectable resources, it is not practical to define in detail the composition of organizational security awareness programs. Rather, each shall implement a program commensurate with the security requirements under which it operates. Some awareness measures which organizations shall consider include:

(1) Periodic discussions by supervisors of the need for, and benefits of, security.

(2) Displaying security reminders, such as posters, stickers, and notices.

(3) Using audio-visual aids, such as security films, video tapes, and slide presentations.

(4) Establishing a system for handling security questions or suggestions.

c. Security Training. In conjunction with security awareness, each organization shall train its employees in the security measures for which they are responsible. This security training shall include:

(1) Identification of the material or information which must be protected.

(2) Explanation of the location and use of security equipment.

(3) Instruction in routine security procedures.

RELEASED - Printed documents may be obsolete; validate prior to use.

(4) Instruction in the procedures to be followed in the event security is breached.

(5) Explanation of each employee's individual security responsibilities.

(6) Any other training or briefing required by other chapters of this KNPR, NASA regulation, Federal law, Executive Order, or regulation.

d. Special Considerations. To be effective, security must be considered at every phase of an activity. Organizations involved in the design, procurement, and construction of facilities or systems must be aware of the protectable resources with which they are involved and of the security requirements attached to those resources. These organizations shall provide sufficient security training to enable their employees to identify, protect, or plan for the protection of those resources. This shall be accomplished by ensuring that employees have a thorough understanding of these portions of all classification guides for which they have a need-to-know.

3.3 BRIEFINGS

a. Required General Briefings. The following briefings have been approved by The Protective Services & Safeguards Office, and are provided to KSC government employees on a scheduled basis by the Joint-Base Operations Support Contractor (J-BOSC). Attendance at briefings may be arranged by telephoning the J-BOSC Security Awareness Office, 861-5146. Contractor employees shall attend on a space-available basis:

(1) Security Orientation. This briefing is required for all persons who work at KSC.

(2) Safeguarding Classified Material. This briefing is required for all persons working at KSC who are cleared for access to classified material.

(3) Hostile Intelligence Threat. This briefing is required for all KSC employees, both NASA and contractor, who have a Secret or Top Secret clearance.

RELEASED - Printed documents may be obsolete; validate prior to use.

(4) Cleared Employee Rebriefing. This briefing is an abbreviated version of (2) and (3) above. It is required annually for all persons who have previously attended (2) and (3).

(5) Triennial Uncleared Employee Review. This briefing is an abbreviated review of (1), (2), and (3) above. It is required every third year after initial orientation for all personnel who do not hold a SECRET or TOP SECRET clearance.

(6) Classified Custodian Briefing. This briefing is required biennially for all personnel designated as Classified Custodians or Alternate Custodians.

The J-BOSC maintains an index of all KSC individuals who have attended general security briefings. This index is updated and distributed monthly. Each organization is given a copy of that part of the index that applies to it. Accompanying the index is a listing of those persons who are due to attend the CLEARED EMPLOYEE REBRIEFING.

b. Specialized Briefings.

(1) The Protective Services & Safeguards Office shall arrange for briefings on:

(a) Cryptographic equipment maintenance.

(b) Communications Security (COMSEC).

(2) The Protective Services & Safeguards Office shall arrange for briefings on TEMPEST design considerations.

c. Program-Specific Security Briefings.

(1) Launch Site Support Managers (LSSM's) shall arrange for briefings dealing with the special security or classification requirements associated with DoD payloads. Individuals shall be briefed only on that information for which they have a need-to-know as determined by the LSSM's. LSSM's shall ensure that The Protective Services & Safeguards Office is provided a list of the attendees and an identification of the information they were given. (NOTE: This information is sensitive and in many cases may be classified.)

RELEASED - Printed documents may be obsolete; validate prior to use.

(2) Other program-specific briefings (e.g., STARLAB, Space Station) shall be arranged by the respective Office of Primary Responsibility.

3.4 SECURITY AWARENESS LIBRARY

The J-BOSC maintains a library of security awareness material, primarily audio-visual. Items from the library are available for loan to organizations to which this chapter applies. A listing of the library's contents and the procedures and terms for loan may be obtained from the J-BOSC Security Awareness Office, mail stop SGS-33, or by telephoning 861-5146.

3.5 REQUIRED DOCUMENTATION

To provide a means of auditing for compliance with the requirements of this chapter, organizations shall document their security awareness and training efforts pursuant to paragraph 01. above. At a minimum, this documentation shall include:

a. A description of the security awareness and training and a listing of the employees to which it is given.

b. An explanation of how that course of awareness and training is determined and at what level(s) it is given. (It is expected that security awareness and training shall not be offered one-on-one, but shall be provided to groups of employees who share common or similar jobs, functions, or situations).

CHAPTER 4. CLASSIFYING AND MARKING

4.1 CLASSIFIED INFORMATION

Information (and material) which is protectable in the interests of the national security is assigned to one of three classifications, from highest to lowest: TOP SECRET, SECRET, and CONFIDENTIAL. The classifications reflect the degree of adverse impact that unauthorized disclosure of the information could have on the national security.

Only certain persons within the Federal Government, referred to as original classification authorities or original classifiers, are authorized to classify information. It is not practical, and often not possible, for them to review all information which is potentially protectable in the interest of the national security. Instead, they describe in Security Classification Guides (SCG's) the types of information which must be protected. These SCG’s not only identify

RELEASED - Printed documents may be obsolete; validate prior to use.

the kinds of information that are classified, but also indicate the level of classification and how long the classification shall remain valid. Most importantly, these guides serve as the authority for cleared persons to classify the information described in the SCG's.

a. Original Classification Authority. Original classification authority has been retained at NASA Headquarters. Any questions concerning classification of information or material should be directed to The Protective Services & Safeguards Office.

b. Derivative Classification Authority. There are two sources of derivative classification authority. They are security classification guides and previously classified information. Derivative classification authority may be exercised by any person who is cleared for access to classified information.

4.2 CLASSIFYING INFORMATION

The originator of material determines its classification, the authority for the classification, downgrading and declassifying instructions, and warning notices.

4.3 DECLASSIFYING AND DOWNGRADING

When a document qualifies for downgrading or declassifying, the individual having custody of it is responsible for changing its markings.

Declassifying, either automatically or by individual review and determination, is not automatically an approval for public disclosure. Accordingly, KSC personnel shall process all requests for public disclosure of "declassified" information through The Protective Services & Safeguards Office.

CHAPTER 5. SAFEGUARDING CLASSIFIED MATERIAL

5.1 GENERAL

This chapter establishes the Kennedy Space Center's system for safeguarding classified material.

5.2 ACCESS TO CLASSIFIED MATERIAL

a. Only those individuals who have been granted the appropriate security clearance and have a need-to-know shall be given access to classified material.

RELEASED - Printed documents may be obsolete; validate prior to use.

b. A recipient's clearance must equal or exceed the material's classification. The custodian of the classified material must verify that the recipient is cleared at the proper level. The level of clearance of KSC Government and KSC contractor employees may be verified by calling the applicable NASA or contractor security office. During non-duty hours, the Visitor's Record Center (VRC), 867-7763, may verify clearances. Clearances of visitors to KSC may be verified at any time by calling the VRC.

c. The need-to-know principle states that a person's clearance for access to classified material does not automatically entitle the individual to that access. The individual must also have a need for access to the classified information or material sought in connection with the performance of official duties or contractual obligations. The final responsibility for determining whether an individual's official duties require possession of, or access to, any element or item of classified information rests upon the individual who has authorized possession, knowledge, or control of the information and not upon the prospective recipient.

5.3 STORAGE

Classified information must be under the personal control and observation of an authorized person, or stored in an approved container or storage area at all times. Approved containers and storage areas are defined as GSA-approved safe-type steel file cabinets equipped with a built-in, three-position, dial-type combination lock, or an approved vault or vault-type room that meets the standards as published by the General Services Administration, or other secure storage areas as approved by the Protective Services and Safeguards Office.

5.4 STORAGE PROVISIONS

a. Each organization shall periodically review its classified holdings for the purposes of reducing them and maintaining them at an absolute minimum.

b. Classified material which is temporarily removed from the normal workplace (e.g., for conferences, studies, or meetings) must be under the continuous control of its authorized holder or properly stored at the temporary location.

c. Classified material shall only be used and stored at places of official business on KSC/CCAFS. Classified material shall not be removed

RELEASED - Printed documents may be obsolete; validate prior to use.

from KSC to a place of residence or other off-Center location without the approval of The Protective Services & Safeguards Office.

d. Classified waste shall be properly stored in containers or facilities approved for storage of classified materials while awaiting destruction.

5.5 STORAGE CONTAINERS

a. Containers which have been approved for storing classified material shall not be used for storing items such as funds, weapons, controlled drugs, precious metals, or other valuable unclassified property. The Protective Services & Safeguards Office may waive this restriction in an emergency, provided action is initiated promptly to provide separate storage for the unclassified items.

b. Classified material storage containers shall not be relocated without prior approval from the applicable NASA or contractor security office.

e. Organizational elements needing security containers must submit requests through their contractor security office or, for NASA accounts, directly to The Protective Services & Safeguards Office.

5.6 COMBINATIONS

All combinations shall be changed upon:

a. The initial receipt of the container or possession of the vault or area.

b. The relief, transfer, discharge, termination, hospitalization, leave of absence, suspension, or revocation of the clearance of any person who knows the combination.

c. The compromise or suspected compromise of the container or its combination (e.g., discovery that the container has been left unlocked and unattended).

5.7 OPENING, LOCKING, AND CHECKING STORAGE CONTAINERS

a. A Standard Form 70, Security Container Check Sheet, shall be used to record the opening, locking, and checking of each container

b. When a classified container is open, it must be under the control of a person whose name appears on the Standard Form 700 as being authorized to control the contents of that container.

d. A classified container must be locked when unattended.

RELEASED - Printed documents may be obsolete; validate prior to use.

e. After a classified container is locked it should be checked. The check may be done by anyone, regardless of clearance level.

5.8 ACCOUNTS

a. A classified material account is required for each organizational element which must retain classified material.

b. Each classified account must have appropriate storage capability for materials assigned to the account.

c. Requests for establishment of classified material accounts shall be forwarded in writing to the Classified Material Control Center (CMCC). The following may request classified material accounts for their organizational elements:

(1) NASA KSC managers at the branch level or higher.

(2) The heads of other NASA organizations or other Federal agencies at KSC.

(3) The security officers or, if none, the heads of contractor organizations at KSC.

d. Closing an Account. When an account is no longer needed, it shall be closed. The primary custodian shall transfer the account's classified material to other accounts or to the CMCC for destruction.

5.9 ACCOUNT CUSTODIANS

One individual shall be appointed as primary custodian of each classified account and shall be responsible for all containers assigned to the account and the classified material held by the account.

5.10 DESIGNATING CUSTODIANS

The primary and alternate custodians shall be designated, in writing, to the CMCC.

5.11 ACCOUNTABILITY

a. To manage its classified holdings, KSC uses a system of classified material accounts reporting to a CMCC.

RELEASED - Printed documents may be obsolete; validate prior to use.

b. The CMCC maintains a record of all accountable classified material. Classified material sent to KSC is received by the CMCC. Classified material received directly by other KSC organizations within the KSC CMCS shall be immediately reported to the CMCC. Similarly, all accountable classified material which is generated at KSC shall be reported to the CMCC. As directed, and with limitations, the CMCC processes classified material and notifies intended recipient to arrange for transporting such material within KSC, and between KSC and CCAFS and PAFB. The CMCC also arranges the reproduction and distribution of classified documents, destroys classified material that is no longer needed, and provides instruction to account custodians.

5.12 INVENTORIES

a. The CMCC shall be requested to assist in an inventory, at least annually, of each account. The primary and alternate custodians shall assist in the inventory, locating and personally viewing each piece of accountable classified material that is charged to the account.

b. An account shall be inventoried by the CMCC upon the removal or replacement of a custodian or alternate custodian. The inventory shall be completed before the custodian departs. Discrepancies shall be reported to the Protective Services & Safeguards Office.

c. Whenever a classified storage container is found unlocked and unattended, the primary custodian shall conduct an inventory jointly with a CMCC representative. An incident report shall be filed as required by Chapter 04 of this KNPR.

5.13 ASSISTANCE VISITS

a. The assistance visit program ensures compliance with the procedures set forth in this KNPR and verifies the adequacy of all classified document accounts within the purview of the KSC Classified Material Control System.

b. Assistance visits shall be made to each classified account to ascertain that all applicable procedures are properly implemented and effectively utilized. Protective Services & Safeguards Office representatives shall identify and document any discrepancies noted during such visits and prepare a written report of their findings.

RELEASED - Printed documents may be obsolete; validate prior to use.

5.14 TRANSMISSION

a. General Requirements.

(1) Classified material transmitted outside of the KSC Classified Material Control System shall be processed through the CMCC.

(2) Classified material shall normally be brought into or taken out of KSC and CCAFS by the U.S. Postal Service. All material not delivered in this manner must be immediately turned in to the CMCC.

(3) Classified material shall not be transmitted outside the continental United States without the written approval of The Protective Services & Safeguards Office.

(4) The Protective Services & Safeguards Office shall be notified if classified material is received and the package:

(a) Has been improperly wrapped.

(b) Shows any evidence or signs of tampering.

(c) Has been improperly transmitted.

e. Transporting Classified Materials on KSC/CCAFS.

CMCC couriers are authorized to transport classified materials on KSC/CCAFS. They are the only couriers authorized to transport classified materials “to organizations not within the KSC CMCC,” to J-BOSC Reprographics for reproduction processing, and to destruction facilities for destruction.

f. Transporting Classified Materials off KSC/CCAFS.

(1) Couriers who carry or accompany classified material shall be briefed by their security officer concerning the requirements and limitations of courier duty. A separate briefing shall be given for each courier assignment. The courier must read and sign a copy of the "Courier Instructions" which are contained in Appendix G. KSC Form 0-49, Authorization to Hand-Carry Classified Material, shall be prepared by the courier's security officer and approved by The Protective Services & Safeguards

RELEASED - Printed documents may be obsolete; validate prior to use.

Office. The KSC Form 0-49 must remain in the courier's possession while transporting classified material.

(2) Couriers required to transport classified materials aboard commercial aircraft shall be issued a letter by The Protective Services & Safeguards Office. The letter shall be used to identify the courier to airline personnel. The KSC Form 0-49 shall not be shown to airline personnel.

(3) KSC Form 0-49 must be completed by all couriers upon completion of courier duty outside KSC/CCAFS/PAFB. The form shall be returned to the CMCC upon completion. Sections concerning deviations in itinerary must explain any deviation or incidents which occurred during the assignment.

5.15 REPRODUCTION

a. Reproduction of classified material shall be kept to a minimum consistent with efficient operations and limited in order to lessen the risk of compromise and the expense of subsequent protection.

b. Reproduction, for purposes of this chapter, is any activity that duplicates classified information. This includes, but is not limited to, photocopying, printing, and photographing, all of which is addressed herein. Any other reproduction of classified material shall be in accordance with procedures as approved by The Protective Services & Safeguards Office.

c. Classified material may be reproduced only on equipment that has been approved for that purpose by The Protective Services & Safeguards Office.

d. Key personnel, as listed below, may authorize reproduction of classified materials for their respective organizational elements:

(1) Branch chiefs or higher of NASA organizational elements for materials classified up to and including SECRET.

(2) The security officer, or a designated representative, of other organizations for material classified up to and including SECRET. Organizations which do not have a security officer at KSC shall consult The Protective Services & Safeguards Office, when classified reproduction is needed.

RELEASED - Printed documents may be obsolete; validate prior to use.

(3) Section chiefs or higher of NASA organizational elements for material which is classified up to, and including CONFIDENTIAL.

f. All requests for reproduction of accountable and non-accountable classified material must be forwarded to the CMCC. The Protective Services & Safeguards Office may authorize reproduction of classified materials by other individuals or organizational functions when deemed necessary in support of launch operations.

5.16 DESTRUCTION

a. Classified material within the KSC Classified Material Control System shall be destroyed only by the CMCC.

b. When doubt exists as to the propriety of destroying classified material received from another Federal department or agency, consult The Protective Services & Safeguards Office, for instructions.

c. To prevent an unnecessary accumulation of classified material, each organization shall continuously review its classified holdings and shall reduce it to the minimum needed for efficient operations. Surplus copies shall be transferred or destroyed as soon as practical. Accountability records for accountable material shall be maintained years from the date that all materials listed thereon have been destroyed.

d. At regular intervals classified waste shall be passed to the CMCC for destruction so that the amount on hand is kept to a minimum.

5.17 FOREIGN GOVERNMENT INFORMATION

Classified foreign government information shall be protected and accounted for in accordance with the procedures as specified in this chapter for comparable U.S. classified information.

5.18 SECURE CONFERENCE ROOMS

General requirements for establishing and maintaining Secure Conference Rooms are contained in Chapter 7, NHR 1600.1, NASA Security Program Procedural Requirements.

RELEASED - Printed documents may be obsolete; validate prior to use.

CHAPTER 6. CLASSIFIED INFORMATION INCIDENT REPORTING

6.1 GENERAL

a. Time is critical when reporting and investigating incidents involving classified material. All organizations shall take steps to ensure the timely reporting of incidents covered by this chapter.

b. In cases where a physical examination of a particular item or site is likely during the course of an investigation, the item or site shall be preserved exactly as found, provided that this does not either jeopardize safety, nor disclose classified information.

c. When an incident may gravely affect the national security or the preservation of critical national resources, the Installation Security Officer or a NASA-KSC investigator, shall, as long as safety is not jeopardized, initiate the following:

(1) Order that the scene of the incident be protected to assure the preservation of evidence by freezing conditions and configurations.

(2) Impound material.

(3) Conduct interviews.

(4) Order persons who are knowledgeable of the incident or investigation not to discuss it except as directed by the Installation Security Officer or NASA-KSC investigator.

6.2 SECURITY VIOLATIONS AND COMPROMISE OF CLASSIFIED INFORMATION

a. Classified information is vulnerable to compromise when personnel allow themselves to become negligent. The most common security violations are:

(1) Failing to properly secure classified material in an authorized container when it is not under their immediate, continuing control and supervision.

(2) Not properly preparing classified material for transmission, or improperly transmitting such material.

RELEASED - Printed documents may be obsolete; validate prior to use.

(3) Discussing or attempting to "talk around" classified information during telephone conversations or in places where unauthorized persons are present.

(4) Misplacing or otherwise losing control of classified material (including classified waste).

(5) Releasing classified information without properly determining the recipient's identity, clearance status, and need-to-know. Also see paragraph 04.3.

b. Emergency Action and Reporting Requirements. Individuals, who observe that classified information is not being given the prescribed protection, or that classified material has been lost or compromised, shall:

(1) Immediately take all interim action possible to restore the prescribed security controls over the information or material. An examination of an item or site is likely during the course of an investigation (such as, in the burglary of a safe), then take care to preserve the site as long as this shall not seriously degrade the integrity or the security of other areas, material, or information. Refer to paragraph 04.1b.

(2) Report the circumstances promptly to an immediate supervisor, or, if not immediately available, directly to The Protective Services & Safeguards Office. Non-NASA personnel shall report the circumstances to their employer's security personnel or, if none, directly to The Protective Services & Safeguards Office.

6.3 OTHER REPORTABLE INCIDENTS

The following incidents may relate to the protection of either classified information or critical Government resources. These incidents shall be reported in the manner described in paragraph 04. This list is not all inclusive. Other incidents, similar to those listed below, may require reporting.

a. The presence of uncleared individuals, without proper escort, in a security area.

b. The presence of an individual in a security area who does not have a need for being in that area.

RELEASED - Printed documents may be obsolete; validate prior to use.

c. Requests for classified information from sources whose need to know is questionable.

6.4 TRAINING

a. Anyone involved in a security compromise that is found to be in violation of law or policy shall be required to attend specific security training to preclude further incidents or violations.

b. Specific training may be recommended by the security office handling the investigation.

c. Unless the individual's clearance is suspended or revoked, the training shall be accomplished prior to the individual returning to duties involving classified material or information.

d. A record of the training shall be maintained with the incident's investigative case file.

6.5 PENALTIES

a. Shallful disregard of any security instruction or policy could result in removal from Federal service.

b. Careless or negligent failure to observe any security requirements or policy could result in disciplinary action.

c. In the event of security violations by military personnel detailed to KSC, the verbal admonishment for the first violation may be administered in the same manner as for civilian employees. Subsequent violations shall be reported to the individual's military organization, where military disciplinary procedures may apply.

CHAPTER 7. FOREIGN CONTACTS, REQUESTS FOR INFORMATION AND FOREIGN TRAVEL

7.1 GENERAL

This Chapter provides direction and reporting criteria for contacts with foreign nationals and unauthorized requests for information. It also provides security briefing criteria for official and personal foreign travel to designated countries and areas.

7.2 RESPONSIBILITIES

RELEASED - Printed documents may be obsolete; validate prior to use.

a. Government employees at the Kennedy Space Center shall follow the requirements in this Chapter.

b. Contractor employees shall follow the requirements in the National Industrial Security Program Operating Manual (NISPOM), Standard Practice Procedures, and this Chapter.

7.3 REPORTING CONTACTS WITH FOREIGN NATIONALS AND REPRESENTATIVES OF A DESIGNATED COUNTRY OR AREA

a. "Establishments" means embassies, consulates, press, airline, travel or business offices representing designated countries or areas.

b. "Foreign National or Representatives" means any designated country or area diplomat, visitor, tourist, student, journalist, engineer, or scientist. Representatives also include United States citizens representing or acting on behalf of a designated country or area.

c. "Contacts" mean any form of meeting, association, or communication, regardless of who made the contact. The contact could be for social, official, private, or any other reason. Contacts made in person, by radio; i.e., HF, UHF, or VHF, telephone, letter, post cards, facsimile, computer/Internet access (electronic mail/electronic bulletin boards) and receiving subscriptions to designated country publications are reportable.

d. Report all contacts with Foreign Nationals, representatives, or establishments of designated countries or areas, including contacts made or received by family members.

e. For NASA KSC Government Employees:

Report "contacts" to the Protective Services & Safeguards Office, 867-456 or 867-465, mail code: TA-G/Safeguards.

f. For Contractor Personnel:

Follow your company's Standard Practice Procedures (SPP's), the National Industrial Security Program Operating Manual, and this Chapter, as appropriate, to report "contacts".

RELEASED - Printed documents may be obsolete; validate prior to use.

7.4 REPORTING REQUESTS FOR INFORMATION

a. All requests for information or materials made by anyone without a need-to-know or outside official channels are unauthorized requests. This means classified or unclassified information, documents, publications, material or equipment that is under government or contractor control.

b. Additional restrictions may also apply on requests for information and the release of information or materials; examples are: The Export Administration Act of 1979 (50 U.S.C App. 401-40), The Arms Export Control Act as implemented by the International Traffic in Arms Regulations (ITAR), CFR Part 15, and the Federal Acquisition Regulation, 35 U.S.C. 05, Subpart 7.3.

c. Do not decide for yourself the significance of a request for information. Take the following action after an unauthorized request:

d. For NASA KSC Government Employees

(1) Report all unauthorized requests for information to the Protective Services & Safeguards Office, 867-456 or 867-465, mail code: TA-G/Safeguards.

(2) Do not discuss the information with anyone other than a representative from the Protective Services & Safeguards Office.

e. For Contractor Personnel

Follow the provisions of the National Industrial Security Program Operating Manual and your company's Standard Practice Procedures (SPP's). If a company security representative is not immediately available, report the occurrence to the Protective Services & Safeguards Office, 867-456 or 867-465, mail code: TA-G/Safeguards.

7.5 FOREIGN TRAVEL

a. For NASA KSC Government Employees:

(1) Travel to countries/areas, that are not listed as designated countries or areas, do not require a travel preapproval. Before traveling however, all employees must request a Foreign Travel Briefing from the Protective Services & Safeguards Office, 867-456 or 867-465, Email:

RELEASED - Printed documents may be obsolete; validate prior to use.

SafeguardsOffice@kscems.ksc.nasa.gov, mail code: TA-G/CI Office, to increase their security awareness.

(2) Foreign travel, whether official or personal, into countries/areas that are listed as designated countries or areas, requires preapproval of the Center Chief of Security. NASA KSC employees occupying Mission-Critical positions, performing Mission-Critical duties, or having access to classified information, must the Protective Services & Safeguards Office/Safeguards with the following information at least 3 weeks before their departure:

(a) Full name, date and place of birth.

(b) Current citizenship.

(c) Organization, duty station, and job title.

(d) Purpose of travel.

(e) Security clearance.

(f) Date of last defensive security briefing.

(g) Passport number, issue and expiration date, and identification of all visas.

(h) Whether or not they are assigned to a Mission-Critical position or are performing Mission-Critical duties.

(i) Whether or not they have access to classified material. (Classified custodian, alternate, or user.) If yes, identify the classified account or material used.

(j) Identify any previous security violations or disclosure of classified information.

(k) Furnish dates of planned entry/visit/exit for each designated country/city/area on the trip.

(l) Identify relationships and addresses of relatives living in any designated country or area.

RELEASED - Printed documents may be obsolete; validate prior to use.

(m) Identify previous designated countries or areas visited, and the dates of such visits.

(n) Identify any citizens of designated countries or areas with whom the employee has associated or corresponded and the nature of such association or correspondence.

(3) NASA KSC employees not occupying Mission-critical positions/duties or having access to classified information, that desire official or personal travel to a designated country or area, do not need a preapproval for foreign travel. However, a foreign travel briefing from the Protective Services & Safeguards Office, (see paragraph 05.5a, above) is required before departure.

(4) All NASA KSC employees traveling to, from, or within designated countries or areas require a security debriefing upon their return to work. Contact the Protective Services & Safeguards Office, 867-456 or 867-465, Email: SafeguardsOffice@kscems.ksc.nasa.gov, mail code: TA-G/Safeguards for an appointment.

b. For Contractor Employees:

Follow your company's Standard Practice Procedures, the National Industrial Security Program Operating Manual and this Chapter, as appropriate.

7.6 DESIGNATED COUNTRIES AND AREAS

a. For travel within the purview of this Chapter designated countries or areas are:

Afghanistan
Angola
Bahrain
Belarus
Bhutan
Burma (now Myanmar)
China, Peoples Republic
Congo (formerly Zaire)
Cuba
Cyprus
Egypt
Haiti
Hong Kong (China)

RELEASED - Printed documents may be obsolete; validate prior to use.

India
Indonesia
Iran
Iraq
Israel
Jordan
Korea, North
Kuwait
Lebanon
Liberia
Libya
Macau (China)
Oman
Pakistan
Qatar
Rwanda
Saudi Arabia
Somalia
Sudan
Syria
Taiwan
United Arab Emirates
Vietnam
Yemen, Republic (Sanaa)
Zimbabwe

b. World situations have caused continual political changes in recent months/years. Prior to traveling, contact the Protective Services & Safeguards Office, 867-456 or 867-465, Email: SafeguardsOffice@kscems.ksc.nasa.gov, for a current list of Designated Countries and areas, travel requirements, and information about your destination(s).

CHAPTER 8. TECHNICAL SECURITY SAFEGUARD SYSTEMS

8.1 GENERAL

This chapter establishes technical standards to be applied during design, development, and procurement of technical security safeguards at KSC and other areas/facilities under the cognizance of KSC.

8.2 CONCEPT

RELEASED - Printed documents may be obsolete; validate prior to use.

The design, installation, and operation of technical security safeguard systems are intended to enhance the overall security posture of an area/facility and contribute to the attainment of both operational effectiveness and KSC security objectives. Such safeguards and systems are designed to detect actual or attempted illegal penetrations of sensitive/critical areas. They must, therefore, be supported by a monitoring station and a security force capable of responding promptly to indicators of illegal penetrations.

8.3 SYSTEM DESCRIPTIONS

a. Intrusion Detection Systems (IDS). IDS are used as technical aids for the security forces to expand conventional capability and to alert security guards and responsible personnel of intrusions at protected facilities. As a minimum, rooms or buildings containing mission-critical assets should be equipped with appropriate intrusion detection systems.

b. Closed Circuit Television (CCTV). CCTV is used as an aid to security force personnel in true/false alarm assessment, as a motion detector (with additional circuitry added), and for personnel identification in conjunction with access control systems. Areas considered for CCTV coverage are those requiring continuous surveillance, those areas which require visual monitoring but which would otherwise impose an excessive expenditure of security force support, and those areas requiring other special visual surveillance.

c. Access Control Systems (ACS). The objectives of an access control system are to permit only authorized persons to enter and exit controlled areas, and to provide information to the respective access control monitor, which shall facilitate assessment and response to indications of unauthorized entry. Access controls can be found in many different forms. In general, security is enhanced by supplementing the conventional guard force with an access control system.

8.4 REQUIREMENTS

a. Identifying the Need. It is the responsibility of site management to identify to the Protective Services & Safeguards Office, the fact that an area or facility may need the added protection of a technical security safeguard/system. The Protective Services & Safeguards Office shall arrange for a Risk Analysis which shall identify specific security weaknesses in and around the area/facility. The Protective Services & Safeguards Office provides the policies and procedures by which these

RELEASED - Printed documents may be obsolete; validate prior to use.

analyses are judged and shall determine the appropriate technical security measures to be instituted.

b. Requesting the Safeguard/System.

(1) Requester/Site Manager must develop a written statement of justification identifying the need for a technical security safeguard/system at the facility. This statement should identify the need or requirement rather than specifying the method of accomplishment. This written statement should include certain site-specific data; such as, exact location, estimated need date, and concept of operations (normal and emergency).

(2) The need identified in the written justification is then forwarded to the Protective Services & Safeguards Office. After Risk Analysis is completed, the requirements are refined jointly between the requester and the Protective Services & Safeguards Office.

(3) After requirements are refined and a method to satisfy them agreed to, the requester generates an Engineering Support Request (ESR). The Protective Services & Safeguards Office, Technical Security Specialist shall, by signature, concur with the ESR before its insertion into the implementation process.

c. Protective Services & Safeguards Office. Once a requester or Site Manager has identified a valid need for a technical security safeguard/system, the Protective Services & Safeguards Office is obligated to insure the need is satisfied in a competent, cost-effective manner that is compatible with other existing and planned Centerwide systems. Therefore, the Protective Services & Safeguards Office shall be the focal point for all such projects, from concept development to system activation/operation.

d. Joint-Base Operations Support Contractor's (J-BOSC) Role. J-BOSC's responsibility in relation to technical security safeguards/systems is, generally, one of operations and maintenance (O&M) and of sustaining engineering functions, including Facility Project design and implementation. They are responsible for the performance of preventive, corrective and breakdown maintenance of all field equipment to ensure that ESS maintains a high level of operational performance. Inherent in this responsibility is the development of maintenance plans, each tailored to the unique system being maintained. Maintenance plans shall include, as appropriate,

RELEASED - Printed documents may be obsolete; validate prior to use.

requirements for testing/retesting. All maintenance and other system support plans shall be coordinated with the Protective Services & Safeguards Office for concurrence, prior to publication and implementation. J-BOSC implements modifications to system configuration, responds to daily operational troubles and documents all associated activity. Their responsibilities also include maintaining and updating ESS system drawings and keeping the Government fully informed of major security activities.

8.5 INTRUSION DETECTION SYSTEMS

a. Requirements for Interior and Exterior Intrusion Detection Systems

(1) Equipment Enclosure. All electronic equipment enclosures used for Intrusion Detection Applications shall be protected against tampering by being equipped with tamper switches or triggering mechanisms electrically compatible with the alarm system. Internal wiring of equipment shall be such that the tamper switches and triggering mechanisms are not bypassed even though the detector itself is operating in the "Access" mode. All controls which affect the sensitivity of the units shall be located inside the tamper-resistant enclosure.

(2) Environmental Requirements. All units shall be designed or selected for the temperature range and highest relative humidity ambient to the unit's intended location.

(3) Dependability. The sensitivity and stability of all detectors shall be designed to withstand neutralization or compromise. All systems shall be designed to provide a probability of detection of 0.9 or better with a confidence level of 95 percent.

(4) Electronic Components. To the extent practicable, all electronic components shall be state of the art and be solid state type.

(5) Detectors/Sensors. All detectors and/or sensors shall initiate a signal under any of the following conditions: (1) When sensing a stimulus or condition for which it was designed to react; (2) if primary power fails; (3) If the detector's circuitry is opened, shorted, or grounded if such condition is capable of compromising the device's normal operation; or (4) If a tamper switch or triggering mechanism is activated. To the extent feasible, the device shall be designed to initiate an alarm if any part or component fails or ages to the extent to render the detector ineffective. Terminals shall be located within the

RELEASED - Printed documents may be obsolete; validate prior to use.

detector enclosure and readily accessible to permit wiring for required combinations of detector units. All controls and terminals which are not required for operation of the detector shall not be readily accessible.

(6) Alarm Monitoring Equipment. The alarm monitoring equipment shall have an access/secure and alarm reset functions. An alarm shall create a lock-on condition which shall require manual restoration, and controls shall be provided to reset the system. When a detector circuit is conditioned for authorized entry into the protected area (Access Mode), the alarm monitoring equipment shall continue to indicate alarms if circuit supervisory limits are exceeded or if any tamper switches are disturbed.

(7) Recording. The alarm monitoring equipment for each system shall have recording capability. The minimum information to be provided for recording shall be: (1) Zone identification; (2) Intrusion; (3) Tamper; (4) Power fail/low battery; (5) Date; and (6) Time.

(8) Circuit Supervisory/Units. The circuit supervisors shall provide security to the communication link between the detectors and/or sensors and the alarm monitoring equipment. Circuit supervision shall be required in wired and wireless systems. Supervision in a wireless system may be achieved either in a full-duplex active mode, or half-duplex timed and coded mode.

b. Interior Intrusion Detection.

(1) Detectors. Detectors shall be Underwriters Laboratory listed and shall be one of the following types:

I - Balanced Magnetic Switch

II - Passive Infrared Detector

III - Vibration Detector

IV - Capacitance Detector

V - Ultrasonic Motion Detector

VI - Microwave Motion Detector

RELEASED - Printed documents may be obsolete; validate prior to use.

VIII - Closed Circuit Television Motion Detector

IX - Conductive Foil

X - Breakwire

XI - Dual Technology

XII - Photoelectric

XIII - Fiber Optic

XIV - Glass Break Detector

(2) Balanced Magnetic Switches (Type I). The switch mechanism shall be of the balanced magnetic type and shall initiate an alarm upon increase, decrease, or attempted substitution of an external magnetic field. The switch and magnet shall be enclosed in separate housings of cast, nonferrous durable material and provide reasonable protection against moisture and dust. The mechanism shall be adjustable from 1/4 inch to 1 inch to accommodate installation variances. The switch shall be electrically protected so that a sudden surge of voltage greater than required for normal operations shall create and alarm. The switch shall be designed so an alarm is initiated whenever the switch housing is moved more than one inch from the magnet housing. When simulating a closed position, the switch shall be rated for a minimum of 500,000 activations without malfunction.

(3) Passive IR Detector (Type II). This detector shall initiate an alarm when a temperature differential between target and background of degrees Celsius or greater occurs within the field of view. The sensor shall detect a person, 5 feet tall weighing 70 pounds, walking at the rate 0.5 to 10 feet per second (FPS) out to a range of at least 30 feet. The system shall stabilize within minutes after being turned on and shall not be capable of being defeated by the use of portable IR absorbent or reflective material placed between the sensor and a person moving in the protected area. The system shall not generate a false alarm as a result of changes in temperature caused by heating, ventilating or air conditioning equipment operation.

(4) Vibration Detector (Type III). This detector shall consist of piezoelectric pickup devices, or an equivalent device, connected

RELEASED - Printed documents may be obsolete; validate prior to use.

through an amplifier/accumulator designed to initiate an alarm signal in response to structurally borne vibration caused by explosion, a short series of blows, a longer series of lighter blows, or similar phenomena. The amplifier/accumulator shall integrate the input stimuli with respect to time, up to the preset alarm level. In addition, the amplifier/accumulator shall be so designed that stimuli of insufficient magnitude to initiate an alarm are bled off to the normal quiescent level at a rate of decay from the level immediately below alarm to 10% to 15% of alarm level in not less than 5, or more than 15, minutes.

(5) Capacitance Detector (Type IV). This detector shall consist of a control unit containing circuitry designed to detect a change in the capacitive coupling which exists between one or more antennas and ground. Antennas shall be energized to create an electrostatic or electromagnetic field, so that if the protected object is touched by a person wearing a heavy glove or approached within 6 inches by a conductive mass of the density and size of a human 5 feet tall, weighing 70 pounds or larger, the capacitive coupling between antennas and ground shall be initiated. The detector shall be designed to disconnect antennas when the detector is in the "access" mode and shall create an alarm when the detector is placed in the "secure" mode.

(6) Ultrasonic Motion Detector (Type V). This detector shall consist of one or more transmitter/receiver elements and the necessary control circuitry. The detector shall sense disturbances in a field (minimum height of field: 8 feet) of acoustic energy above a frequency of 18 KHz. Movement of a human, 5 feet tall, weighing 70 pounds or larger, within the protected area for a distance of 3 feet or more at any velocity between 0.5 fps and 10 fps, shall cause the control unit to initiate an alarm signal.

(7) Microwave Motion Detector (Type VI). This detector shall consist of transmitter/receiver elements and necessary control circuitry to saturate the protected area with electromagnetic energy. Movement of a human 5 feet tall, weighing 70 pounds or larger, within the protected area for a distance of 3 feet or more at any velocity between 0.5 fps and 10 fps, shall cause the detector to initiate an alarm signal. The microwave detectors shall be designed so that nuisance alarms due to electromagnetic emission of other equipment such as fluorescent lights or motors are prevented.

RELEASED - Printed documents may be obsolete; validate prior to use.

(8) Pressure Mat Detector (Type VII). This detector shall be in the form of a flat mat and shall initiate an alarm when a weight of 70 pounds or more is applied to any 3 square-inch top surface of the mat. Detectors shall be resistant to water and dust and the wiring circuitry shall be capable of supervision. The detector shall be rated to withstand no less than 500,000 activations without failure.

(9) Video Motion Detector (Type VIII). This detector shall detect the presence of an intruder by electronically comparing successive scenes for difference in images. An alarm shall be initiated when the compared images differ by more than 6.5%. The detector shall be capable of desensitizing portions of the viewed areas where naturally moving objects occur. Comparison of present video information with previous information shall occur at least twice per second. Failure of the camera shall produce an alarm independent of any detectable scene difference occurring in the secure area. The video motion processor shall be designed to operate with cameras which automatically compensate for scene illumination.

(10) Conductive Foil (Type IX). This material is intended for application to glass and other surfaces to detect intrusion. It is installed and connected into an electrically supervised detector circuit. Breaking or grounding the foil shall cause an alarm to be initiated. Foil shall not exceed 1. pounds in tensile strength and shall be capable of carrying a maximum electrical current of 60 milli-amperes at 60 volts with a temperature rise of not more than 1 degree Celsius. Adhesive and protective coating material necessary for application shall be provided with the foil and shall be of types resistant to aging, moisture, and temperature change. Foil for glass shall be not more than 1/-inch wide. Foil for other purposes shall be not more than 1-inch wide.

(11) Breakwire (Type X). This wire is intended to be used in fabricating screens and grids, open wiring, and grooved striping in various configurations to detect penetrations through movable openings, floors, walls, ceilings, and skylights. When correctly arranged, properly installed, and connected into an electrically supervised detector circuit, cutting, breaking, or grounding the breakwire shall initiate an alarm. Hard drawn breakwire used in fabricating security screens shall not exceed 4.0 pounds tensile strength and shall be able to carry a current of 60 milli-amps at

RELEASED - Printed documents may be obsolete; validate prior to use.

60 volts with a temperature rise of not more than 1 degree Celsius. Wire shall not be larger than 4 AWG.

(1) Dual Technology (Type XI). Dual technology sensors may be any mixture of passive infrared, ultrasonic and microwave elements. Which ever mixture is used, each element must meet the appropriate standards for that technology individually. The dual technology unit must also electronically combine the outputs of the individual elements to minimize false alarms. Each element must be capable of independent testing, zone alignment and verification. The unit must provide independent element failure status indication.

(13) Photoelectric (Type XII). These sensors shall be multibeam modulated type consisting of a minimum of two transmitters and two receivers per set. A photo electric system shall be capable of detecting an individual 5 feet tall, weighing a minimum of 70 pounds passing between the transmitters and receivers at a rate up to 30 feet per second, whether walking, running, jumping, crawling, or rolling. Furthermore, the sensors shall be able to operate as above with an excess gain factor of 0.

Photoelectric sensors shall be installed so that, at any point, the lowest beam is no higher than 9 inches above grade, and the highest at least 63 inches above ground. Sufficient overlap of beams shall exist such that an individual cannot intrude between the beams and remain undetected.

c. Exterior Intrusion Detection.

(1) Systems. Systems used for exterior intrusion detection shall be Underwriters Laboratory listed and be one of the following listed types. Any system/sensor rated for exterior intrusion detection may be used for interior service, where applicable.

I - Mechanical Fence Sensor

II - Electromechanical Fence Sensor

III - Strain Sensitive Cable

IV - Magnetic Point Sensor

V - Magnetic Buried Line Sensor

RELEASED - Printed documents may be obsolete; validate prior to use.

VI - Seismic Buried Line Sensor

VII - Photoelectric Detector

VIII - Microwave Detector

IX - E-Field Detector

X - Video Motion Detector

XI - Passive Infrared Detector

XII - Fiber Optic Sensor

(2) Mechanical Fence Sensors (Type I). This system shall initiate an alarm upon movement of the fence. All sensors in this system shall house adjustable sensitivity mechanical switches with normally opened or closed contacts as specified. The sensors shall be mounted on the fence posts at a maximum of 0 feet apart or every fence post for high security applications. If the sensors are mounted on the fence fabric, they shall be placed at a maximum of 10 feet apart. This system shall employ some count and time criteria in the signal processor to differentiate between intrusions and nuisance indications.

(3) Electromechanical Fence Sensors (Type II). This system shall be capable of initiating an alarm when the sensor is acted upon by accelerations generated in the fence fabric during penetration. Transducers shall be placed on every fence post or on the fence fabric between posts. Each transducer shall be connected in series along the fence with a common cable to form a single zone of protection. The maximum single detection zone shall not exceed 300 feet. The cable shall be routed in sealed conduit and the transducers shall be installed in electrical enclosures. If the cable is installed underground, it shall be either routed in conduit or be direct burial cable.

(4) Strain Sensitive Cables (Type III). This system shall be capable of initiating an alarm when the duration of a series of impulses is exceeded. (This is determined by the sensitivity setting.) Movement of the cable shall produce an output voltage when the cable is moved. Cables shall be fastened directly to the fence using wire ties so movement of the fence fabric is coupled directly to the transducer cable.

RELEASED - Printed documents may be obsolete; validate prior to use.

(5) Magnetic Point Sensors (Type V). This system shall be capable of detecting an individual weighing more than 70 pounds crossing the sensitive area of the system at a minimum speed of 0.5 feet per second, whether walking, crawling, or rolling. The system design shall employ techniques (e.g., electronic signal processing) to eliminate nuisance alarms from adverse environmental phenomena. The sensors shall be installed at a depth below the ground surface stated by the manufacturer. The sensors shall be in two separate parallel lines at a distance of 5 to 6-1/ feet apart. The sensors and electronic circuitry buried in the ground shall be a durable, moisture-proof, rodent-resistant material.

(6) Magnetic Buried Line Sensors (Type VII). This system shall be able to detect a 14-ounce ferrous material rod moving at a rate of 0. feet per second within a radius of 1 foot of a sensor cable. The detection system shall be equipped with inhibitor coils to minimize nuisance alarms due to electromagnetic interference. No more than six sensing loops per inhibitor coil shall be used in order to prevent simultaneous desensitizing of the entire system.

(a) The sensing loops of a electrical cable shall be buried in the ground according to the manufacturer's stated depth. Multiple units (cable and amplifier) shall be used to protect a perimeter. All associated buried circuitry shall be buried within the protected zone and packaged in hermetically sealed containers. The cable shall be laid in accordance with the manufacturer's recommended geometrical configurations to reduce nuisance alarms from external sources. When cable is being installed in rocky soil, care shall be taken to remove sharp rocks during backfilling over the cable. Inhibitors shall be buried in the ground at least 0 feet from the cable inside the protected perimeter.

(b) Continuous electromagnetic interference obstructs the detection of an intruder carrying metal over the buried cable by keeping the inhibitor activated, thereby preventing the alarm unit from responding to a change in flux caused by the intruder. The device shall therefore be used only where the environment is relatively free of severe manmade electromagnetic interference (e.g.,

RELEASED - Printed documents may be obsolete; validate prior to use.

overhead power cables, pole-mounted transformers, generators). The cable shall never be installed close to overhead power transmission lines. Moreover, the cable shall be placed at least 15 feet from parallel running metal fences, and at least 60 feet from public roads to minimize nuisance alarms.

(7) Seismic Buried Line Sensors (Type VIII). This passive system that includes piezoelectric, pressure, geophone sensors or their equivalent. This system shall be capable of detecting an individual weighing more than 70 pounds crossing the sensitive area of the system at a minimum speed of 0.5 ft. per second, whether walking, crawling, or rolling. The system design shall employ techniques to eliminate nuisance alarms from adverse environmental phenomena. The sensors shall be installed at the depth below the ground surface stated by the manufacturer. Detection zones shall extend approximately 40 inches on each side of the buried transducers.

(8) Photoelectric Detector (Type IX). This system shall be a multibeam modulated type consisting of a minimum of three transmitters and three receivers per set. A photoelectric system shall be capable of detecting an individual weighing a minimum of 70 pounds passing between the transmitters and receivers at any velocity up to 30 feet per second, whether walking, running, jumping, crawling, or rolling, or detecting a vehicle 15 feet long traveling 60 mph. Furthermore, the systems shall be able to operate as above with an excess gain factor of 0 to compensate for loss due to atmospheric attenuation at maximum range.

(a) A photoelectric system shall be installed so that, at any point, the lowest beam is no higher than 9 inches above grade and the highest beam at least 63 inches above ground. Sufficient overlap of beams shall exist such that an individual cannot intrude between the beams and remain undetected. The ground areas between the beams must be a constant grade and free of vegetation which could block the beam. A barrier to prevent tunneling under the lower beam is required to a depth of at least 6 inches below grade. This may be accomplished by using concrete, asphalt, or a similar material in a path at least 40 inches wide and 6 inches deep or alternatively 6 inches wide and 40 inches deep between the posts.

RELEASED - Printed documents may be obsolete; validate prior to use.

(b) It is recommended that the photoelectric system be installed inside the physical perimeter barrier with the transmitter and receiver units positioned a minimum of 10 feet from the barrier to prevent intruders from jumping over the beams from the top of the fence into the protected area.

(9) Microwave Detector (Type X). This system shall be capable of detecting an intruder weighing a minimum of 70 pounds passing between the transmitter and receiver at a rate between 0.5 and 15 feet per second, whether walking, running, jumping, crawling, or rolling. The beam shall be modulated and the receiver shall be frequently selective to decrease susceptibility to receiver "capture."

(a) The transmitter and receiver shall be installed on even terrain clear of trees, tall grass, and bushes. Each unit shall be mounted rigidly at a distance of about 40 inches above the ground. Because of variances in the antenna pattern of different microwave systems, this height may have to be varied slightly in order to obtain proper ground coverage. The distance between a transmitter and its receiver shall be in accordance with the manufacturer's specifications and site-specific requirements. Neither the transmitter nor the receiver shall be mounted on a fence. To prevent passage under the microwave beam in the shadow of an obstruction, hills shall be leveled, ditches filled, and obstructions removed so that the area between transmitter and receiver is clear of obstructions and free of rises or depressions of a height or depth greater than 6 inches. The clear areas shall be sufficiently wide to preclude generation of alarms by objects moving near the microwave link (e.g., personnel walking or vehicular traffic). Approximate dimensions of the microwave pattern shall be provided by the manufacturer.

(b) If the microwave link is installed inside and roughly parallel to a perimeter fence or wall, the transmitter and receiver shall be positioned to prevent an intruder from jumping over the microwave beam into the protected area from atop the fence or wall. Typically, a chain link security fence with an overall height of 8 feet shall require a minimum of 7 feet between the fence and the center of the microwave beam.

RELEASED - Printed documents may be obsolete; validate prior to use.

(c) Provisions shall be made for adjusting the sensitivity to intruder motion, range, or both, to cover areas of various sizes and configurations.

(10) E-Field Detector (Type XI). This sensor shall initiate an alarm with an individual weighing a minimum of 70 pounds and at least 0 inches from the sensing wire, whether crawling or rolling under the lower sensing wire, stepping and jumping between the field and sensing wires, or jumping over the top sensing wire of the system. The field and sensing wires should be supervised to prevent the undetected cutting or bypassing of the system. The system design shall employ techniques to minimize alarms caused by high winds, thunderstorm related electrical phenomena, high winds, and small animals.

(11) Video Motion Detector (Type XII). This system shall detect the presence of an intruder by electronically comparing successive scenes for difference in images. An alarm shall be initiated when the compared images differ by more than 6.5 percent. The detector shall be capable of desensitizing portions of the viewed areas where naturally moving objects occur. Comparison of present video information with previous information shall occur at least twice per second to prevent high speed, undetected, pass through. Failure of the camera shall produce an alarm independent of any scene differences occurring in the secure area. The video motion processor shall be designed to operate with cameras which automatically compensate for scene illumination.

(1) Passive IR Detector (Type XIII). This detector shall initiate an alarm when a temperature differential between target and background of degrees Celsius or greater occurs within the field of view. The sensor shall detect a person, 5 feet tall, weighing 70 pounds, walking at the rate of 0.5 to 10 feet per second, out to a range of at least 50 feet. The system shall stabilize within minutes after being turned on and shall not be capable of being defeated by the use of portable IR absorbent or reflective material placed between the sensor and a person moving in the protected area.

(13) Fiber Optic Sensor (Type XIV). Laser Powered systems which use inteferometric sensing to disturbance of buried or non buried fiber optic sensing cable in order to detect intrusion within a zone of protection. Individual zones shall be determined by

RELEASED - Printed documents may be obsolete; validate prior to use.

the object or area being protected. The system shall detect a person weighing 70 pounds or more passing through the sensitive area at speeds 0.5 feet per second or greater, whether walking, crawling, running or rolling. The system shall employ techniques which eliminate false alarms which are due to environmental phenomena and seismic vibrations from nearby vehicles or other sources. The system shall contain self-diagnostic reporting circuitry. The sensing fiber shall withstand normal vehicular drive over without damage or degradation of performance, whether used in clear zone applications or tactical deployment scenarios. When applied to fences, the fiber optic sensor shall detect a person attempting to climb out, or lift the fence fabric.

8.6 CLOSED CIRCUIT TELEVISION (CCTV)

a. Unless specially warranted, CCTV systems shall be color, where possible.

b. CCTV components shall be supervised and designed to resist or report tampering.

c. When appropriate and cost effective, CCTV should incorporate pan, tilt and zoom features to improve the security monitoring capabilities.

d. Appropriate illumination shall be provided for the area under CCTV observation. This requires an examination of the CCTV system parameters and of the operational requirements.

e. Cameras shall be installed to have an unobstructed view of the area under observation.

f. Topographic and environmental factors shall be considered in designing CCTV systems.

g. In low light areas, where additional lighting is inappropriate or prohibited, special low light level cameras must be used.

h. When stipulated, CCTV should be recorded on a video cassette recorder (VCR).

8.7 ACCESS CONTROL SYSTEMS (ACS)

RELEASED - Printed documents may be obsolete; validate prior to use.

a. Types: There are generally three types of access control systems: (1) manual, (2) machine-aided manual, and (3) automated. Although there can be a wide variation in technical complexity and cost, an equal level of security can be provided by each of these systems. The type of system used depends on a number of factors, such as:

(1) Number of personnel requiring access.

(2) Frequency of access.

(3) Type of facility (research, development, production, or operations).

(4) Classification of facility (critical, essential, support).

(5) Types of additional safeguard measures utilized.

(6) Compatibility with existing KSC-wide systems.

(7) Operations and maintenance requirements.

b. Since these factors are site-specific considerations, no single system can be recommended for universal use. A system which is well suited for one facility may be totally unsuited for use at another or incompatible with existing Centerwide systems. An examination of all factors must be made before determination of the type of access controls best suited to a facility.

8.8 SYSTEM UPGRADE

Where existing systems do not meet the revised standards, there is no requirement or funding authorized to upgrade the systems solely to meet the new standards.

CHAPTER 9. COMMUNICATION SECURITY

9.1 GENERAL

This chapter establishes the responsibilities and provides procedural requirements for implementation of a comprehensive Communication Security (COMSEC) Program at KSC.

9.2 RESPONSIBILITIES

a. The NASA/KSC COMSEC Officer is responsible for:

RELEASED - Printed documents may be obsolete; validate prior to use.

(1) Managing development, implementation, and execution of the KSC COMSEC Program to include COMSEC configuration control.

(2) Establishing all requirements for secure communications systems including Data Encryption Standard (DES) requirements and Public Key Cryptography (PKC).

(3) Providing management oversight of the KSC STE and STU-III system to include evaluating all requests for installation, periodic inspection and inventory of STE and STU-III terminals to ensure that security requirements are being met. Function as STE and STU-III user representative for KSC.

(4) Requisitioning materials and establishing methods for design, test, inspection and evaluation of secure communications systems.

(5) Approving all cryptographic systems (encryption devices, decryption devices, and keying material) including DES and PKC equipment and keying materials, prior to system installation and activation.

(6) Ensuring compliance with this chapter's requirements as follows:

(a) Review and approve Tier I/II and review Tier III/IV security plans, OMI's, and other documentation which covers installation and operation of secure communications systems prior to implementation of such systems.

(b) Conduct scheduled and unscheduled inspections of secure communications systems, facilities, and areas where classified information is processed.

(c) Appoint the NASA/KSC COMSEC Account Manager (CAM) and alternate(s).

(d) Evaluate each secure communications system to ensure that COMSEC measures are correctly applied and to ensure that COMSEC plans, procedures, and operations are integrated with the KSC Security Program.

RELEASED - Printed documents may be obsolete; validate prior to use.

(e) Review requests for waiver or exception to provisions of this chapter and submit them, with recommended course of action, to the Installation Security Officer.

(f) Act as the interface between NASA/KSC, the NASA Central Office of Record (COR), the National Security Agency (NSA), and other Government departments and agencies for obtaining technical direction and requirements on all COMSEC matters, including procurement of COMSEC equipment and keying material.

(7) Overseeing all contractor COMSEC accounts under purview of KSC; conducting periodic inspections to ensure Government regulations are being complied with; and maintaining a master inventory of all COMSEC account holdings.

(8) Appointing a cryptonet controlling authority, in writing, for each cryptonet under KSC purview.

(9) Administering a COMSEC training program at KSC.

b. The NASA/KSC COMSEC Account Manager and Alternate(s) are responsible for:

(1) Receiving, storing, shipping, and accounting for all COMSEC material issued to the NASA/KSC account, and maintaining accurate records of these transactions.

(2) Preparing and submitting COMSEC Material Reports as required.

(3) Conducting all required COMSEC inventories.

(4) Ensuring that amendments, corrections, and changes to COMSEC publications are entered correctly without undue delay.

(5) Ensuring that COMSEC material is available to properly cleared individuals who have a valid need to know. A record of material issued from the KSC COMSEC account shall be maintained.

RELEASED - Printed documents may be obsolete; validate prior to use.

(6) Administering COMSEC briefings to individuals whose duties require access to COMSEC materials and maintaining associated records.

(7) Performing routine destruction of superseded COMSEC material.

(8) Reporting any known or suspected COMSEC insecurity as required by applicable directives.

(9) Performing other COMSEC accounting duties as outlined in NHB 1600.6, and as directed by the NASA Central Office of Record.

c. Heads of Primary Organizations are responsible for:

(1) Ensuring that secure communications systems are approved by the NASA KSC COMSEC Officer prior to commencing classified or unclassified sensitive operations.

(2) Ensuring compliance with all security requirements, standards, and procedures applicable to secure communications systems; and ensuring that only COMSEC materials distributed through the COMSEC Material Control System, or as approved by the NASA KSC COMSEC Officer, are used.

(3) Appointing a COMSEC representative who is appropriately cleared and briefed.

(a) Ensuring that each COMSEC representative performs his or her duties effectively in accordance with applicable requirements and standards.

(b) Ensuring that each COMSEC representative has written authorization to suspend COMSEC support or service to any user not adhering to security regulations and procedures.

(4) Preparing and submitting cryptographic system requirements, security plans, operating procedures, and other secure communications system documentation to the NASA/KSC COMSEC Officer for review.

RELEASED - Printed documents may be obsolete; validate prior to use.

Note: Care must be taken to forecast cryptographic system requirements well in advance of the need date. COMSEC equipment, unlike other types of hardware, is produced and procured to match actual requirements, and is not bench stocked. The contracting and manufacturing process normally takes approximately years from the date of funding. The length of this acquisition cycle shows the importance of forecasting COMSEC equipment requirements as early and as accurately as possible.

(5) Providing technical assistance or resources to assist the NASA/KSC COMSEC Officer in managing the KSC COMSEC Program.

(6) Ensuring that security requirements are considered from the conceptual stage for all new facilities, systems, and applications through which classified or sensitive information is to be processed.

(7) Ensuring that the NASA/KSC COMSEC Officer's involvement and concurrence is obtained from the conceptual stage for all COMSEC systems.

d. COMSEC Representatives are responsible for:

(1) Serving as focal points for all COMSEC matters within a particular facility, activity, or organization.

(2) Preparing COMSEC plans, procedures, OMI's, and other documentation for installation and operation of secure communications facilities under their purview.

(3) Conducting periodic inspection of communications facilities to ensure compliance with the requirements of this chapter and other applicable directives.

(4) Preparing requests for waiver or exception to provisions of this chapter and submitting them to the NASA/KSC COMSEC Officer.

(5) Assisting the COMSEC Officer, as required, in administering a COMSEC training program.

9.3 OBJECTIVES

RELEASED - Printed documents may be obsolete; validate prior to use.

a. National Policy. The National Communications Security Committee (NCSC) established broad policies for protection of national security information processed by communications systems. The Director, NSA, is the Federal Government's Executive Agent for COMSEC, and has published a series of documents designed to implement national policies. The objective of the U.S. COMSEC effort is effective and efficient application of security measures to all communications of the U.S. Government.

b. STE and STU-III Technology. The Federal Government has long recognized the most severe threat to the security of classified and sensitive information is our telecommunications habits and practices. Substantial amounts of classified and sensitive information are leaking to our adversaries over nonsecure telecommunications (telephone) circuits. The STE and STU-III provides a low-cost, user-friendly system to protect both classified and sensitive unclassified Government information. KSC fully supports National policy, which encourages the widespread implementation and use of the STU-III.

c. KSC Objectives. KSC shall support the national COMSEC effort through adherence to national policies and NSA doctrine.

9.4 COMSEC PROGRAM

There are a number of disciplines which, when combined, constitute a COMSEC program. The following elements and requirements constitute the COMSEC Program at KSC.

a. Cryptographic Security. All communications networks, systems, and circuits (including voice, teletypewriter, data, telemetry, television, and facsimile) used to transmit national security and sensitive information shall be secured with approved COMSEC equipment. All COMSEC equipment and keying materials, including DES and PKC, must be approved by the NASA/KSC COMSEC Officer prior to installation and use.

b. Physical Security. COMSEC material requires physical protection over and above that provided to most other classified material. The loss of certain COMSEC materials could result in compromise of all classified or sensitive information transmitted over circuits protected by the material. All persons responsible for COMSEC material must comply with applicable physical security regulations.

RELEASED - Printed documents may be obsolete; validate prior to use.

c. Transmission Security. Measures must be taken to protect transmissions from interception and exploitation, by means other than cryptanalysis. Examples of poor application of transmission security are:

(1) A sudden activation or increase in communications activities just prior to an event.

(2) Improper use of code systems or use of homemade codes.

d. Emission Security. Control of compromising emanations (TEMPEST) is covered in detail in Chapter 10 of this KNPR. TEMPEST is mentioned here since it is a basic element of COMSEC. The provisions of NSTISSAM TEMPEST -95 should be followed for facility design and equipment installation. However, due to ever changing federal standards on TEMPEST requirements, all TEMPEST discussions concerning equipment installation and facility design shall include the KSC TEMPEST Officer.

9.5 COMSEC EQUIPMENT MAINTENANCE

COMSEC equipment is designed to provide security to communications. Maintenance of this equipment by certified technicians is accomplished within specified requirements as authorized by interagency agreements, NSA instructions, and other applicable documents. Maintenance is defined as:

a. Limited. Maintenance performed at KSC. Persons designated to perform limited maintenance must complete approved COMSEC maintenance training courses and be formally certified prior to assuming maintenance duties.

b. Depot. Maintenance performed at an authorized crypto repair facility.

9.6 COMSEC MATERIAL CONTROL SYSTEM

COMSEC material is distributed to users through the COMSEC Material Control System. Only those materials distributed through the CMCC may be used to protect classified or unclassified sensitive information.

9.7 EMERGENCY PLANNING AND ACTIONS

All organizations conducting COMSEC operations or holding classified COMSEC material must consider the possibility of an emergency arising which would expose COMSEC materials to possible compromise. An emergency action plan must be made which shall prevent entirely, or at least

RELEASED - Printed documents may be obsolete; validate prior to use.

minimize, the extent and effect of compromise. The COMSEC Emergency Action Plan must be coordinated with the overall facility or activity emergency plan to ensure harmony of actions during emergencies. COMSEC Emergency Action Plans shall be submitted to the NASA/KSC COMSEC Officer for review and approval prior to implementation.

a. Emergency Action Plan.

(1) When preparing an emergency action plan, there are two basic types of emergencies to consider: (1) accidental occurrences and (2) hostile action. The first includes natural disasters (such as, earthquake, flood, hurricane, and tornado) and manmade accidents (such as, explosion and fire). The second is hostile action of malcontents. The primary goal of an emergency action plan is to ensure that classified COMSEC material is safeguarded at all times through proper storage or through destruction.

(2) All personnel involved with COMSEC operations must be indoctrinated in step-by-step emergency procedures. Routine training exercises should be conducted frequently (once each quarter is recommended) to ensure that all personnel are completely familiar with action to be taken during an emergency.

(3) The emergency action plan shall designate specific facility management officials empowered to direct execution of the plan in an emergency.

b. Notification. Immediately upon executing an emergency action plan, the person responsible shall notify the NASA/KSC COMSEC Officer and the CAM who issued the COMSEC material involved.

c. Emergency Action. Plans for protecting COMSEC material during an emergency should include the following actions:

(1) Securing the material.

(a) Zeroize all cryptographic equipment or remove keying material from equipment and store in a safe. Secure all other classified COMSEC material, except bulky equipment, in a safe. Lock the doors of all rooms or vaults containing COMSEC material, except in case of fire.

RELEASED - Printed documents may be obsolete; validate prior to use.

(b) Secure all power within the COMSEC room or vault before leaving.

(c) Post a guard in the area, if feasible.

(d) Upon return, conduct an inventory of all COMSEC material. Missing material must be reported immediately to the NASA/KSC COMSEC Officer and the CAM who issued the material.

(e) In the event of fire, life safety is the primary consideration. Every reasonable effort to properly secure all classified material, especially COMSEC material, should be made prior to permitting fire personnel to enter; however, inability to secure classified material must NOT preclude entry of fire personnel.

(2) Removing the Material. This course of action is preferred over destroying COMSEC material if time and conditions permit.

(3) Destroying the Material. Implements and methods for rapid destruction of equipment and material shall be available if the decision for destruction is made.

d. Combining Actions. It may be desirable in certain situations to combine some or all actions listed above. For example, if it appears a civil uprising shall be short lived and the COMSEC room is to be abandoned for a short period, superseded material may be destroyed, all other material removed, and the equipment made secure.

e. Reducing COMSEC Inventory in Anticipation of an Emergency. It may be advisable to reduce the COMSEC inventory in anticipation of an emergency. This is accomplished by retaining current keying material (to ensure continued communications until the last moment) and destroying or relocating all other material. If destruction of future (reserve on board) keying material is directed, the issuing office must be advised so immediate replacement can be made after the danger has passed.

9.8 COMSEC EVALUATIONS

a. A general inspection of each COMSEC facility and each COMSEC account shall be conducted at least annually by the NASA/KSC COMSEC Officer or his/her designated representative. The inspection shall include all aspects of COMSEC. A letter report which lists

RELEASED - Printed documents may be obsolete; validate prior to use.

deficiencies requiring corrective action shall be prepared and forwarded to the CAM and the COMSEC representative.

b. CAMs and users of COMSEC material may use the COMSEC Checklist, as a guide when conducting self-inspections. Self-inspections should be conducted periodically as an element of COMSEC account administration. The COMSEC Checklist, although comprehensive, is intended as a guide and may not include all aspects of the inspection.

9.9 COMSEC AWARENESS

a. Each individual with access to COMSEC material must be made aware of the special sensitivity and handling COMSEC material requires. Prior to being granted access to COMSEC material, each individual must be fully briefed on all aspects of COMSEC sensitivity. At KSC, this is accomplished through a series of briefings arranged by the NASA/KSC COMSEC Officer and through the respective efforts of each organization to which this chapter applies.

b. It is not practical to identify COMSEC awareness requirements here. Rather, each organization shall implement an awareness program commensurate with the COMSEC requirements under which it operates.

9.10 COMSEC TRAINING

a. COMSEC training for all users of KSC communications systems may be scheduled by calling the NASA/KSC COMSEC Officer, 867-45.

b. Maintenance training is provided for individuals working with COMSEC equipment. All personnel who maintain or install COMSEC equipment must have a current certification of training and proficiency. Submit written requests for formal training to the NASA/KSC COMSEC Officer.

c. Documentation of training shall be maintained in accordance with applicable regulations. COMSEC training records shall be a subject of inspection during various COMSEC evaluations.

CHAPTER 10. TEMPEST--CONTROL OF COMPROMISING EMANATIONS

10.1 GENERAL

RELEASED - Printed documents may be obsolete; validate prior to use.

a. This chapter provides requirements for establishing a special TEMPEST program for NASA and NASA contractor facilities located on KSC and at all other off-Center areas under the cognizance of KSC; i.e., Cape Canaveral Air Force Station and Patrick Air Force Base.

b. All TEMPEST decisions covering equipment installation and facility design shall include the KSC TEMPEST Officer.

10.2 RESPONSIBILITIES

The NASA/KSC TEMPEST Officer, a member of the Protective Services & Safeguards Office, is responsible for:

a. Functioning as the primary point of contact on all matters relating to TEMPEST at KSC. This includes ensuring that the national-level TEMPEST policies are properly addressed and included in the overall TEMPEST program at KSC.

b. Coordinating KSC's TEMPEST efforts with appropriate U.S. Government agencies and with the security elements of KSC tenants, both Government and contractor, by participation in design reviews during the engineering phase of projects involving RED/BLACK systems/facilities/equipment.

c. Ensuring that equipment, systems, and facilities used for secure (RED) operations at KSC conform to the appropriate design, acquisition, construction, installation, modification, and/or relocation requirements/criteria.

d. Determining the necessity of and arranging for all TEMPEST tests which involve KSC equipment, systems, and/or facilities.

e. Processing deviations to the TEMPEST standards established for KSC, recommending appropriate action and disposition of such deviations to the appropriate approval authority.
Note: Caution should be exercised with regard to deviations and waivers as they may constitute vulnerabilities and subsequently require classification. Coordination with the TEMPEST Officer prior to preparation of any documentation should result in the safeguarding of potentially damaging information. These subjects are not to be discussed telephonically unless it is done on a secure communications network.

f. Providing requirements and assistance to all KSC organizations on TEMPEST matters.

RELEASED - Printed documents may be obsolete; validate prior to use.

g. Investigating and making appropriate disposition of all instances of noncompliance with TEMPEST standards/instructions/procedures.

h. Participating in periodic examination of KSC facilities, equipment, systems, or components for compliance with TEMPEST standards.

i. Acting as the point of contact for coordination of formal TEMPEST training for NASA/KSC Employees and KSC contractors.

10.3 TEMPEST

a. Compromising Emanations. Electronic and/or electromechanical equipment used for information processing may produce compromising emanations. These are defined as unintentional data-related and/or intelligence-bearing signals which, if intercepted and analyzed, would disclose classified information that is being transmitted, received, handled, or otherwise processed by the equipment. It has been established that such compromising signals can be propagated through space and along nearby conductors. TEMPEST is the unclassified name referring to investigations and studies of compromising emanations.

IAW NSTISSI No. 7000, TEMPEST efforts to control compromising emanations must be incorporated into equipment design, facility construction, and system layout/installation.

b. No RED systems, equipment, or components may be placed in service or restored to service after repair/modification without the concurrence of the NASA/KSC TEMPEST officer. This is formally accomplished by the TEMPEST officer's assessment during the continuing security compliance/configuration management process. This applies to such items as:

(1) Secure automated information processing systems.

(2) Electric typewriters, word processors, and audio/video recording/playback devices used for RED processing and/or presentations.

(3) Secure telephone, teleconference, communications equipment (such as, headsets and microphones), and facsimile systems used for RED processing.

RELEASED - Printed documents may be obsolete; validate prior to use.

(4) Cryptographic systems and related equipment/components.

c. Once approved for secure (RED) processing, all systems/equipment/components must be properly protected/controlled to assure that security integrity is maintained. Access to controlled space containing RED processors shall be strictly controlled. Access to, and work performed upon, RED systems equipment or components shall be limited to cleared personnel having a valid need for such access. Modification, reconfiguration, or moving of any previously approved RED equipment shall be handled with the NASA/KSC TEMPEST Officer's signature/concurrence.

d. Certain secure telephone systems, such as the Secure Telephone Unit, (STU-III), are capable of operation in both BLACK and RED modes.

CHAPTER 11. TECHNICAL SURVEILLANCE COUNTERMEASURES

11.1 GENERAL

a. The primary objective of the Technical Surveillance Countermeasures (TSCM) program at KSC is to locate and neutralize technical surveillance devices that have been targeted against KSC facilities/interests. The secondary objective is to identify and enable the correction of vulnerabilities. TSCM services shall be used to accomplish these objectives.

b. The purpose of TSCM services is to provide an extra level of protection to established security areas likely to be targets of technical surveillance penetrations. These surveys augment normally sound security practices and are not substitutes for other proper measures (access controls, physical security, etc.). They are not compliance-oriented administrative inspections and should not be considered as such. They are highly specialized counterintelligence investigations conducted by specially trained TSCM personnel only.

11.2 RESPONSIBILITIES

The TSCM Program Manager, a member of the Protective Services & Safeguards Office, is responsible for:

a. Conducting TSCM services at facilities under the cognizance of KSC.

b. Investigating the discovery of actual and suspected technical surveillance devices in facilities under the cognizance of KSC.

RELEASED - Printed documents may be obsolete; validate prior to use.

Coordinating such investigations with DoD, FBI, and other Government agencies. Rendering reports, as appropriate.

c. Ensuring that areas used for classified and/or sensitive discussions/presentations conform to adequate and appropriate technical security standards.

11.3 REQUIREMENTS

a. Secure Discussion/Presentation Areas. The generic NASA standards for secure conference rooms are contained in NHR 1600.1. These standards apply to all KSC elements, including contractors, and shall be used as requirements in establishing any facility that may be subject to recurring TSCM surveys. The TSCM Program Manager shall be contacted for any interpretation of the NASA standards, including protective measures for telephones.

b. TSCM services at KSC areas or areas under the cognizance of KSC shall be coordinated and conducted by the TSCM Program Manager only.

c. Sponsors of classified/sensitive briefings, conferences, and symposia must make every effort to hold these gatherings in secure discussion areas. However, when the number of attendees exceeds the capabilities of any available secure areas, a limited TSCM service may be provided to protect the event to the maximum extent possible.

d. Radios, two-way transceivers, pagers, beepers, recording devices, laptop computers, and similar electronic devices represent technical security vulnerabilities by inherent design characteristics. They are, therefore, prohibited in those areas subjected to recurring TSCM surveys. Exceptions may be permitted on a case-by-case basis by the Center Chief of Security.

e. Requests for TSCM services should be treated as sensitive/proprietary information and handled in a secure manner.

11.4 PROCEDURES

The following procedures are intended for the use of those individuals responsible for a particular building/site, program, or activity in which classified and/or sensitive (i.e., proprietary) information is or shall be used.

RELEASED - Printed documents may be obsolete; validate prior to use.

a. Identify those areas where the following information is or shall be routinely discussed or presented in audible or visual format:

(1) Classified information.

(2) Certain unclassified proprietary information; such as, significant procurement actions and major contractual bids, negotiations, and awards.

b. Request the NASA TSCM Program Manager to arrange a TSCM survey or monitor. Since the request shall be treated as a sensitive matter, it may not be made over an unsecure telephone. Even if an approved secure telephone is available in the area to be surveyed, do not use it to request a TSCM survey for that area.

11.5 DISCOVERY OF DEVICES/SUSPECT DEVICES

Whenever an actual or suspected device is discovered in any KSC facility or facility under the cognizance of KSC, it is imperative that the following actions be taken:

WARNING

a. Do not touch or disturb the device in any manner. Leave this to electronics and explosives experts. Devices can and have been booby trapped.

b. Do not attempt to remove it or analyze it.

c. Immediately establish physical control over the area to prevent the removal of the device by those who installed it and to prevent access by the curious.

d. Allow no verbal comments in the area that would in any way disclose the fact that a device has been found. This could negate any further efforts to identify and prosecute those responsible.

e. Immediately notify the TSCM Program Manager by secure means.

CHAPTER 12. LAW ENFORCEMENT

12.1 GENERAL

This chapter is to describe the law enforcement functions, relations, duties, responsibilities, and jurisdictions which are in effect at the KSC.

RELEASED - Printed documents may be obsolete; validate prior to use.

12.2 LAW ENFORCEMENT DUTIES

Nothing within this KNPR shall be construed to obviate the role, responsibilities, and authorities of the Office of the Inspector General as contained in appropriate NASA Management directives.

a. The Protective Services & Safeguards Office shall:

(1) Be the initial focal point for all matters involving law enforcement for KSC.

(2) Ensure in its oversight role to the security and law enforcement portion of the J-BOSC that the contractor provides sufficient qualified officers to perform the law enforcement function on KSC.

(3) Establish and maintain liaison with the local, State, and Federal law enforcement community.

(4) Formulate mutual aid agreements, letters of understanding, or other obligatory instruments affecting the disposition of KSC's security assets on KSC or within the local community, and the use of local assets on the Center.

(5) Develop the strategy and philosophy for protection of assets on KSC and for the enforcement of laws pertaining to the Center.

(6) Develop and implement a system to deal with violations or noncompliance by companies not under the jurisdiction of the J-BOSC.

b. The J-BOSC shall, within the limits of its contract with NASA and, with the approval and coordination of The Protective Services & Safeguards Office:

(1) Provide sufficient officers qualified for deputization by the Brevard County Sheriff's Office, and cooperate with the Sheriff's Office in achieving deputy status for those officers.

(2) Provide sufficient training to designated deputized officers so that traffic accidents may be investigated, traffic laws may be enforced, and analysis for intoxicants and drug use can be

RELEASED - Printed documents may be obsolete; validate prior to use.

conducted. The J-BOSC shall provide appropriate procedures, training, certification, and equipment for this testing.

(3) Enforce all Florida statutes and laws on KSC through a procedure of investigations, apprehension/arrest, and prosecution by the State Attorney's Office.

(4) Provide training for all officers assigned law enforcement duties, to include basic law enforcement training, the use of force, application of State laws, report writing, crime scene, evidence handling, etc.

(5) Develop, with the concurrence of The Protective Services & Safeguards Office, procedures for the application of law enforcement on KSC. These should include, but not be limited to:

(a) Use of force.

(b) General firearms policy.

(c) Reporting, handling, and documentation of incidents.

(d) Operation and maintenance of sobriety test equipment.

(e) Crime scene procedures.

(f) Traffic crash investigation.

(6) Provide appropriate administrative support for the law enforcement function, including the storage and retrieval of arrest records, accident investigations, and traffic citation records. The offices conducting this administrative support shall conduct liaison with State agencies as is required by state law.

c. Directors of first-line directorates and staff offices shall appoint, as a minimum, a security officer or security point of contact for law-enforcement-related issues. This person shall, as a minimum:

(1) Interface with both the Protective Services & Safeguards Office and J-BOSC Security.

(2) Ensure that the directorate/office complies with the provisions of all security directives/regulations applying to KSC.

RELEASED - Printed documents may be obsolete; validate prior to use.

(3) Be the point of contact to both the Protective Services & Safeguards Office and J-BOSC Security in the processing of traffic and criminal violations or incidents involving his/her organization's employees on KSC.

(4) Coordinate, through the Protective Services & Safeguards Office, the development of a program of progressive sanctions to be taken in the event of criminal violations to include, if appropriate, termination.

(5) Coordinate, through the Protective Services & Safeguards Office, the development of a program to observe, recognize, and deal with substance abuse within the organization.

(6) Formulate a crime prevention program for his/her respective organization. This program shall have as its objective the dissemination of information that shall result in the reduction of crime through preventive measures.

(7) In conjunction with Protective Services & Safeguards Office and J-BOSC Security, develop and implement a program designed to educate the employees in what is expected of them as part of the law enforcement program for KSC. The program shall include basic security philosophy and information concerning topics such as theft, substance abuse, and driving while under the influence of intoxicants.

d. KSC contractors shall, within the limits of their contracts or subcontracts, appoint, as a minimum, a company security officer or security point of contact for law-enforcement-related issues. This person shall, as a minimum:

(1) Interface with the Protective Services & Safeguards Office and J-BOSC Security.

(2) Ensure that the company complies with the provisions of all law enforcement instructions and regulations applying to KSC.

(3) Be the point of contact for both The Protective Services & Safeguards Office and J-BOSC Security in the processing of traffic and criminal violations or incidents involving his/her company's employees on KSC.

RELEASED - Printed documents may be obsolete; validate prior to use.

(4) Develop a program of progressive sanctions to be taken in the event of criminal violations. The company must be prepared to take appropriate action against an employee, up to and including termination.

(5) Formulate a crime prevention program. This program shall have as its objective the dissemination of information that shall result in the reduction of crime through preventive measures.

(6) In conjunction with The Protective Services & Safeguards Office and J-BOSC Security, develop and execute a program designed to educate the employee in what is expected as part of the security program for KSC.

(7) Develop a program to observe, recognize, and deal with substance abuse on KSC.

12.3 JURISDICTION

The Florida Deeds of Dedication gives the National Aeronautics and Space Administration (NASA) a proprietorial interest in KSC property. This authority is based primarily upon State and Federal statutes. Similar to other land owners in the State of Florida, NASA must rely upon properly deputized officers of the State or county to enforce State laws and upon Federal officers to enforce Federal laws. In agreement with the Brevard County Sheriff's Office, the J-BOSC shall obtain and maintain deputization for designated officers performing law enforcement duties on KSC. The deputized officers are empowered as J-BOSC Security/Special Deputies and are authorized to conduct all law enforcement activities, including arrests on KSC, within the limits of the Florida State Statutes (see paragraph 401.3b.(1) below). NASA Federal Law Enforcement Officers shall, under applicable law, intervene in the commission of a felony and shall, within the confines of KSC, hold suspects until a deputized officer can respond to affect an arrest.

a. Federal Agencies. The Federal agencies listed and described below have jurisdiction at KSC as indicated:

(1) Department of the Interior. Congress has granted the Secretary of the Interior authority to use and administrative authority over, all land, submerged land, and waters within the perimeter of KSC. National Park Service, U.S. Fish and Wildlife Service, and Canaveral National Seashore officials have responsibility to control access to the National Seashore; to construct, alter, operate, and maintain dikes, impoundments, and water control; and to enforce all rules and regulations governing the use of

RELEASED - Printed documents may be obsolete; validate prior to use.

land and the protection of natural resources and wildlife. These officers enforce Federal statutes regarding trespass, traffic, and criminal acts. The National Park Service enforces the provisions of Title 36 CFR, while the U.S. Fish and Wildlife Service enforces those found in Title 50 CFR. Separate agreements have been promulgated between NASA and these agencies concerning lines of jurisdictional responsibility, mutual assistance, and coordination.

(2) Federal Bureau of Investigation (FBI). FBI agents enforce the United States Criminal Codes. In addition, the Bureau provides investigatory support to NASA in cases of espionage, sabotage, and theft of government property. They also are available to support anti or counter-terrorist situations affecting the Center.

(3) United States Customs Service (USCS). The primary interface KSC has with the Customs Service is in the area of recovered contraband. Contraband found on the Center or on the persons of individuals apprehended who are believed to be transporting it illegally from outside the continental United States is released to the USCS. Individual(s) apprehended under such circumstances are released to the Customs Service for their disposition. Additionally, hardware and other equipment associated with payload operations may be subject to inspection and/or review by USCS at KSC and other facilities under KSC cognizance.

(4) United States Secret Service. The Secret Service's two main areas of responsibility are the protection of selected high ranking government officials (both U.S. and foreign) and the investigation of crimes involving counterfeiting of U.S. currency. In both of these areas, KSC works closely with the Service. Close contact with the Orlando office of the Secret Service is accomplished by The Protective Services & Safeguards Office.

(5) United States Department of State. Officials of the U.S. or foreign governments on official or unofficial state visits to this country come under the protection of the Department of State. The Department of State is also called upon to provide liaison with foreign governments for NASA at contingency landing sites worldwide.

(6) U.S. Coast Guard. The United States Coast Guard is responsible for providing security support during launch and

RELEASED - Printed documents may be obsolete; validate prior to use.

landing operations. This includes enforcing the off coast Security Zone beginning upon rollout and continuing until a "No Return to Launch Site" is declared and resuming 3 hours prior to landing until released after a safe landing. They also patrol island waters (the Banana River south of the NASA Causeway and the Mosquito Lagoon north of Haulover Canal) using the Coast Guard Auxiliary.

(7) Other Federal Agencies. The Protective Services & Safeguards Office is the single point of contact for the agencies listed above and all other Federal agencies in matters pertaining to crime on the Kennedy Space Center or property under the cognizance of KSC worldwide.

(8) NASA Inspector General. The NASA Inspector General is responsible to NASA Headquarters for investigating all allegations of fraud, waste, and abuse on KSC as contained in NASA Management directives.

b. The Brevard County Sheriff's Office. As described below, has stated jurisdiction over the Kennedy Space Center:

(1) The Brevard County Sheriff is required by law to enforce Florida State Statutes in Brevard County, which includes most of the Kennedy Space Center. (A small portion of the Center is in Volusia County. The Volusia County Sheriff has jurisdiction in this area.) Through an agreement between NASA and the Sheriff, the Sheriff shall deputize selected members of the J-BOSC Security force who meet the minimum standards required by the State for law enforcement officers. These J-BOSC Security/KSC Reserve Deputies are empowered to enforce Florida law on KSC. The Brevard County Sheriff's Office (BCSO) works closely with The Protective Services & Safeguards Office in enforcing Florida State Criminal Statutes on the Center, investigating capitol crimes, and arresting wanted persons on the Center.

CHAPTER 13. PROTECTIVE FORCES

13.1 GENERAL

a. This chapter establishes standards at KSC for protective forces under contract to NASA. Protective forces subject to this document are to protect NASA employees and security interests, primarily space

RELEASED - Printed documents may be obsolete; validate prior to use.

vehicles, facilities, and associated hardware, on KSC. Assets shall be protected against theft, sabotage, and other hostile acts that may cause adverse impact to the U.S. space program, national security, or the health and safety of employees or the public.

b. A protective force consisting of armed security officers and support personnel is required as provided by in the J-BOSC. This force shall protect NASA/KSC assets as provided in this document, in the NASA Resource Protection (NRP) Plan, and as directed by the NASA Contracting Officer and the Contract Manager's Representative (CMR).

c. As a minimum, there shall exist the following elements for KSC security:

(1) Personnel to provide the armed security force including Plant Protection, Law Enforcement, and Special Response Team (SRT) officers to execute security plans and procedures.

(2) Personnel to survey and audit the KSC security posture, and conduct long-range security planning.

(3) Personnel to manage the technical aspect of traffic and law enforcement on KSC, provide K-9 support, and conduct investigations.

(4) Personnel to conduct administrative tasks, administer traffic and reserve parking programs, develop short-to-mid range plans, develop special operational procedures, conduct training, and generally support the uniformed security operations.

13.2 MANAGEMENT OF PROTECTIVE FORCES

a. Plans and Orders.

(1) Development. The protective force management shall develop plans, orders, and procedures. Plans and orders, in conjunction with supporting directives, instructions, manuals, and procedures, shall provide direction to protective force personnel in the conduct of their duties. Written requirements shall be prepared to cover routine operations, foreseeable contingencies, and emergency situations. Plans requiring participation by other agencies or KSC elements shall be documented and coordinated. Where possible, a memorandum of understanding or other signed agreements shall be obtained.

RELEASED - Printed documents may be obsolete; validate prior to use.

The elements of security, safety and operational expediency shall be addressed in all plans.

(2) Preparation. Written direction to protective force elements shall be based on contractual obligation, CMR direction, NASA requirements, site-specific needs, threat assessments, plans, or procedures. A procedure for review and revision of all plans, orders, Standard Operating Procedures (SOP's), or other written directives shall be developed and followed.

b. Qualifications.

(1) Personnel performing as security officers must meet medical and job performance standards as directed by NASA. Officers are also required to meet training and firearms proficiency standards as set by NASA. All officers must be eligible for, and be granted, a Secret clearance. Officers shall be evaluated for compliance with NASA standards prior to job assignment, and for job performance during the first 90 days of employment. Records of all training, medical standards, job performance standards, and job performance evaluations shall be maintained.

(2) Personnel performing as law enforcement officers shall meet standards specified for security officers and other standards as required by NASA or the contractor. In addition, these officers shall meet the requirements specified by the State of Florida for law enforcement officers and shall meet any standards set by the Brevard County Sheriff's Office (BCSO). In order to qualify as a law enforcement officer personnel must be deputized by the BCSO.

(3) Personnel performing as SRT officers shall meet basic requirements for training and security clearance. In addition, they shall meet enhanced standards specified by NASA. This shall include more stringent health and job performance standards, increased training requirements, and specialized weapons qualifications.

(4) Personnel performing as security supervisors shall meet the basic requirements for security officers and those increased standards for each listed category as appropriate. Assignment to supervisory status is contingent on qualifications agreed upon between the contractor and the CMR.

RELEASED - Printed documents may be obsolete; validate prior to use.

(5) Authority to Carry Firearms.

(a) The National Aeronautics and Space Act of 1958 (4 USC 456) empowers NASA to authorize the arming of contractor security personnel. All NASA and J-BOSC security personnel so authorized shall have met standards for training and performance as prescribed by the Center Chief of Security to include certification in the NASA Federal Law Enforcement Program. Each officer upon receiving the authority to carry firearms, and while doing so during the performance of duties, shall carry a Certificate of Authority to Carry (Unconcealed or Concealed) Firearms. This certificate shall state the individual's name, nature and location of duties, date of issue, date of expiration, and the signature of the Center Chief of Security/Chief, Protective Services & Safeguards Office.

(b) Appropriate NASA forms shall be prepared for personnel authorized to carry firearms. Copies of these forms shall be retained by the certifying official and issued to the authorized bearer.

c. Allocation of Personnel Resources.

(1) Location, Manning, and Scheduling. The location and manning of fixed and mobile posts shall be determined by the Protective Services & Safeguards Office after it considers the approved threat level, characteristics of the assets to be protected, terrain, and environment. Work schedules for protective force personnel shall be developed by the contractor based on contract obligations and current conditions to provide the maximum efficiency in the use of human resources for the protection of KSC assets.

(2) Law Enforcement Officers. A contingent of qualified and certified law-enforcement officers shall be provided as required by contract in order to enforce the laws of the State of Florida and to investigate traffic accidents, as well as to support the security mission.

(3) Special Response Team. A contingent of SRT officers shall be provided as required by contract in order to provide response and neutralization capabilities.

RELEASED - Printed documents may be obsolete; validate prior to use.

(4) Supervision. Supervision of protective personnel shall be provided, as required, to ensure proper and adequate performance of duties.

(5) Manpower Baseline. A Manpower Baseline shall be provided to the Lead, NASA, on a semi-annual basis. This document shall detail available staffing and the disposition of forces. J-BOSC protective forces headcount shall be determined by current budget limitations.

13.3 PROTECTIVE FORCES DUTIES

a. Officers. Patrol officers shall perform duties, as required by KSC and the security contractor. These shall include, but are not limited to, the following:

(1) Access Control. Officers shall control access to the facility and designated areas throughout KSC according to criteria established by NASA.

(2) Mobile Patrol. Officers shall patrol designated areas of KSC in order to observe activity and to respond to emergencies.

(3) Emergency Response. All officers, but particularly law enforcement and SRT officers, shall respond to emergencies as required to effectively neutralize any threats or hazards, or to make appropriate reports.

(4) Post and Patrol Operations.

(a) Officers shall be trained and qualified to operate all vehicles, equipment, and weapons issued for normal job assignments.

(b) Officers shall be trained to recognize suspicious actions and contrary to regulations or to law applicable to KSC.

(c) Officers shall be trained in all access criteria applicable to KSC.

b. Special Response Forces.

(1) Law Enforcement officers shall perform duties comparable to municipal law enforcement officers. They shall enforce all State

RELEASED - Printed documents may be obsolete; validate prior to use.

Statutes on KSC, investigate accidents, and perform general crime prevention/security patrols.

(2) Special Response Team (SRT) officers shall provide a ready response force capable of countering organized and trained adversaries. These officers shall be trained and armed as directed by NASA.

c. Supervisory Responsibilities. Supervisors and Managers shall:

(1) Meet all training and performance qualifications specified for officers in each appropriate category.

(2) Be familiar with duties and responsibilities for all security posts.

(3) Be familiar with all facilities, operations, and procedures associated with their duties.

(4) Ensure that all security posts/personnel are performing assigned functions efficiently. This requires that each post be visited at least once during each shift.

(5) Ensure that all logs, reports, or other required documents are maintained, completed, distributed, or complied with.

(6) Obtain additional training and skills for management personnel, as determined by the contractor.

13.4 PROTECTIVE FORCES TRAINING

a. Purpose. The overall objective of the formal training program for the protective force is to develop and maintain, in an effective and efficient manner, the competencies essential by protective force personnel to perform the tasks required, in order to fulfill the security mission on KSC. The formal training program includes all organized, documented training activities which are the responsibility of the protective forces training element. This includes training activities conducted for pre-service employees, NASA Federal Law Enforcement Training, on-the-job training on each shift, and during annual recertification.

b. Program Requirements. The training program shall:

(1) Be based on valid and complete analysis of job tasks.

RELEASED - Printed documents may be obsolete; validate prior to use.

(2) Be clearly organized, with measurable criteria for objectives to be evaluated during training.

(3) Accommodate the various levels of skills for each category of officer (i.e., pre-employment vs. Special Response Team) so that the maximum efficiency in training takes place.

(4) Achieve a well defined, minimum level of competency to perform each required task.

(5) Employ standardized lesson plans with clear performance objectives as a basis for instruction.

(6) Be supported by adequate resources, including qualified instructors, adequate time, facilities and funding.

(7) Be planned, organized, and directed to make optimum use of available resources.

(8) Be documented so that individual and overall training status is easily accessible.

c. Officers.

(1) Basic Training. Prior to initial assignment to duty, officers shall successfully complete a basic training course, to include NASA Federal Law Enforcement certification. The basic training course shall be approved by the Chief, Protective Services & Safeguards Office. This course shall equip officers with the necessary knowledge and skills to maintain minimum performance requirements on the job.

(2) Annual Training. Officers shall receive annual refresher training as approved by the Chief, Protective Services & Safeguards Office. This training shall serve to recertify officers in required knowledge and skills or to impart new training as required.

d. Special Response Team. SRT and law enforcement officers shall receive additional training as required by the Chief, Protective Services & Safeguards Office.

e. Supervisors. All protective force supervisors shall successfully complete basic and annual training for assigned categories as required for officers.

RELEASED - Printed documents may be obsolete; validate prior to use.

f. Additional Training. Some officers and management personnel shall be required to participate in specialized training; i.e., intoxilyzer, radar, gunsmith, physical security, canine handling, etc.

g. Refresher Training. All officers, who carry weapons, shall complete NASA Federal Law Enforcement refresher training, once every two years.

13.5 PROTECTIVE FORCES EQUIPMENT

Protective force equipment shall enhance the ability of the protective force to effectively, efficiently, and safely perform routine duties and to prevent adversaries from accomplishing their objectives.

a. Individual and Special Equipment.

(1) Uniforms. Protective force personnel shall be distinctively uniformed while on duty and identified with their function by appropriate variances in uniform. The uniform shall be such as to enhance the efficient performance of routine and emergency duties, and shall promote the image of professionalism.

(2) Duty Equipment. Certain items are to be assigned to each officer (either permanently or from on-shift supplies). These include the appropriate weapons, holster, ammunition, and radio. Additional equipment shall be issued as required for specific assignments and current conditions.

(a) Primary Weapon. The 9-mm Glock semiautomatic pistol.

(b) Secondary Weapon. A 9-mm submachine gun, 1-gauge shotgun, or a HK-33 rifle is available and shall be issued concurrent with the type of duty and level of protection to be afforded.

(c) Weapons Storage and Handling. Procedures shall be developed to facilitate storage and accountability of weapons when maintained at Security Headquarters, Building K6-496, and when assigned to officers.

(d) Ammunition, Pyrotechnics, and Explosives. The protective force shall maintain sufficient ammunition, pyrotechnics, and explosives to accomplish the identified mission.

RELEASED - Printed documents may be obsolete; validate prior to use.

(3) Special Equipment. The protective force shall maintain such specialized equipment as required to accomplish the security mission. This includes mobile command post, boats, explosives and nuclear material detectors, specialized radios, night observation devices, off road vehicles, and other equipment items.

(4) Equipment Inventory and Accountability. The protective force shall establish NASA and J-BOSC approved procedures for maintaining inventory and accountability of all equipment.

b. Protective Force Vehicles.

(1) Vehicle Type. Protective force vehicles shall exhibit a degree of reliability commensurate with their intended function. These vehicles shall enhance the efficiency, speed, and safety of routine and emergency duties under all weather conditions. The vehicles are to be of a type and size suitable for the intended use.

(2) Vehicle Maintenance. Procedures shall be developed to ensure that vehicles are maintained in a serviceable condition. Records of all maintenance shall be maintained by GSA.

c. Communications Equipment.

Protective force communications equipment shall provide multichannel capability with clear transmissions. Encoded transmission capabilities shall be available when required. Communications equipment shall be readily available in sufficient numbers to equip protective forces.

CHAPTER 14. INCIDENT MANAGEMENT SYSTEM

14.1 GENERAL

This chapter provides management direction for all actual or suspected or probable crisis incidents that may occur requiring emergency planning, control, and resolution. Incident Management System (IMS) events for Security may result from either natural disaster, industrial accidents, and criminal or malicious intent.

14.2 RESPONSIBILITIES

a. The Chief, Protective Services & Safeguards Office, is responsible for:

RELEASED - Printed documents may be obsolete; validate prior to use.

(1) Managing command, control, and communications as the Incident Commander (IC) at the scene of an incident occurring on KSC.

(2) Establishing requirements for planning, development, and coordination of detailed procedures by KSC organizational elements and their associated contractors.

(3) Providing requirements for establishing Incident Management Teams (IMT) for Security to ensure effective emergency operational performance and return of all elements to normal status.

(4) Providing coordination of collateral support to other KSC elements or Government agencies.

b. Heads of management support and heads of primary organizations are responsible for: Immediately, upon the request of the Chief, Protective Services & Safeguards Office, or Lead, NASA Security Operations, providing personnel under their control to assist in efforts concerning:

(1) Protection of life and property.

(2) Maintaining continuity of operations.

(3) Evidence/data impoundment and/or control.

(4) Damage assessment and repair.

(5) Resumption of normal activities following emergency or crisis situations.

c. The Lead, NASA Security Operations, is responsible for:

(1) Establishing requirements for reporting, investigating, and resolving all incidents involving criminal or malicious intent covered within the scope of this chapter.

(2) Supporting collateral investigations by other Government agencies.

RELEASED - Printed documents may be obsolete; validate prior to use.

(3) Ensuring that detailed plans and procedures are in effect identifying security measures applicable for various emergency or crisis incidents.

14.3 SECURITY INCIDENT MANAGEMENT TEAM

a. The initial management response to any emergency or crisis situation is to establish a Security Incident Management Team (SIMT). Due to the diverse incidents which may present a crisis situation, various KSC organizations may be represented in comprising the IMT. Representatives from The Protective Services & Safeguards Office shall be part of the primary team structure because of their interrelationship in controlling emergency situations. Other Incident Management Team members may include, but not be limited to: Fire personnel, Safety personnel, KSC Senior Management, Public Affairs Office personnel, and personnel from other Government agencies.

b. The Chief, Protective Services & Safeguards Office, or designee shall identify initial IMT representation for Security and coordinate its activation.

c. Personnel comprising the IMT for Security must remain knowledgeable and current on plans, procedures, and capabilities of their respective organizations.

d. The objective of Security's IMT is to ensure effective response, resolution, and return of all elements to normal status. Of primary concern shall be the protection of life and property.

14.4 PREPARATION AND PLANNING

The incident management topics described in the subsequent paragraphs of this chapter require general and detailed preparation/planning for responding to an incident at KSC or to sites under KSC jurisdiction. Preparation shall include identifying requirements for equipment and training necessary to ensure proficient performance in handling these situations. Planning must specify Incident Command responsibility pertaining to initial response and handling of any specific crisis situation.

14.5 NATURAL DISASTERS.

JHB 2000, "Consolidated Comprehensive Emergency Management Plan", and KNPR 8715.3, "KSC Safety Practices Procedural Requirements" both provide precautionary measures which shall be performed in advance of a potential disaster, either a natural disaster, or as a result of a safety accident;

RELEASED - Printed documents may be obsolete; validate prior to use.

i.e., hurricane, adverse weather, tornadoes, safety accidents, toxic vapors/hypergolic and cryogenic spills, emergency medical operations, fire, nuclear accident/radiological incident, inadvertent space vehicle/aircraft accidents, utility contingencies, etc.

14.6 BOMBS AND BOMB THREATS

a. Definitions:

(1) Bomb: A device capable of producing damage to material and injury or death to personnel when detonated or ignited. Bombs are classified as explosive or incendiary. An explosive bomb causes damage by fragmentation, heat, and blast wave. The heat produced often causes a secondary incendiary effect. An incendiary bomb generates fire-producing heat without substantial explosion when ignited. Bombing occurs when an explosive bomb detonates or an incendiary bomb ignites.

(2) Bomb Threat: A message, delivered by any means that may or may not specify the location of a bomb, time of detonation, ultimatum related to the detonation, or concealment of the bomb.

(3) Bomb Incident: Any event concerning the execution of a bomb threat, discovery of a bomb device, or detonation of a bomb on KSC.

b. Policy: The primary mission shall be protection of life, flight hardware, and government property. Actions to be taken shall be based on an evaluation of all available information and circumstances present in each situation.

c. Procedure: Bomb threats are usually received by either mail or telephone. It is important that the person receiving the threat knows what to do in each case.

(1) Threats by Mail:

(a) Carefully preserve the letter, in plastic container if possible, handling it as little as possible until released to a security representative.

(b) Note time and manner in which letter was received.

RELEASED - Printed documents may be obsolete; validate prior to use.

(c) Report all incidents to the Joint Communications Control Center (JCCC), by calling 911, or 867-11, immediately.

(2) Threats by Telephone: Most threats are received by telephone. Unlike a letter, a phone call leaves no physical evidence on which to base a plan of action. For this reason, security authorities must rely heavily on the information conveyed by the person taking the call. The form on the last page of the KSC Telephone Directory should be used as requirements to record important information for investigating authorities. Upon receiving a bomb threat by phone:

(a) Make a note of the exact time of the call.

(b) Try to remember the exact message, word for word (take notes).

(c) Obtain as much information from the caller as possible by listening to background noises, noting sex, age, accent, etc.

(d) Report incident to the JCCC, 911/867-11, immediately.

(3) Suspect Objects/Packages: If an object is visually detected and suspected of being an explosive device:

(a) Do not touch or move object.

(b) Do not operate radio transmitters or cellular telephones in the vicinity (minimum of 150 feet) of the device. They could detonate it.

(c) Report incident to JCCC, 911/7-11 immediately.

(d) Stand by at a distance of at least 300 feet to warn approaching personnel until security personnel arrive.

(4) Execution:

(a) The IMT, initially comprised of representatives from The Protective Services & Safeguards Office and J-BOSC Security, shall analyze the information received to determine the seriousness of the threat and the appropriate response.

RELEASED - Printed documents may be obsolete; validate prior to use.

(b) The Incident Commander shall decide if it is necessary to search or evacuate the area. Instructions for personnel shall be coordinated with the affected site manager.

14.7 HOSTAGE/TERRORIST INCIDENTS

a. Definition: Terrorism is the unlawful use of force against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

b. Policy: Presidential Decision Directive 39 (PDD-39), "United States Policy on Counterterrorism" directs a number of measures to reduce the Nation's vulnerability to terrorism, to deter and respond to terrorists' acts, and to strengthen capabilities to prevent and manage the consequences of terrorist use of Nuclear, Biological, and Chemical (NBC) weapons including Weapons of Mass Destruction (WMD). PDD-39 discusses Crisis Management and Consequences Management.

(1) Crisis Management: Includes measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. The laws of the United States of America assign primary authority to the Federal Government to prevent and respond to acts of terrorism; State and local governments provide support and assistance as required. Crisis Management is predominantly a Law Enforcement response.

(2) Consequence Management: Includes measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses and individuals affected by the consequences of terrorism. The laws of the United States assign primary authority to the States to respond to the consequences of terrorism; the Federal Government provides assistance as required. The Federal Emergency Management Agency (FEMA) retains responsibility for consequence management throughout the Federal response, and acts in support of the FBI, as appropriate, until the Attorney General, in consultation with the FBI Director and the FEMA Director, determine that such support is no longer required.

c. Lead Agency Responsibilities:

RELEASED - Printed documents may be obsolete; validate prior to use.

KSC Security is capable of responding to a hostage/terrorist incident, however, PDD-39 validates and reaffirms existing Federal Lead Agency responsibilities for counterterrorism, which are assigned to the Department of Justice, as delegated to the FBI, for threats or acts of terrorism within the United States. For this reason, the FBI shall be notified immediately when KSC is confronted with a hostage/terrorist situation. As stated in the Federal Response Plan, it is FBI policy that Crisis Management shall involve only those Federal agencies requested by the FBI to provide expert requirements and/or assistance, as described in the PDD-39 Domestic Guidelines (Classified) and FBI Incident Contingency Plans (Classified).

When the FBI is summoned, the KSC Incident Commander should be prepared to brief the arriving team leader on the following items:

(1) Actions already taken

(2) Logistics of the situation

(3) Human resources available, deployed

(4) Special tools, equipment available

(5) Staging areas

(6) Supplies

The KSC Incident Commander must understand that the FBI has it's own plans to implement. The FBI may use a Classified version of operational plans to run the operation, and many aspects may not be immediately shared. Time constraints may prevent the FBI from releasing information. In some instances, the FBI may already be aware of the threat and could cut the KSC Incident Commander's in-brief short.

The KSC Incident Commander should be ready to adjust the action plan, if necessary. Roles and responsibilities may be altered. The key to a successful operation is to disturb as little as possible, provide the logistical support needed, and remember the common goal.

d. Unified Command System (UCS):

In all probability, a UCS shall be established. The UCS establishes goals and objectives, develops a single action plan, allows shared resources, and establishes specific responsibilities for the emergency

RELEASED - Printed documents may be obsolete; validate prior to use.

response. The primary features of the UCS are:

(1) Single integrated incident organization

(2) Co-allocated facilities

(3) Shared planning, logistical, and finance/administration

(4) Coordinated process for resources acquisition

e. Shared Resources: Responders that may support the situation and should be a part of any training and exercises on terrorism are:

(1) Fire Services; HazMat; Emergency Medical Personnel

(2) Public Works; Electrical, Gas, Water

(3) Law Enforcement

(4) Media and Public Affairs

(5) Local Community Emergency Management

Further information concerning response to terrorist activities is contained in the Federal Response Plan, Terrorism Incident Annex, T-1.

JHB 2000, Annex O - Security Operations, develops general and specific requirements pertaining to planning for, and responding to, incidents of a terrorist/sabotage nature that may threaten life or property; compromise classified operations/information or threaten the National Space Program; or result in adverse publicity for NASA or KSC. These documents ensure that specific procedural requirements are provided identifying authority (as listed above and outlined below) to handle response, containment, and neutralization of any potential threat.

f. Hostage/Barricaded Subjects.

(1) Definition: A hostage is a person held against his/her shall as security for fulfillment of certain terms or demands.

(2) Policy: This chapter specifies measures for: (1) responding to a hostage/barricaded-subject situation where the threat against

RELEASED - Printed documents may be obsolete; validate prior to use.

human life or the loss of Government property has been expressed, (2) actions for the safety and protection of persons who may be held hostage or be threatened with bodily harm, or (3) barricaded subjects. A hostage or barricaded-subject situation shall be considered any time a person is held against his/her shall by threat of violence, either to that person or others; or those situations where persons barricade or otherwise secure an area and refuse to leave or comply with directions given by security authorities. If the barricading subject threatens violence, the threat must be considered real. The goal is to neutralize the situation with the minimum amount of force necessary and without injury to suspects or innocent bystanders.

(3) Procedure:

(a) Reporting: If a hostage/barricaded-subject situation should occur, the person reporting the incident should notify JCCC immediately by calling 911 or 867-11, giving as much detail as possible about the situation, including reporting the person's name, location, and phone number. Maintain telephone contact, if feasible, providing information as requested until security personnel arrive on the scene.

(b) Execution: Upon notification of a hostage or barricade situation, J-BOSC Security shall notify the crisis negotiators. The Senior Security Supervisor shall immediately respond to the area as the Incident Commander and:

1. Maintain a low profile, taking no overt or covert actions that may indicate an attempt to take control of the incident.

2. Establish an inner perimeter to isolate the area, an outer perimeter to maintain control, and a command post.

3. Evacuate nonessential personnel from the area.

4. Gather intelligence; such as, who is being held hostage, who is the suspect, what is the objective of the suspect, etc., taking extensive notes to brief the crisis negotiator upon arrival.

RELEASED - Printed documents may be obsolete; validate prior to use.

5. Keep conversation with suspect to a minimum, but when conversation is necessary, speak in a calm, slow voice, making no threats or promises. Keep in mind that time is the greatest tool of the negotiator, and any attempts to end the incident rapidly may cause the deterioration of the negotiation process.

g. Sabotage.

(1) Definition: Acts or processes tending to hamper or hinder operations by unauthorized destruction of property or obstruction of operation and maintenance activities.

(2) Policy: KSC is vulnerable to acts of sabotage which may be committed at any time and without warning. Circumstances surrounding each threat/incident, including location, time, and previous countermeasures taken, shall dictate action to be taken. Heightened security measures shall be taken prior to all launches at launch-critical facilities/areas. J-BOSC Security shall respond to all acts of sabotage. Fire, medical, safety, and other KSC elements shall respond, as required.

(3) Procedure:

(a) Reporting: The reporting person shall respond depending on how the information was received:

1. By Observation: Should a person observe an act that is suspected of being sabotage, immediately notify JCCC, 911/867-11.

2. By Telephone: Security authorities must rely heavily on the information conveyed by the person taking the call. The form on the last page of the KSC Telephone Directory should be used as a guideline to record important information for the investigating authorities. Upon receiving information/threat by phone:

a. Make a note of the exact time of call.

RELEASED - Printed documents may be obsolete; validate prior to use.

b. Try and remember exact message, word for word (take notes).

c. Obtain as much information from caller as possible by listening to background noises, noting sex, age, accent, etc.

d. Report incident to JCCC, 911/867-11, immediately.

3. By Mail:

a. Carefully preserve letter, in plastic container if possible, handling as little as possible until released to a security representative.

b. Note time and manner in which letter was received.

c. Report incident to JCCC, 911/867-11, immediately.

d. Execution: The Security Incident Commander shall coordinate all activities relative to evacuation, personnel control, and other regulatory and restrictive measures necessary to provide maximum protection to personnel and property, initiate investigations, and advise and coordinate with other elements involved in the incident.

14.8 CRIMINAL ACTS

JHB 2000, "KSC Comprehensive Emergency Preparedness Plan," develops general and specific requirements which pertains to, planning for and responding to incidents of a criminal nature that may threaten life or property, compromise classified operations/information or threaten the National Space Program, or result in adverse publicity for NASA or KSC. JHB 2000, ensures that specific procedural requirements are provided identifying authority pertaining to response, containment, and neutralization of any potential threat.

a. Civil Disturbance.

RELEASED - Printed documents may be obsolete; validate prior to use.

(1) Definition: The act of disturbing normal activities by civilian personnel.

(2) Policy: It is NASA and KSC policy to comply to the fullest extent practical with the applicable requirements regarding Civil Disturbances.

(a) Disturbances in and around KSC controlled areas are prohibited. Participants should be advised that all persons entering controlled areas must be authorized/badged to enter or be subject to eviction or possible arrest.

(b) All positive actions taken under this plan shall be accomplished in the least provocative manner. Procedures most likely to elicit the cooperation of the demonstrators should be used where possible. KSC personnel, while acting in an official capacity to bring the disturbance under control, are not expected to endure abusive language or threats to their person or government property.

(c) Information on civil disturbances shall be released to the news media and KSC personnel by the NASA Workforce & Diversity Management Office only.

(3) Procedure for Outside Controlled Areas of KSC Property: Upon notification of a demonstration or anticipated civil disturbance:

(a) J-BOSC Security shall:

1. Respond to the scene to ensure impact on ingressing/egressing traffic poses no threat to controlled area. Maintain a surveillance of the demonstration and immediately report any escalation.

2. Perform notification as shown in JHB 2000, Annex L, Emergency Support to Local Government.

3. Notify The Protective Services & Safeguards Office immediately, who shall determine need for further reporting of the situation.

RELEASED - Printed documents may be obsolete; validate prior to use.

4. Standby to form an Incident Response Team with sufficient vehicles to ensure mobility for instant positive response.

5. Open an incident response log, entering significant events and actions. At a minimum, hourly entries shall be made.

6. Submit an After-Action Report to The Protective Services & Safeguards Office within 30 days of the termination of the disturbance.

(b) The Protective Services & Safeguards Office shall:

1. Notify NASA Senior Management and assure notification of Center Operational activities (Shuttle, Payload, Center Support).

2. If it appears that the KSC controlled area may be threatened, direct the formation of a J-BOSC Incident Response Team. This group shall stage at J-BOSC Security Headquarters with sufficient vehicles to ensure mobility for instant positive response.

3. Submit an After-Action Report to the Center Director through the Director of Spaceport Services.

(c) The KSC Installation Security Office (CCS), or Designated Representative, shall:

1. If the KSC controlled area is threatened or civil authorities have not arrived in sufficient number to control the situation outside the controlled area; the ISO shall take charge of the situation; may direct the dispatch of the Incident Response Team.

2. Should participants enter the controlled area and refuse to leave, their eviction or arrest may be requested of civil authorities. If civil authorities are not present in sufficient numbers, the J-BOSC Security Incident Response Team may be directed

RELEASED - Printed documents may be obsolete; validate prior to use.

to employ required force to ensure the integrity of the controlled area.

(d) KSC photographers shall photograph the proceedings, in particular, evictions or arrests by J-BOSC Security.

(4) Procedure for Disturbances Within KSC Controlled Areas:

(a) J-BOSC Security shall:

1. Respond to the scene to evaluate the situation and control the disturbance.

2. Perform notification as shown in JHB 2000, Annex L, Emergency Support to Local Government.

3. Notify The Protective Services & Safeguards Office immediately, who shall determine the need for further reporting of the situation.

4. Standby to form an Incident Response Team with sufficient vehicles to ensure mobility for instant positive response.

5. Open an incident response log, entering significant events and actions. At a minimum, hourly entries shall be made.

6. If the crowd is non-violent/not unruly: may provide for the ISO or Director or representative to talk to the participants to resolve the matter through discussion. If the decision is to disperse the group, unauthorized/unbadged persons shall be advised they are subject to eviction and possible arrest. They shall be allowed to leave the controlled area in a peaceful manner or be arrested, if they refuse to leave. Properly badged employees shall be advised of possible disciplinary action, if they fail to disperse.

7. If the crowd is unruly, threatening, or disruptive; may provide for the ISO or representative to advise the participants they are subject to eviction and possible arrest, determine course of action,

RELEASED - Printed documents may be obsolete; validate prior to use.

and advise participants. If necessary, the Incident Response Team shall evict or arrest participants.

8. Submit an After-Action Report to The Protective Services & Safeguards Office within 30 days of the termination of the disturbance.

(b) The Protective Services & Safeguards Office shall:

1. Notify NASA Senior Management and assure notification of Center Operational activities (Shuttle, Payload, Center Support).

2. If it appears that the KSC controlled area may be threatened, direct the formation of a J-BOSC Security Incident Response Team. This group shall stage at J-BOSC Security Headquarters Building K6-496, with sufficient vehicles to ensure mobility for instant positive response.

3. Submit an After-Action Report to the Center Director through the Director of Spaceport Services.

(c) The ISO, or designated representative, shall take charge of the situation; determine course of action; and advise participants.

(d) KSC photographers shall photograph the proceedings, in particular, evictions or arrests affected by J-BOSC Security.

b. Related Statutes and Directives:

(1) Federal Personnel Manual 751-4, Enforced Leave.

(2) Florida Statutes, Chapter 810, Burglary and Trespass.

(3) Florida Statutes, Section 81.18, Trespasses.

(4) Florida Statutes, Section 861.01, Obstructing Highways.

(5) Florida Statutes, Section 877.03, Breach of Peace, Disorderly Conduct.

RELEASED - Printed documents may be obsolete; validate prior to use.

CHAPTER 15. BADGES AND PASSES

15.1 GENERAL

This chapter establishes the procedures and details responsibilities for issuing and controlling identification badges, Temporary Passes, and special badges used at KSC.

15. RESPONSIBILITIES

a. The Director, External Relations and Business Development, is responsible for providing transportation, tours, and other NASA visitor's services, as required, in support of visits to KSC by persons invited by the Center Director or Deputy Director, or persons referred by NASA Headquarters.

b. The Deputy Director, KSC, is responsible for managing the approval, control, and conduct of tours of Space Shuttle operational areas by visitors, guests, dignitaries using the Center Director's guest credential (Gold Badge).

c. The Installation Security Officer (ISO) is responsible for the issuing of badges and passes, to include those for contractors and other official visitors. To respond to real-time security requirements, unforeseen events, and operational changes, the ISO may change or enhance, as required, the procedures and responsibilities for the issuance and control of identification badges, temporary passes, and special badges.

d. Persons requesting badges or passes are responsible for conduct individuals they sponsor while they are on KSC or CCAFS.

15.3 ACCESS TO KSC/CAPE CANAVERAL AIR FORCE STATION (CCAFS)

a. Entry to KSC property or into controlled areas on KSC or CCAFS is a privilege that can be denied, suspended, or revoked.

b. Access to KSC shall be allowed only when it furthers the conduct of NASA business (hereafter referred to as "official business"). This applies to employees of NASA, its contractors, and tenants on KSC, as well as others with business to conduct at KSC. Approved guests, visitors, and participants in tours are included in the category of "official business."

RELEASED - Printed documents may be obsolete; validate prior to use.

c. Access to KSC is normally controlled through use of KSC or CCAFS issued identification badges or passes. Other special badges may be issued for launches, tours, or other special occasions.

d. Access to security areas (limited or controlled) on KSC or CCAFS is granted by the system or facility Office of Primary Responsibility (OPR) and is controlled by use of an Area Permit system, in addition to appropriate NASA, KSC, or CCAFS issued identification badges. When special operational safety or other conditions are in effect, special badges, access lists, or other devices authorized by the ISO may be used to grant access. NASA employees not duty-stationed at KSC may use their NASA identification badges for access to KSC/CCAFS. Access to security areas may be granted based on clearance information in the "Installation Cleared Personnel Roster" maintained at the Visitor Records Center (VRC).

e. The VRC shall verbally verify a visitor's level of security clearance to NASA personnel or KSC organizational security representatives, if the visitor's clearance is on record and if the individual is making an official/classified visit.

f. Appropriately badged and qualified individuals shall act as escorts, when required.

g. Individuals requesting access to KSC or NASA controlled areas on CCAFS must provide positive identification at any badging station or Gate. Primary acceptable forms of identification include a driver's license; state-issued identification card; U.S. Passport, passport; DoD, Federal, state, and local ID Card; U.S. Coast Guard Merchant Marine ID Card, Resident Alien ID Card; or Foreign National Passport. Identification must be presented before the individual shall be issued a badge or pass. Secondary acceptable forms of identification are: U.S. Birth Certificate; Certificate of U.S Citizenship; Certificate of Naturalization; Unexpired Temporary Resident Card; Voter Registration Card; Native American Tribal Document; U.S. Social Security Card; Certificate of Birth Abroad issued by the Department of State.

h. Unless specifically approved by the ISO, no individual shall possess more than one NASA or KSC ID. This provision does not limit the possession of required Area Permits or special access badges.

RELEASED - Printed documents may be obsolete; validate prior to use.

15.4 BADGE RECEIPTING

a. The computer-generated KSC Identification Badge and the KSC\CCAFS Temporary Badge is receipted for during its preparation. The Personnel Access Security System (PASS) signature pad, when signed and the signature image is transferred to the computer-generated badge, constitutes receipt.

b. The individual, by acceptance of the badge, agrees to abide by the regulations of KSC and CCAFS, and to subject themselves and any property in their possession or control, to any search or detention necessary for the protection of information and property.

15.5 DISPLAY AND CONTROL OF THE BADGE

a. Each individual authorized access to KSC/CCAFS shall adhere to the following rules concerning wearing and use of badges and passes:

(1) On KSC/CCAFS, the badge/pass shall be worn above the waist, plainly visible, face side out, unless operational considerations/requirements dictate the badge be removed because of special clothing requirements (clean room garments, SCAPE suits, etc.), placed on a badge board, or worn below the waist for safety reasons. Badges may be inserted into clear plastic holders. The KSC Safety, Health & Independent Assessment Directorate must approve necklace material for use.

(2) Individuals shall comply with any request by security personnel, management, or authorized auditors to surrender the badge/pass for physical inspection.

(3) Items such as tape, pins, clips, etc., shall not be fastened to the badge/pass in any manner so as to obstruct, alter, or in any way change the appearance of the badge.

(4) While it is permissible for companies to issue company badges, the primary badge used on KSC is the KSC issued identification badge. As mentioned above, while on KSC/CCAFS, the KSC badge shall be worn above the waist, plainly visible and not behind the company badge.

RELEASED - Printed documents may be obsolete; validate prior to use.

b. Badges shall be safeguarded when not being utilized. Vehicles are not recognized nor authorized as a proper location for storage of the badge.

c. Badges that are faded, separated, or in otherwise poor condition shall be replaced.

d. Badges shall be replaced when physical appearance is changed; i.e., beard growth or removal, plastic surgery, etc.

e. Use/Misuse

(1) The use of any KSC badge for other than KSC/CCAFS use is strictly prohibited. See paragraph 404.8, Violations.

(2) The photocopying or photographing (duplication) of badges is not permitted. Badges are not authorized for use in the transaction of personal business. Merchants and financial institutions may not make copies of KSC badges.

15.6 LOST BADGE/AREA PERMIT REPORTING

a. NASA employees who have lost their picture badges, Area Permits, PACAS cards, or any special badges or permits must submit within working days a "Lost Badge Statement" to the VRC explaining the circumstances (when and where lost, and what attempts were made to find it). The statement must also indicate that if the badge is found, it shall be turned in to the VRC, with a new KSC Form 0-168.

b. Contractor employees who have lost their picture badges, Area Permits, PACAS cards, or any special badges or permits must submit the above-mentioned "Lost Badge Statement" to their organization's badging official who shall endorse and forward the statement to the VRC. Contractor Badging Officials shall complete a new KSC Form 16, for re-issue of the picture badge. Lost badge statements are available at the VRC, PIDS I, PIDS III, and F Gate.

c. Employees who have lost their picture badges shall be issued temporary passes valid for a 7-day period to allow the employee time to conduct a thorough search for the badge. At the end of that time, if the badge has not been located, a new badge shall be issued.

d. Report of a lost Temporary Pass may be submitted on KSC O/T Form 439, Lost/Stolen Temporary Pass. This form is only available at Pass and Identification Station (PIDS) 1, 3, F-Gate, and the VRC.

RELEASED - Printed documents may be obsolete; validate prior to use.

15.7 TERMINATION, LEAVE OF ABSENCE, VACATION, AND FOREIGN TRAVEL

a. When authorization to possess a picture badge no longer exists (i.e., upon termination of employment, end of visit, leave of absence, or expiration of contract), the badge shall be surrendered to the respective KSC or contractor security office. An Exit Pass, KSC Form 0-133, shall be issued to the individual for departure from the installation, if necessary.

Note: Disciplinary or administrative leave policy: As directed, badges shall be turned in and held until expiration of the action. Vacation: KSC badges shall not be taken on vacation. Foreign travel: Unless specifically authorized by the ISO, no badge or pass shall be taken into a foreign country. Medical: An absence over 90 days requires that picture badges be turned in.

b. Contractor employees who are not permanently stationed at KSC or CCAFS, and have been issued picture badges containing an expiration date, are required to turn their badges in to their security office or representative when departing the area for a significant period of time (e.g., return to permanent home in another county or State). The badges shall be held for those individuals until their subsequent return to KSC, or until expiration.

15.8 VIOLATIONS

Any individual having the knowledge or suspicion that badging regulations are or have been violated is required to report those violations to his/her security office.

Note: Unauthorized use of a Government badge/pass, (including but not limited to the transfer, sale, gift, loan, use as collateral, or use to gain access to, or remain in an area or on the installation for other than official purposes) or any mutilation, destruction, or forgery (including alteration or duplication) thereof, may subject the person responsible to exclusion from KSC, punishment by law, and/or administrative action by his/her employer.

15.9 PASS REQUESTS MUST BE WRITTEN AND SIGNED

RELEASED - Printed documents may be obsolete; validate prior to use.

All temporary pass requests must be submitted in writing and signed by the authorized requester. The KSC Form -889 is provided for this purpose and is listed in the KSC Electronic Forms Program.

15.10 ADVERSE INFORMATION REPORTING

a. Immediate supervisors of NASA employees and supervisory personnel of other organizations shall report to the appropriate NASA or contractor security office, any adverse or derogatory information concerning their employees as soon as they know that information.

b. Adverse information reporting shall be consistent with KNPR 1610.1B, Chapters 04 and 409.

c. All individual employees at KSC have the responsibility to report adverse information, when it becomes known to them. Individuals who wish to remain anonymous may submit reports directly to NASA Protective Services and Safeguards Office.

15.11 RESIDENT BADGES

a. NASA Civil Service Badge

(1) The NASA Civil Service Badge is uniform throughout the agency and shall be issued to NASA civil servants, NASA non-appropriated fund employees, consultants, and other Federal employees and military personnel detailed to NASA. Badge standards shall be consistent with the NASA Badging System. The individual's security clearance shall not be designated by any device, color, or code on the badge.

(2) The NASA Director of Workforce and Diversity Management shall process necessary forms and coordinate with The Protective Services & Safeguards Office to obtain approval for the issuance of badges. The Director of Workforce and Diversity Management shall designate by letter, up to five (5) people to approve requests for picture badges. Signature cards, KSC Form 0-157, shall be forwarded to the Visitor Records Center for authentication verification purposes.

(a) NASA/KSC Directors may appoint themselves and up to five (5) people to serve as badging officials for their directorate. They may also appoint between five (5) and ten (10) people, to request temporary passes, depending on their mission. Badging officials authorized to request

RELEASED - Printed documents may be obsolete; validate prior to use.

pictures badges are also authorized to request temporary passes.

(b) The Visitor Records Center shall provide directorates with a unique number for authentication of badge/pass requests.

(3) Color codes used to indicate individual status:

White top and bottom	-	Active employee
Silver/gray top and bottom	-	Non-appropriated fund
Orange top and bottom	-	Consultant

(4) KSC Retirees

NASA retirees are issued a KSC Retiree ID Card which shall allow them to be issued a one day pass, during normal working hours, Monday through Friday. Exceptions to this policy may be granted on an individual basis by the Protective Services and Safeguards Office.

b. KSC Resident Contractor Badge

(1) The KSC Resident Contractor Badge shall be issued to NASA/KSC contractor employees, party to a NASA-related contract, whose normal work location is KSC or CCAFS. A Temporary Pass shall be utilized until a Resident ID is issued.

(2) A Resident ID Contractor Badge is blue to the left of the picture and the company's name shall be imprinted in the blue area.

(a) A prime contractor may designate up to five (5) persons as badging officials. Additional persons for each sub-contractor may be designated by their prime contractor by submitting a written request and furnishing the names to the VRC. The subcontractor shall submit their request for badging officials through the prime contractors' security office. New contract must have the badging officials approved by NASA Protective Services and

RELEASED - Printed documents may be obsolete; validate prior to use.

Safeguards Office. KSC Forms 0-157 shall be submitted when adding badging officials. The Visitor Records Center shall provide contractors a number unique to their company, to validate badge/pass requests.

(b) Correspondence showing delegation of badging authority shall include the local company address and phone number, work phone numbers of authorizing personnel, areas of performance, contract number, and expiration date of contract or subcontract. Prime contractors shall be responsible for badges issued under their own authority and those requested by their subcontractors.

(c) Designated badging officials shall submit badge requests to the VRC on KSC Form 0-16. The VRC shall maintain names and identification of designated badging officials on file.

15.12 NONRESIDENT BADGES

a. The Nonresident Badge shall be issued to Government and contractor employees, party to a NASA-related contract, (but not a KSC Contract) whose visits to KSC are for more than 180 consecutive days or are sufficiently repetitive within the visit year.

(1) The Nonresident badge is colored orange on both sides of the picture. The company's name is imprinted in the orange on the left of the picture. The badge expiration date is printed to the right of the picture.

(2) The Nonresident badge expiration date shall not exceed the length of the contract.

(3) Badging officials must ensure that they keep the number of Non-Resident badge requests to an absolute minimum necessary to accomplish the required tasks. A Temporary Pass should be issued in place of the Non-Resident Badges for requests less than one year. Prior approval through the NASA Protective Services and Safeguards Office is required for requests longer than one year.

b. When required, the badge shall be marked with a day, month and year to indicate the expiration date.

RELEASED - Printed documents may be obsolete; validate prior to use.

c. Sponsors of individuals holding Nonresident badges shall be required to submit requests for new badges 30 days prior to expiration. Sponsors shall submit badge requests in writing using KSC Form 0-16, Request for KSC Picture Badge, to the VRC.

d. The Nonresident badge may also be issued for the following categories of visitors to KSC:

(1) Construction

(a) Supervisory employees, party to a NASA-related contract, whose normal work location is KSC or CCAFS. The badge shall be imprinted with the word "CONSTRUCTION" in the orange area to the right of the individual's picture.

(b) Construction company personnel holding non-resident badges may interchange between construction projects at KSC or CCAFS by meeting the operating entities' procedures. However, should all contracts with NASA/KSC or NASA contractors terminate, the KSC badge/pass must be returned even though a contractor may still hold a valid contract with the Air Force. Such employees would then be required to be rebadged with a CCAFS badge.

(2) Support Personnel

(a) Included in this category are those people whose services are required for activities such as installing or servicing machines, to persons such as safety or health inspectors, insurance investigators, vendors (not salespersons), truck drivers, and delivery persons who require frequent access to KSC/CCAFS. The badge shall be imprinted with the word "SUPPORT" in the orange area to the right of the individual's picture.

(b) Badging officials must ensure that the number of badges issued are keep to the absolute minimum necessary to accomplish the required tasks.

RELEASED - Printed documents may be obsolete; validate prior to use.

(3) Groves

Fruit grove lessees and their permanent personnel may be issued badges. Grove badges are only good to and from grove areas. U.S. Fish and Wildlife badging officials must request badges for grove personnel by submission of KSC Form 0-16. The badge shall be imprinted with the word, "GROVES" in the orange area to the right of the individual's picture.

(4) News Media Members

(a) Media personnel, who are authorized to have frequent access to the LC-39 Press Site, and have approval of the NASA/KSC Public Affairs Office, may be issued KSC identification badges. The KSC PAO must coordinate with NASA Protective Services and Safeguards Office prior to approving issuance of badges. Badge requests shall be submitted to the VRC. The badge shall be imprinted with the words "NEWS MEDIA" in the orange area to the right of the individual's picture.

(b) The badge shall permit access to KSC through KSC access gates, 3, 4, 4TT, and 6TT only, during designated days, as approved by The Protective Services & Safeguards Office, for travel by the shortest route to the LC-39 Press Site when it is in operation. Access to all other areas, except the LC-39, shall be under PAO escort.

(5) Labor Union Representatives

Union representatives who meet the requirements of KSC/CCAFS regulations may be issued KSC identification badges. **Only the NASA Labor Relations Office may approve requests for these badges**. The badge shall be imprinted with the words "LABOR UNION REP." in the orange area to the right of the individual's picture.

(6) Foreign Nationals

Foreign Nationals (FN) and Foreign Representatives (FR) who have been accredited by the NASA/KSC PSSO Office, may be issued badges. This badge shall be distinguished by the addition of a pale green transparent band extending horizontally

RELEASED - Printed documents may be obsolete; validate prior to use.

across the width of the badge immediately above the picture and covering the badge number.

15.13 TEMPORARY PASSES

a. Temporary passes are computer-generated passes that may be issued for temporary access to KSC and CCAFS. Computer generated temporary passes are issued at KSC PIDS III, CCAFS PIDS I, VRC, and F Gate. Temporary Pass Types are as follows:

(1) White (WTP) – No escort required. Issued to visitors with a known employment or personal history with the person authorizing the pass. WTP visitors may escort pink or green pass visitors.

(2) Pink (PTP) – Escort required. Issued when employment or personal history with the person authorizing the pass is not known. Must be escorted at all times.

(3) Green (GTP) – Foreign Nationals. Escort required at all times

(4) Escort Designee Acknowledgement Form 8-893 must be provided to the security officer at the gate when entering the gate, for all personnel with a pink or green temporary pass.

(5) Two forms of identification are required by the badging station/gate to verify the identity of the visitor.

(6) Primary ID – Drivers License; State ID Card; DoD, State or Local Government ID Card, U.S. Passport; Resident Alien ID; Foreign National Passport; U.S. Coast Guard Merchant Marine ID Card.

(7) Secondary – Certificate of U.S. Citizenship; U.S. Birth Certificate; Certificate of Naturalization; Unexpired Temporary Resident Card, Voter Registration Card; Native American Tribal Document; U.S. SS Card; Certificate of Birth Abroad issued by the Department of State.

b. Temporary passes may be issued for short-term visits not to exceed 364 days. Temporary Passes may be issued to:

RELEASED - Printed documents may be obsolete; validate prior to use.

(1) NASA employees visiting KSC and/or NASA controlled areas at CCAFS, who have not been issued a NASA or KSC identification badge.

(a) Unclassified Visits. Arrangements for visits should be made sufficiently in advance to allow badging to be arranged as required.

(b) A prime contractor may designate up to 10 persons as authorized temporary badging officials for each subcontractor. The names shall be furnished by correspondence to the VRC through the prime contractor security office.

(c) Delegation of badging authority correspondence should include the local company address and phone number, work phone numbers of authorizing personnel, areas of performance, contract number, and expiration date of subcontract.

(d) Designated badging officials for Construction Contracts must contact the VRC to arrange for a briefing and assignment of a control number. This control number must be used each time a badge or pass is requested.

(e) Classified Visits NASA employees shall arrange for their installation security office to forward clearance information to the VRC as follows: Full name, Social Security Account Number, date of birth, place of birth, clearance level, date clearance granted, and name of organization granting clearance.

(2) Visitors from organizations holding a Facility Security Clearance The visitor shall have the security officer who maintains the original Letter of Consent, forward it to the VRC with the following information in writing by e-mail, FAX, or letter.

(a) Employee's full name.

(b) Employers complete name including, if applicable, department or division and address; also address of security officer, if different.

(c) Employee's level of clearance.

RELEASED - Printed documents may be obsolete; validate prior to use.

(d) Date clearance was granted.

(e) Name and location of authority who granted the clearance.

(f) Employee's social security account number (SSAN), date and place of birth and citizenship.

(g) Dates covered by visit clearance, not to exceed the duration of the contract.

(h) Name and telephone number of KSC contact or person to be visited.

(i) Purpose of visit.

(j) Applicable NASA contract number, if any.

(3) Non-NASA Government Employees The employee shall have his/her security office forward to the VRC by FAX**,** E-mail or letter the information required in the above paragraph (NASA contract number not required).

(4) Official Visitors. The pass must be authorized by a badging official employed by a firm or organization under contract or subcontract to NASA/KSC, by a badging official of a KSC tenant organization, or by a NASA/KSC official or his/her representative. The VRC shall have on file a list of designated badging officials.

(5) Delivery Persons

(a) Company badging officials of the company/organization receiving the shipment must verify deliveries and request a pass be issued. Multiple passes may be issued off one Bill of Lading to accommodate co-drivers, helpers, etc.

(b) Individuals making deliveries/pickups after hours or on weekends shall not be issued a Temporary Pass until coordination has been made to ensure that a representative is available at the delivery or pickup site.

(6) Salespersons

RELEASED - Printed documents may be obsolete; validate prior to use.

(a) A designated badging official of the organization requesting sales or by a NASA/KSC official or their representative must approve the Pass.

(b) Sales demonstrations for NASA organizations must be approved by NASA Procurement, prior to arrival of the individual presenting the demonstration.

(c) Passes shall be normally issued for one day only.

(7) Fruit/Grove Employees

(a) A group pass may be issued upon request by a picture-badged grove employee. The request must include full names and Social Security Numbers of all persons to be included in the pass. The pass shall be limited to citrus picking and grove maintenance crews and shall be issued for 1 day only. The number of persons shall be shown on the face of the pass. The Badging Security Officer shall verify identification of the workers prior to their issuing the passes.

(b) Individual grove pass may be issued to other persons affiliated with the groves such as fruit buyers, salesmen, etc., upon request by an authorized grove badging official through the VRC.

(c) Citrus grove employees may enter and exit KSC through KSC gates only. Those employees who enter on a "group" temporary pass must be escorted at all times by a "GROVES" picture-badged employee.

(8) Personnel Attending Meetings, Conferences, or Employment Interviews The pass must be authorized by a badging official employed by a firm or organization under contract or subcontract to NASA/KSC, by a badging official of a KSC tenant organization, or by a NASA/KSC official or his/her representative. The VRC shall maintain a list of designated badging officials.

(9) KSC Employees Who Left Their Badges at Home Temporary passes can be issued to employees that have left their badges home at PIDS or, an access gate when PIDS are closed. A white temporary pass shall be issued upon verification of employment through the VRC Personnel Access Security

RELEASED - Printed documents may be obsolete; validate prior to use.

System (PASS) and with proper identification. Left Badge at Home (LBH's) passes are normally issued for one (1) day to employees who left their badge a home.

(10) News Media

(a) A temporary pass may be issued to news media members after approval has been received by the VRC from the NASA/KSC Public Affairs Office.

(b) During launch and landing activities, the Public Affairs Office issues passes to news media members from the Gate , Pass and Identification Station.

(11) Foreign Nationals and Foreign Representatives Visits by foreign nationals and foreign representatives to NASA KSC require approval from the NASA KSC International Visits Coordinator.

(l2) Construction Employees

(a) A badging official of the employee's organization or contractor organization to whom they are subcontracted must request the pass. Passes may be issued for a period of 364 days or until the expiration of the contract, whichever is shorter.

(b) Temporary passes issued to construction employees shall be marked with the word **"CONSTRUCTION"** in bold letters across the top.

(13) Other Individuals who have been Authorized and Approved through the VRC

Personnel under the age of 16 years shall not be issued a Temporary Pass without approval of NASA Protective Services and Safeguards Office.

c. Information Required

(1) Badging officials requesting temporary passes must provide the following information:

(a) Full proper name of visitor. (i.e., Robert, not Bob)

RELEASED - Printed documents may be obsolete; validate prior to use.

(b) Social Security Account Number

(c) Date(s) of visit

(d) Company or agency the visitor represents, street address, city, and state

(e) Area(s) to be visited

(f) Purpose of visit

(g) Approving company or NASA department

(2) The visitor shall be asked to show proper identification [See para 15.13, (a)(6) and (a)(7), above] upon arrival at the Pass and ID Station. Upon confirmation that the pass has been approved, the pass shall be issued.

(3) After normal working hours and on weekends and holidays, temporary passes shall be issued by the Security Officer at the gate after confirmation that the individuals visit authorization has been processed through the VRC or J-BOSC Security Watch Commanders Office.

d. Description The temporary pass may be completed/filled in by computer or be hand-written and contain at least:

(1) Name of individual

(2) Expiration date of approved visit

(3) PRP status, if authorized

(4) Organization/employer

(5) Areas authorized to visit on KSC or CCAFS

(6) Special identification (news media, delivery, grove, or construction), if applicable.

(7) When entering information into PASS, all the required should be completed with the individual's information.

e. Use

RELEASED - Printed documents may be obsolete; validate prior to use.

(1) The Computer-generated Temporary Pass is used for access to KSC/CCAFS and shall be worn above the waist by the individual. Whenever possible, the Temporary Pass should contain a photo and signature.

(2) An escort shall be required in secure areas (limited or controlled) unless the individual has been issued an additional permit or badge requiring no escort.

(3) Temporary passes are not required to be returned to security personnel at the end of an official visit, but should be destroyed upon expiration of the pass.

f. Advanced Temporary Pass

(1) Designated badging officials may request advanced Temporary Passes from the VRC when it is necessary to accommodate personnel supporting operational activities. Advanced passes shall not be issued for more than five (5) duty days. Then the pass holder must be issued a new pass with photograph and signature.

(2) After providing the information required in paragraph 404.13(b)(1-10), to the VRC, the requesting officials, when notified that the advanced passes are completed, shall pick-up the completed advanced temporary passes.

(3) The requesting official shall be responsible for the delivery of the temporary passes to the visitors and shall ensure proper identification is made.

(4) Temporary passes issued without the visitor’s picture shall not be issued for periods exceeding 5 days in duration. If duration is for a longer period of time, the individual must report to VRC, PIDS I or PIDS III, to renew the pass with a picture and signature.

15.14 OFFICIAL VISITOR PASS(ESCORT REQUIRED)

a. Official Visitor passes may be issued to NASA/KSC Directorates and Chief Executive Officers (CEO's) of KSC's primary contractor organizations (BOC, SPC, and PGOC) for their convenience in badging important visitors on official business.

RELEASED - Printed documents may be obsolete; validate prior to use.

b. Official Visitor passes approved by a Director/CEO, may be issued to VIP visitors, when it is considered to be more appropriate than a temporary pass.

c. Official Visitor passes may be issued by the NASA Workforce & Diversity Management Office to organizations that do not have badges on an as-requested basis for one-time use when the request is made directly from a Director/CEO.

d. KSC Directors and contractor CEO's, or their representatives, who have been designated in writing, shall be required to sign for the Official Visitor passes assigned to their organization.

Receipts provided by the VRC shall contain the issued pass serial numbers and the instructions for issuing the badge. After receipt, the custodian shall maintain a copy of the receipt with the passes. Together with the passes and receipt, a KSC form 0-43, "Identification Log", shall be maintained and used to log the use of the passes. The log sheet shall be filled out as follows:

(1) Serial Number: Enter the pass number.

(2) Issued to: Print name of individual requesting the pass.

(3) Signature: Have requester sign the log.

(4) Organization: Enter mail code and phone number of requester.

(5) Date Issued: The date the pass leaves organizational custody.

(6) Date Returned: The date the pass was returned to organizational custody.

(7) Clearance: The company or organization that the visitor represents.

(8) Remarks: Print the visitor's name; indicate if the visitor is a minor. If the request for the visit was made via an AVO, the AVO should be referenced and a copy attached to the log.

Log sheets shall be forwarded to the VRC or The Protective Services & Safeguards Office on a monthly basis, but only after

RELEASED - Printed documents may be obsolete; validate prior to use.

the pass have been returned. Badges are not intended for long-term issue; therefore, the log sheets should be completed by the end of the first work week of the month and forwarded. Negative reports are not required.

Official Visitor passes shall be securely maintained. Pass shall be stored in locked desks, file cabinets, or secure storage containers (safes).

e. Official Visitor passes are not allowed access into operational or sensitive security areas.

f. **Official Visitor passes are not issued to Foreign Nationals or representatives of foreign nationals, unless specifically approved through the Protective Services and Safeguards Office.**

g. Public Affairs personnel are responsible for conducting official tours. These responsibilities cannot be delegated to others; therefore, Official Visitor passes **ARE NOT** authorized for tours.

h. Official Visitor passes must be returned to the sponsor upon completion of the visit. In case of loss, a "lost badge" memo (ref. paragraph 404.6) must be submitted to the VRC by the person to whom the pass had been issued, with the signature of the Director/CEO having had the badge originally, indicating their knowledge of the loss of the badge.

i. Upon expiration of their contract, contractors must return all assigned Official Visitor Passes to the VRC.

j. Official Visitor passes are not issued to persons under the age of 16 years without approval of NASA Protective Services and Safeguards Office.

15.15 EXIT PASS

a. The Exit Pass, KSC Form 0-133, is authorized for use by both NASA personnel and KSC contractors, primarily for exit of terminated employees whose valid badges have been surrendered to designated badging officials. It may also be utilized for other purposes, as specifically authorized by The Protective Services & Safeguards Office. This pass is valid for exit only from either KSC or CCAFS gates.

RELEASED - Printed documents may be obsolete; validate prior to use.

b. NASA or the contractor security office processing the terminated employee shall issue the exit pass.

c. Exit passes are not required to be turned in to security personnel. However, they are valid only for the date of issuance and for the reason indicated.

15.16 SPECIAL BADGES AND PLACARDS

a. General. Special badges and placards are used to meet the special requirements of the KSC Director, visiting dignitaries, public affairs events, special meetings, conventions, operational considerations, landings, and launches. Most of the documentation for their specific use, issue, and control is fragmentary and provided to the security force as addendum to post orders. These special badges and placards are an adjunct to the established system; come in a variety of shapes, sizes, colors, and designs; provide personnel and vehicle access to KSC; and provide the attendee with a memento of some event associated with KSC.

b. Request Procedures. Special badges and placards may be requested from NASA Protective Services and Safeguards Office through the Visitor Records Center (VRC), as required, for special events, ceremonies, meetings, etc., and should be coordinated in sufficient time to allow specific verbal or written access instructions to be conveyed to the guests/attendees prior to the special function.

c. The Center Director's Guest Credential. The Center Director's Guest Credential was established to provide a means to handle distinguished visitors of the CD. It is the top-level credential for official visits and is controlled by CD letter dated January 1, 1998.

CHAPTER 16. PERSONNEL CONTROL AND AREA PERMITS

16.1 GENERAL

Kennedy Space Center Area Permits (KSCAP), Personnel Access Control and Accountability System (PACAS) cards and Temporary Area Authorizations (TAA's) are used to control access to operational, flight hardware, and restricted areas at KSC and at NASA-controlled facilities at CCAFS.

Area Permits and TAA's shall be issued only to individuals requiring access to controlled areas in conjunction with official duties and shall not be requested for convenience or status purposes.

RELEASED - Printed documents may be obsolete; validate prior to use.

The KSC Visitor Records Center (VRC), operated by the J-BOSC, maintains clearance and badging data, and processes, fabricates, and issues badges, permits, and identification cards for all KSC organizational elements, their contractors, and visitors, according to standards set by The Protective Services & Safeguards Office.

16.2 RESPONSIBILITIES

a. The Center Chief of Security is responsible for establishing requirements for entry to KSC and its controlled access areas/facilities, and for managing and implementing the KSC Area Permit program for controlling access to those areas/facilities.

b. Heads of KSC organizational elements are responsible for identifying and furnishing to The Protective Services & Safeguards Office, a listing of all operational, flight hardware, and restricted areas requiring access controls by Area Permits/TAA's in which mission-related tasks or tests are being performed within their areas of responsibility.

c. The Director, Safety, Health, and Independant Assessment is responsible for establishing safety training requirements which must be completed prior to issuance of a KSC Area Permit or TAA, authorizing unescorted access to controlled areas and approving and establishing manloading requirements at, or within each area designated as hazardous.

d. Heads of primary organizations are responsible for ensuring the following:

(1) Those personnel who do not require frequent access to controlled areas are issued TAA's rather than a KSC Area Permit.

(2) That areas contained on the KSC Area Permit and TAA's are limited to those necessary in the performance of an individual's duties.

16.3 DISPLAY AND SAFEGUARDING OF KSCAP AND TAA

a. The Area Permit or TAA shall be worn above the waist, readily available for inspection, at all times while in a controlled area.

RELEASED - Printed documents may be obsolete; validate prior to use.

(1) Area Permits may be inserted into clear plastic holders and worn on a necklace-type material.

(2) TAA's may be attached directly to a necklace or to clothing by a clip or other fastener.

(3) Necklace material must be of a type approved for use by the safety office.

(4) Items; such as, tape, clips (except badge clips), pins, etc., shall not be fastened to Area Permits, PACAS cards, or TAA's in any manner. Area Permits, PACAS cards, and TAA's shall be carried by the person to whom issued at all times while on KSC/CCAFS. While off duty, they must be safeguarded to prevent loss or use by unauthorized personnel. Vehicles are not recognized or authorized as a proper location for storage of Area Permits, PACAS cards, or TAA's.

b. PACAS cards are not required to be displayed.

c. Individuals shall comply with any request by security personnel, or access control personnel to surrender Area Permits, PACAS cards, or TAA's for physical inspection.

16.4 ACCESS PROVISIONS

a. All personnel requiring access to KSC-controlled operational, flight hardware, and restricted access areas must possess (1) a NASA, KSC identification badge or Temporary Pass, or CCAFS identification badge or visitor's pass, and (2) a KSC Area Permit or TAA.

b. Area Permits and TAA's shall be issued to essential personnel only. The sponsoring organization shall be considered responsible for the essential nature of the access requirement, certification of required training, and the conduct of the employee within controlled areas. Each individual must meet one or more of the following criteria to be authorized access (issued an Area Permit or TAA) to a controlled area:

(1) Operations personnel associated with STS/ELV/ISS or other payload assembly, processing, or testing.

(2) Support personnel required for maintenance and operation of the facility and associated equipment.

Note: An individual may be issued both an Area Permit and a TAA.

RELEASED - Printed documents may be obsolete; validate prior to use.

c. In addition to meeting one of the criteria listed in b.(1) or (2), an individual shall only be issued a KSCAP to those areas where a frequent access requirement has been clearly demonstrated. Otherwise, a TAA shall be requested and used as the access credential.

Refer to appropriate chapters in this document for personnel security clearance and investigation requirements.

d. Each KSC organization shall have web based access to the "KSC Area Access Authorization Matrices" listing personnel who are authorized to approve access to controlled areas on KSC/CCAFS. Individuals listed in the matrices have the authority to approve access to specific areas under their operational jurisdiction. (Note: If an organization cannot obtain web based access to the matrices, an organization may request a printed copy from the VRC.)

e. Consultants, subcontractors, and miscellaneous service contractors with a limited number of personnel shall be treated as part of the sponsoring NASA, Government agency, or contractor organization for Area Permit and TAA processing.

f. When authorization to possess an Area Permit or PACAS card no longer exists (i.e., upon termination of employment, end of visit, leave of absence, or expiration of contract), the Area Permit/PACAS card shall be surrendered to the employee's organization Authorized Requester.

Note: Foreign Travel: Generally, KSCAPS, TAA's, and PACAS credentials shall not be taken into a foreign country. Personnel assigned TDY to non-CONUS Transatlantic Abort Landing (TAL) sites shall take KSCAPS and TAA's to meet access requirements in the event that a Space Shuttle lands at one of the TAL sites.

TAA's should be destroyed by the holder immediately after the TAA expiration date. When a TAA is still valid and determination is made the TAA is no longer required, it should be turned in to the VRC or Gate F Pass and ID personnel.

g. Should an area that is controlled under the Area Permit System have an emergency situation declared, all necessary emergency personnel (i.e., fire, medical, security, environmental health, etc.) responding to

RELEASED - Printed documents may be obsolete; validate prior to use.

the area shall be allowed access to the areas even though they may not possess an Area Permit or TAA.

Note: Protective Services & Safeguards Office personnel may enter all areas on KSC upon presentation of their security credentials.

h. Any individual having the knowledge or suspicion that regulations regarding Area Permits, PACAS cards, and TAA's are or have been violated is required to report those violations to their security office. Unauthorized use of any Government-issued identification or access card or credential (including, but not limited to, the transfer, sale, gift, loan, use as collateral, or use to gain access to or remain in an area or on the installation for other than official purposes) or any mutilation, destruction, or forgery (including alteration or duplication) thereof, may subject the person responsible to exclusion from KSC, punishment by law, and/or administrative action by his/her employer.

i. New areas for coverage under the KSC Area Permit System may be added only after need and implementation criteria have been determined and approval received from the Protective Services & Safeguards Office.

16.5 SAFETY FAMILIARIZATION REQUIREMENTS

a. Personnel requiring access to certain designated operational areas require safety familiarization training before being granted unescorted access to those areas. Area safety training shall be scheduled through the respective organization’s training coordinator.

Courses may be presented as video, film, or lecture courses in a classroom setting or as a physical "walkdown" at the designated location.

b. Forms certifying completion of safety training shall be forwarded by the respective NASA and contractor organizations (except for the Shuttle Processing Contractors) to J-BOSC Training for inclusion into the KSC Training Certification Record System database.

c. Shuttle Flight Operations Contractor (SFOC) shall forward forms certifying completion of safety training to SFOC Technical Training. Cargo Assembly Payload Processing Services (CAPPS) personnel and NASA Payload customers shall forward forms certifying completion of safety training to CAPPS Technical Training.

RELEASED - Printed documents may be obsolete; validate prior to use.

16.6 TEMPORARY AREA AUTHORIZATIONS

a. A Temporary Area Authorization (TAA) may be issued to an individual who requires access to controlled areas occasionally, but not often enough to justify possession of an Area Permit, or who does not meet both security and safety training requirements. TAA's are not issued to personnel who have Guest, Flight Crew, Barge Crew or "bullet badges".

The TAA is a paper card with preprinted numbers on the front to indicate to which controlled areas the holder is authorized access, and the expiration date stamped in bold numbers/letters on the front. The TAA may be issued as an unescorted or to be escorted credential.

b. An Unescorted TAA, shall be issued on a machine printed plastic card or on KSC Form 0-147A, to individuals who meet both security and safety training requirements. Holders of KSC Form 0-147 shall be allowed unescorted access to the areas indicated on the front.

c. A "To Be Escorted" TAA, shall be issued on a machine printed plastic card or on KSC Form 0-147A, to individuals who do not meet both security and safety training requirements. Holders of "To Be Escorted" TAA's must be accompanied by an authorized individual at all times while in a controlled area. The "To Be Escorted" TAA shall allow the holder access to the areas indicated on the front.

d. An escort, when required for holders of "To Be Escorted" TAA's, may be provided by any person bearing a properly coded NASA badge, KSC identification badge, or CCAFS picture badge, in addition to a properly coded KSC Area Permit or Unescorted TAA for the area(s) to be accessed. Escorts are responsible for maintaining physical control of personnel they are escorting. Normally, escorts are limited to escorting no more than five personnel at one time.

e. Audits shall be made to ensure that employees receiving TAA's have completed the proper safety training requirements. Personnel who do not have current area safety training may be requested to surrender their KSCAP, TAA, and/or PACAS cards. Falsification of any employee's training status may result in loss of an organization's authorization to request TAA's.

RELEASED - Printed documents may be obsolete; validate prior to use.

16.7 REQUESTING AREA PERMITS, PACAS CARDS, TAA's

Individual Area Permits, PACAS cards, and TAA's must be requested as follows:

a. Area Permits shall be requested on KSC Form 0-94, "Kennedy Space Center Area Permit Application." In addition to an original Area Permit request, a new KSC Form 0-94 must be submitted for each employee when:

(1) An employee requires additional authorizations (numbers added to the Area Permit) to enter controlled areas.

(2) An employee does not require access to some areas and requests numbers be deleted from the Area Permit.

(3) An employee is reassigned to a function or organization which requires a different access number(s) on the Area Permit.

(4) An employee's safety familiarization training for KSCAP area(s) or personnel reliability program certification has expired.

b. Employees who require a new Area Permit because of a name change (marriage or legal action) shall be issued a new Area Permit in conjunction with their new picture badge request. An Area Permit application form is not necessary for this type action.

c. TAA's may be requested by telephone, electronically (e-mail or fax), or in person through the organization's Authorized Requester. The Authorized Requester shall provide required information to the VRC or Gate F Badging personnel, where the TAA shall be issued.

d. The PACAS card is a uniquely coded device used in conjunction with the Personnel Access Control and Accountability Subsystem (PACAS) to provide automated control and accountability of personnel into and out of selected areas through use of a card reader system. When a PACAS card is presented at a reader, the encoded signal is compared to the stored data for authorized access. If the entry or exit is authorized, a command shall be generated to unlock the control device (turnstile, gate, or door) to permit unalarmed entry or exit. Unauthorized attempts shall initiate an alarm in the KSC Joint Communications Control Center (JCCC). PACAS cards may also be used for entry/exit at facilities controlled by subsystems of the ESS.

16.8 LOST AREA PERMIT, TAA, OR PACAS CARD

RELEASED - Printed documents may be obsolete; validate prior to use.

a. When an Area Permit, TAA, or PACAS card has been lost, the individual to whom the Area Permit, TAA, or PACAS Card was issued must immediately report the loss to the VRC, telephone 867-7763. Contractor employees shall also report the loss to their security office. This action shall be accomplished by telephone, or in person.

b. A written or typed statement describing the loss must be forwarded by NASA personnel to the VRC. Contractor employees should forward the statement to their organization Authorized Requester. The statement must contain the following information:

(1) Name.

(2) Organization.

(3) Area Permit, TAA, or PACAS card number, if known.

(4) Type (Area Permit, TAA, or PACAS card).

(5) Circumstances surrounding the loss (where, when, attempts to locate).

(6) Statement indicating that if the Area Permit, TAA, or PACAS card is found, it shall be turned in to the Visitor Records Center.

c. If the Area Permit or PACAS card is not found within 7 days, a replacement of the type originally issued may be obtained through the organization Authorized Requester where originally issued. A TAA shall be issued to allow access to authorized areas until a replacement Area Permit is issued. A replacement TAA for a lost TAA may be issued after determination by the employee's Authorized Requester that the TAA requirement is still valid.

d. A defective KSC Area Permit and/or PACAS card can be turned in at the Visitor's Records Center or at "F" Gate where a Temporary Area Authorization (TAA) shall be issued for thirty (30) days. Replacement Area Permits and/or PACAS cards shall be issued through the organization's Authorized Requester. Or, an appointment can be made with the Security Assistant working at the VRC Area Permit Desk to have the PACAS card and the Area Permit replaced during the appointment.

CHAPTER 17. FOREIGN VISITORS

RELEASED - Printed documents may be obsolete; validate prior to use.

17.1 GENERAL

This chapter provides NASA/KSC procedures for processing visit requests of foreign nationals and foreign representatives to KSC. It does not pertain to foreign nationals and foreign representatives associated with the public information media, and those visitors as defined by NPG 1371.A.

17.2 RESPONSIBILITIES

a. The Center Director is responsible for:

(1) Implementing NASA standard procedures and requirements for receiving, coordinating, reviewing, and approving/disapproving requests for visits from foreign nationals or representatives to KSC.

(2) Designating a Center International Visit Coordinator.

b. The Center International Visit Coordinator (IVC) is responsible for:

(1) Ensuring that procedures and requirements for coordination and control of foreign visitors are established and maintained.

(2) Receiving, coordinating, reviewing and approving/disapproving, each request for foreign visitor access to KSC.

(3) Forwarding to the Office of Security Management & Safeguards, NASA Headquarters, for coordination and decision, all requests for visits by foreign heads of state or government, ambassadors, and heads of foreign government ministries and space agencies, and nationals or representatives of countries on the Designated Areas List (NPG 1371.A, Appendix A).

(4) Initiating a National Agency Check (NAC) for all foreign visitors working on accredited NASA-KSC programs or projects.

(5) Collecting and compiling data on all foreign visits and access by foreign national employees of NASA, contractors or grantees to KSC.

(6) Providing visit reports as necessary to the Office of Security Management & Safeguards, NASA Headquarters.

c. The Center Export Administrator is responsible for:

RELEASED - Printed documents may be obsolete; validate prior to use.

(1) Reviewing the information provided by the IVC for foreign visits and making all appropriate contacts and/or inquiries to make a recommendation for or against the visit in question.

(2) Approving Technology Transfer Risk Assessments for long term visits.

d. Heads of primary organizations and NASA Contractors are responsible for:

Ensuring that personnel under their cognizance familiarize themselves and comply with the requirements of this chapter.

17.3 VISITOR IDENTIFICATION/PROGRAM DEFINITIONS

a. Foreign National (FN). Any person who is not a citizen of the United States.

b. Foreign Representative (FR) or Representative of a foreign entity. Any person, including a citizen, permanent resident alien or protected individual of the United States, who represents a government, business, organization, or person of a country other than the United States.

c. Accredited FN/FR. Foreign nationals or representatives who have received the appropriate checks and credentials, and been approved for repeat visits to specific NASA Centers for the purpose of implementing an “agreed” NASA international cooperative or reimbursable program or project.

d. Non-accredited FN/FR. These FNs/FRs are individuals who have been approved for access to KSC, for reasons other than the specific program/project involvement.

e. Agreed international program or project. One that has a signed Space Act Agreement between NASA Headquarters and a foreign entity (e.g. an agency or organization of a foreign government, a foreign educational institution, a foreign company, or an international organization.)

f. Visit. Access to a NASA Installation or acility by foreign nationals or a U.S. citizen representative of a foreign entity for a period of 30 ay or less.

RELEASED - Printed documents may be obsolete; validate prior to use.

g. Assignment. Access to a NASA Installation or Facility by a foreign national or a U.S. citizen representative of a foreign entity for a period in excess of 30 days.

17.4 VISIT TYPES AND DEFINITIONS

a. Standard Foreign Visits. Any visit by a FN or FR of any country except countries identified as a designated area (see NPG 1371.A, Appendix A). The exception to this would be if the individual from the designated area is on a Center approved accreditation list working on an agreed international program or project for which the accreditation list was established. The international program or project must be with, or provide for participation by, that country in order for the individual to be on that accreditation list.

b. Nonstandard Foreign Visit. A visit by a FN or FR of a country identified as a designated area in NPG 1371, Appendix A.

c. High Level Protocol Visits. A visit by a senior foreign official, distinguished individual, or a high-ranking delegation that requires detailed, advance preparation and coordination on matters of protocol (i.e., foreign heads of state, government ministers, ambassadors, and heads of governmental agencies). The High Level Protocol Visit may include a courtesy meeting with the Center Director or other senior management representative, a guided tour of the Center's major facilities, and possibly a detailed briefing on NASA's programs or projects.

d. Designated Area. A country of special concern or interest for the reasons identified in NPG 1371.A, Appendix A.

17.5 VISIT REQUEST PROCEDURES

a. All requests for a standard visit, nonstandard visit, and/or High Level Protocol Visit should be submitted, in writing, to the KSC IVC. Requests may be sent by e-mail, fax, or through the mail (e-mail is preferable).

b. Requests should be complete and contain the following information:

(1) Full Name

(2) Date and Place of Birth (City and Country)

(3) Citizenship

RELEASED - Printed documents may be obsolete; validate prior to use.

(4) Passport/Visa Number, Date and Place Issued

(5) Passport/Visa Expiration Date

(6) Visa Type (i.e., B-1, H1-B, etc.)

(7) Social Security Number (if applicable)

(8) Company Affiliation

(9) Company Address

(10) KSC Point of Contact and Telephone Number

(11) Dates of Visit

(12) Areas to be visited

(13) Accreditation information, if known (i.e., international program or project, responsible accrediting Center).

(14) Detailed justification for visit (include whether visitor shall have access to computers, data to be disclosed, etc.).

c. An Technology Transfer Risk Assessment is to be provided by the Requester for Center Export Administrator (CEA) review and approval on all visits in excess of thirty (30) days or the individual is a frequent visitor, and when the visitor is from a Designated Area (regardless of visit duration).

d. The request shall be reviewed by the IVC.

If the request is for an individual from a designated area after local checks and approval, the request shall be forwarded to the Office of External Relations, NASA Headquarters, for final approval.

e. If the request is denied, the IVC shall advise the Requester that the request was denied.

f. Requesters must allow sufficient time to permit processing of requests.

(1) Short-term visit requests (1 to 30 days in duration) shall be reviewed by the IVC and approved or disapproved within 10 working days (weeks).

(2) Long-term visit requests (longer than 30 days) shall be reviewed by the IVC and approved or disapproved within 0 working days (4 weeks).

RELEASED - Printed documents may be obsolete; validate prior to use.

(3) VIP tour requests shall be handled as expeditiously as possible.

(4) Short-notice visit requests shall normally be denied. Emergency short-notice visits shall be worked on a case by case basis.

17.6 ACCESS AUTHORIZATIONS

a. FNs/FRs may receive a picture badge, or a Temporary Pass for up to one year. The picture badge must be retrieved each time the FN/FR leaves to return to their country. The Temporary Pass may be set up for short or long duration and may be renewed if an extension is necessary. The FNs/FRs may also have unescorted access to some controlled areas, providing safety training and operational needs are met and a KSC Form 0-181 (Foreign National Security Questionnaire) has been received by the Protective Services & Safeguards Office.

b. The IVC, or designee, is the final approval authority on badging and access to KSC by FNs/FRs.

17.7 TOURS

All tours with FN/FR participation shall be processed through the KSC IVC. The KSC IVC shall coordinate VIP tours (described in paragraph 406.4c) with the Office of External Relations, NASA Headquarters, and with the organization requesting the tour. The IVC shall also coordinate any tours deemed appropriate with the CEA.

This coordination should take place before the letter requesting tour credentials is processed through the Center Director's Office. It should be indicated in the credential request letter that coordination with the IVC has already taken place.

The IVC shall notify the Center Director's staff if a tour has been disapproved so credentials shall not be issued.

17.8 FOREIGN PUBLIC INFORMATION MEDIA

Requests by, or on behalf of, foreign national members of the public information media to KSC or a component Facility must be forwarded promptly to the NASA Workforce & Diversity Management Office for coordination, as appropriate, with NASA Headquarters in accordance with 14 CFR Part 113.

17.9 DISCUSSIONS AND REQUESTS FOR MATERIALS

RELEASED - Printed documents may be obsolete; validate prior to use.

Discussions with and documents provided to FN/FR visitors should be limited to information or documents authorized for public release, or specifically committed under an approved bilateral agreement. Outside presentations and papers for publication should have the approval of the Center Export Administrator.

17.10 EXTENDING INVITATIONS TO VISIT NASA/KSC

NASA encourages visits by FNs/FRs of countries allied with/or friendly to the United States. NASA employees may, with prior approval by NASA Headquarters or the KSC IVC, extend invitations to FNs/FRs of countries other than those identified as designated areas in Appendix A. No invitation to visit NASA/KSC may be extended to FNs/FRs of any designated areas without the prior written approval of the Office of External Relations, NASA Headquarters.

17.11 VISITS TO MERRITT ISLAND LAUNCH AREA (MILA) SPACECRAFT TRACKING DATA NETWORK (STDN) STATION, FLORIDA

Foreign visit requests for this area shall be processed in the same manner as previously stated in this Chapter. When a visit is approved, the IVC shall notify the Station Director in addition to the Requester and VRC.

CHAPTER 18. PROTECTIVE BARRIERS AND OPENINGS

18.1 PROTECTIVE BARRIERS AND OPENINGS

a. Purpose. To establish minimum criteria for physical security barriers and openings at KSC. However, Space Transportation System (STS) facilities, hardware, and operations when under the provisions of the NASA Resource Protection Program must meet specific criteria. Physical barrier requirements are designed to deny, impede, or discourage access to security areas by unauthorized personnel or groups. This is accomplished by one or more of the following:

(1) Defining the perimeter of security areas.

(2) Creating a physical and psychological deterrent to entry as well as "making a legal statement" that entry is not permitted.

(3) Delaying intrusion into security areas, thus making more likely the detection and apprehension of intruders by protective forces.

RELEASED - Printed documents may be obsolete; validate prior to use.

(4) Facilitating effective and economical utilization of protective forces.

(5) In addition, physical barriers serve the purpose of directing the flow of personnel and vehicles through designated portals in a manner which permits efficient operation of the personnel identification and control system.

b. Types of Barriers. Protective barriers are divided into two major categories: natural and structural.

(1) Structural barriers are manmade devices such as fences, walls, floors, roofs, grilles, bars, road blocks, or other structures which deter penetration.

(2) Natural barriers include forests, rivers, swamps, beaches, or other terrain difficult to traverse.

c. General Consideration. Established physical security barriers at KSC are not designated to stop a determined intruder but rather to deter or delay. Therefore, such barriers, depending on area security, should be augmented by security personnel. When planning or in the establishing of security barriers at KSC, the Protective Services & Safeguards Office shall be notified for assistance and advice. The Protective Services & Safeguards Office shall consider the following prior to recommending security barriers:

(1) Physical barriers, which are as personnel-proof as economically feasible, should be established around all security areas. The type of barrier used should be determined after a study of local conditions by The Protective Services & Safeguards Office.

(2) In some instances, the temporary nature of the security interest makes the construction of costly permanent physical barriers impracticable and unjustifiable. In such cases, the security interest must be protected by other means, such as use of temporary barriers, additional protective forces, patrols, and other compensating protective measures.

(3) In cases of extreme criticality and vulnerability of KSC facilities, it may be necessary to establish two lines of physical barriers at the security area to be protected.

(4) The immediate boundaries of KSC or a specific security area should be fenced and/or posted as a security area. As a

RELEASED - Printed documents may be obsolete; validate prior to use.

minimum, two or more strands of barbed wire with "No Trespassing" signs with appropriate prosecution warnings attached not more than 500 feet apart along, and at each corner of, the boundaries of the land shall suffice. This defines the perimeter, provides a buffer zone, facilitates control, and makes accidental intrusion unlikely.

(5) In establishing any perimeter barrier at KSC, due consideration must be given to providing emergency entrances and exits in case of fire.

(6) The size of a security area shall depend on the degree of sensitivity required and the complexity of the area. As a rule, size should be kept to a minimum consistent with operational efficiency. Positive barriers at KSC shall be established for:

(a) Controlling vehicular and pedestrian traffic flow.

(b) Checking identification of personnel entering or departing.

(c) Defining a buffer zone for more highly classified areas.

(7) KSC's geographical and environmental characteristics, specifically water and swamp boundaries, present special security problems. Such areas at KSC should be defined by appropriate signs, buoys, booms, etc. Boat patrols may be required at KSC where mission-critical assets, essential facilities, or areas which are otherwise essential to the mission are located near inland or coastal waters. In inclement weather, such patrols may not provide an adequate degree of protection and must be supplemented by other means.

(8) Construction of new security barriers and removal of existing barriers and related work must be approved by The Protective Services & Safeguards Office and scheduled to provide a continuous level of security for the activity/program.

d. Temporary Barriers. In some instances, the temporary nature or infrequent existence of a sensitive program/project requiring security constraints does not justify the construction of more permanent physical perimeter barriers. In such cases, a KSC-designated limited area or closed area of temporary nature and short duration may be established in which the reduction of security resulting from

RELEASED - Printed documents may be obsolete; validate prior to use.

deficiencies in physical barriers is compensated for by additional security forces, patrols, and other security measures during the period of restriction. KSC barricade requirements are outlined in paragraph 408. below. In any case, a designated temporary security area shall not exceed 30 days from date of installment without specific authorization from The Protective Services & Safeguards Office. The use of wire barriers or similar construction for temporary enclosures is recommended as being both expeditious and effective with a minimum use of security forces required to control and safeguard the area.

18.2 BARRICADE CLASSIFICATION AND SPECIFICATIONS

a. Barricades on KSC are permanently erected installations that control access through highways, trails, secondary roads, railways, construction sites, etc. Many barricades serve as a controlling barrier to the Impact Limit Line (ILL) or into critical operation areas. Barricade markings (i.e., traffic warning devices) vary depending on the location of the barricade.

b. In an attempt to ensure that proper barricade-marking and motorist-warning devices are installed on any barricade that is erected, the following barricade classifications and specifications are furnished.

(1) Class A is defined as: When a major arterial highway is temporarily closed to traffic because of operational requirements (i.e., emergency situations, disasters, etc.). The barrier shall consist of:

(a) Three rails marked in alternate red and white stripes sloping downward at a 45-degree angle in both directions toward the center of the barricade.

(b) Red light rotating at 360 degrees.

(c) Supplemental warning signs, reflecting: ROAD CLOSED 1000 FEET AHEAD and ROAD CLOSED 500 FEET AHEAD, placed at the appropriate distance preceding the barricade.

(d) NASA RESTRICTED AREA/NO TRESPASSING sign.

(e) Stop sign measuring 30 inches across.

(f) Three red reflectors attached to the gate posts facing traffic.

RELEASED - Printed documents may be obsolete; validate prior to use.

(2) Class B is defined as: A road or street adjacent to a major arterial highway that is frequently traveled but may be temporarily or permanently closed. The barrier shall consist of:

(a) Two rails marked in alternate red and white stripes sloping downward at a 45-degree angle in both directions toward the center of the barricade.
(b) Red light rotating at 360 degrees.

(c) Supplemental warning signs, reflecting ROAD CLOSED, placed 500 feet preceding the barricade or on the barricade, as appropriate.

(d) NASA RESTRICTED AREA/NO TRESPASSING sign.

(e) Stop sign measuring at least 30 inches across.

(f) Three red reflectors attached to gate posts facing traffic.

(3) Class C is defined as: A secondary road, street, or trail that is normally open but may warrant temporary closure. The barrier shall consist of:

(a) Two rails marked in alternate red and white stripes sloping downward at a 45-degree angle in both directions toward the center of the barricade.

(b) Supplemental warning sign, reflecting ROAD CLOSED, placed on the barricade.

(c) NASA RESTRICTED AREA/NO TRESPASSING sign.

(d) Stop sign measuring 30 inches across.

(e) Three red reflectors attached to gate posts facing traffic.

(4) Class D is defined as: A secondary road, street, or trail that is normally closed to all traffic. The barrier shall consist of:

(a) One rail marked in alternate red and white stripes sloping downward at a 45-degree angle in both directions toward the center of the barricade.

RELEASED - Printed documents may be obsolete; validate prior to use.

(b) NASA RESTRICTED AREA/NO TRESPASSING sign.

(c) Stop sign measuring at least 30 inches across.

(d) Three red reflectors attached to gate posts facing traffic.

Note: Individual barricade specifications may deviate due to frequency of roadway use, operational requirements, or other considerations.

CHAPTER 19. TRAFFIC AND PARKING CONTROL

19.1 PURPOSE

This chapter establishes provisions and procedures for the supervision of motor vehicle traffic and the Reserved Parking Program at KSC. The Reserved Parking Program is also applicable to those areas of CCAFS occupied by NASA.

19.2 GENERAL

a. This chapter covers all moving and non-moving traffic regulations, the required crash reporting procedure, and the issuance of traffic citations on Kennedy Space Center. It shall provide requirements for the movement of flight hardware and over dimensioned/overweight equipment, and movement against traffic.

b. This chapter directs the assessment of points against an individual's driving record in accordance with an established schedule. It also defines the procedure for appealing the issuance of a KSC citation or the suspension of driving privileges.

c. The "Manual on Uniform Traffic Control Devices for Streets and Highways" as published by the United States Department of Transportation (U.S. DOT) and the companion Florida DOT (FDOT) Manual are the documents governing all traffic control devices on Kennedy Space Center.

d. This chapter applies to civil service and contractor personnel (GS-15 or equivalent) requesting reserved parking spaces for private and/or government vehicles at KSC and in those areas of CCAFS occupied by NASA, and to designated contractor employees who are given duties and responsibilities relating to the issuance, control, and termination of such authority.

RELEASED - Printed documents may be obsolete; validate prior to use.

19.3 MOVING/NON-MOVING TRAFFIC REGULATIONS

a. J-BOSC Security, under the direction and guidance of the Chief, Protective Services and Safeguards Office, shall be the single KSC organization responsible for the enforcement of all NASA and State of Florida Traffic Regulations. J-BOSC Security shall also investigate all motor vehicle crashes and all matters related to the safe and efficient flow of motor vehicle traffic on KSC roadways. The J-BOSC shall be responsible for the placement and maintenance of all official traffic control devices.

Any KSC Organization which requires to detour, or deviation of standard traffic patterns on KSC, shall be responsible for informing the Security Traffic Management Office, at least 30 days prior to the requirement.

b. Responsibilities:

Heads of primary organizations, or their designees, shall be responsible for:

(1) Assuring that employees and their respective contract managers are cognizant of this KNPR.

(2) Assuring that all employees within their respective organizations adhere to the requirements contained in this KNPR.

(3) Upon notification from the Lead, NASA Security Operations, taking appropriate administrative action against employees identified as habitual traffic offenders.

c. All personnel operating a motor vehicle upon the roadways of KSC must possess a motor vehicle driver's license recognized by the State of Florida as being a valid driver's license.

d. Drivers and owners of vehicles being operated on KSC shall be in compliance with all Florida Statutes concerning licensing of drivers and Florida Financial Responsibility Laws at all times.

e. Persons committing a violation of a traffic regulation on KSC shall be subject to the following:

(1) They may be issued a Florida Uniform Traffic Citation (FUTC).

RELEASED - Printed documents may be obsolete; validate prior to use.

(2) They may be issued a KSC Traffic Citation.

(3) An Offense Incident Report, with supporting documents, may be filed with the State Attorney's Office requesting a warrant be issued for the arrest of the violator.

(4) Suspension of driving privileges at the discretion of the Protective Services & Safeguards Office.

f. Personnel with accumulated points against their driving record on KSC in accordance with the schedule shown in Figure 1, (page 408-5) shall have their driving privileges suspended on KSC and by reciprocal agreement on CCAFS. The length of suspension time shall be determined by the number of points accumulated during a particular time frame as defined in Figure 1. Points accumulated as a result of an FUTC shall be assessed in accordance with existing State law. Points assessed due to issuance of an FUTC may result in the suspension of state driving privileges.

g. Persons who witness a traffic violation on KSC when no law enforcement officer is present and wish to report the violation must file a written complaint with J-BOSC Security Operations.

h. Bicycles shall be operated on KSC in compliance with Florida Statute Chapter 316.065.

i. Movement of Improperly Parked or Abandoned Vehicles to Impound Area

(1) When a vehicle is improperly parked or abandoned OR is creating a traffic hazard, the vehicle shall be towed. If it is a GSA vehicle, a duplicate key shall be obtained from transportation.

(2) Owner/drivers are responsible for contacting J-BOSC Security to report their disabled/abandoned vehicle. Disabled/abondoned vehicles shall be red tagged, defined as a “Red Tag” (KSC Form OT-79), by a Security Officer. The “Red Tag” explains to the owner that they have 7 hours to remove the vehicle or J-BOSC Security shall have it towed.

j. Parking Restrictions.

(1) Parking is not permitted on grassy areas, blocking driveways, adjacent to yellow marked curbs, in fire lanes, within 15 feet of a

RELEASED - Printed documents may be obsolete; validate prior to use.

fire hydrant, posted "No Parking" areas, reserved spaces inscribed by name, position, permit, or organization, in spaces reserved for other types of vehicles, or in any area on KSC not specifically designated for parking. Parking of vehicles is permitted on grassy areas when instructed by a J-BOSC Security Officer or if designated as overflow parking.

(2) Persons whose primary job assignments or offices are located within a building are not permitted to use that building's parking spaces reserved for visitors or Senior Management. Visitor and Senior Management parking spaces are reserved for the use of persons visiting the building. Other persons using these spaces shall be cited.

RELEASED - Printed documents may be obsolete; validate prior to use.

TRAFFIC POINTS

Points against a person's driving record on KSC shall be assessed in accordance with the State of Florida, Department of Highway Safety and Motor Vehicles guidelines. In addition, points shall be assessed for the following KSC violations:

			POINTS
*	1.	Moving violations resulting in a crash	4
*	.	Reckless driving	4
*	3.	Speed in excess of 15 mph over the posted speed limit	4
*	4.	Speed not in excess of 15 mph over the posted speed limit	3
*	5.	All other moving violations	3
	6.	Includes, but not limited to; failure to obey the directions of a Security Officer, or failure to obey an official KSC Traffic Regulatory sign	3
*	7.	Improper/defective equipment (brake lights, headlights, reflectors, wiper blades, etc.)	
	8.	Includes, but not limited to; Violation of KSC parking regulation	1
	9.	Failure to use seat restraints	1
	10.	Includes, but not limited to; failure to properly process a KSC traffic citation	1

* These violations are in accordance with Florida Statutes and are not considered just a KSC violation. The violations not marked with an asterisk (*), are points assessed solely on KSC and not Florida Statutes.

FIGURE 1

RELEASED - Printed documents may be obsolete; validate prior to use.

SUSPENSION

Persons who accumulate sufficient points to cause their driving privileges to be suspended shall have their driving privileges suspended, in accordance with the schedule below:

1 points accumulated within 1 months	30 days suspension
18 points accumulated within 18 months	90 days suspension
4 points accumulated within 36 months	1 year suspension
Refusal to submit to an approved breath alcohol test for a traffic-related offense	1 months suspension
Convicted of DUI by a Court of Law	1 year suspension (or the Court-imposed suspension, whichever is greater)
Driving while driving privileges are suspended.	The Chief, Protective Services & Safeguards Office, shall request administrative action be taken against the defendant
Failure to produce proof of insurance	KSC driving privileges shall be suspended by the Chief, Protective Services & Safeguards Office, until such proof is produced
Reckless or careless operation of a Motor Vehicle	KSC driving privileges shall be suspended at the discretion of The Protective Services & Safeguards Office

FIGURE 2

RELEASED - Printed documents may be obsolete; validate prior to use.

19.4 OVERWEIGHT/OVERDIMENSION EQUIPMENT/VEHICLES AUTHORITY/ESCORT

a. Movement of equipment/vehicles which exceed the maximum width, height, length, and weight criteria set forth in Chapter 316 of the Florida Statutes is authorized within the confines of KSC. The following requirements are to be observed for movement of over dimensional equipment/vehicles on KSC.

(1) Width:

(a) All loads or vehicles that do not exceed the maximum height and length, but are between 8 feet, 6 inches (.61 meters) and 10 feet (3.07 meters) wide shall be flagged on each corner of the equipment/vehicle. No escort is required.

(b) All loads or vehicles between 10 feet (3.07 meters) and 1 feet (3.69 meters) wide shall be flagged on each corner of the equipment/vehicle and have "Wide Load" warning signs on the front and rear of the equipment/vehicle. No escort vehicle required.

(c) All loads or vehicles between 1 feet (3.69 meters) and 13 feet (4 meters) wide shall be flagged on each corner of the equipment/ vehicle, have "Wide Load" warning signs on the front and rear of the equipment/vehicle, and shall require one user escort vehicle. The escort vehicle shall be in the front on a two-lane roadway and in the rear on a four-lane roadway. User escort vehicle must be equipped with amber flashing light and an “Escort in Progress” sign visible to affected traffic. Lights shall conform to Florida DOT trucking manual standards.

(d) All loads or vehicles over 13 feet (4 meters) wide shall be flagged on each corner of the equipment/vehicle, have "Wide Load" warning signs on the front and rear of the equipment/vehicle, and shall be escorted by two user escort vehicles. The escort vehicles shall be in the front and rear of the load. User escort vehicle must be equipped with amber flashing light and an “Escort in Progress” sign visible to affected traffic. Lights shall conform to Florida DOT trucking manual standards.

RELEASED - Printed documents may be obsolete; validate prior to use.

(e) All loads or vehicles that exceed 14 feet (4.3 meters) in width shall be flagged on each corner of the equipment/vehicle, have "Wide Load" warning signs on the front and rear of the equipment/vehicle, and shall be escorted by two Security vehicles. Exemption to this requirement shall be made on a case-by-case basis, or as specifically exempted in this KNPR. Two-user escort vehicles may be used after approval by the J-BOSC Security Projects and Integration Office during normal working hours or the Shift Operations Office, after hours.

(f) All loads or vehicles which oppose the flow of normal traffic shall be flagged on each corner of the equipment/vehicle, and shall be escorted by three Security vehicles. The Security escort vehicles shall be in front and rear of the convoy.

(2) Height:

(a) All loads or vehicles that exceed 13 feet, 6 inches (4.15 meters) but are less than 16 feet (4.9 meters) in height shall require one user escort vehicle. On a two-lane roadway, the escort vehicle shall be in the front of the convoy. On a four-lane roadway, the escort vehicle shall be in the rear of the convoy. User escort vehicle must be equipped with amber flashing light and an “Escort in Progress” sign visible to affected traffic. Lights shall conform to Florida DOT trucking manual standards.

(b) All loads or vehicles that exceed 16 feet (4.9 meters) in height shall require two user escort vehicles, one in front and one in the rear of the convoy. User escort vehicle must be equipped with amber flashing light and an “Escort in Progress” sign visible to affected traffic. Lights shall conform to Florida DOT trucking manual standards.

(c) All loads or vehicles that exceed 13 feet, 6 inches (4.15 meters) and must oppose traffic to bypass an overhead obstruction shall be supported by two Security vehicles for that portion of the convoy move.

RELEASED - Printed documents may be obsolete; validate prior to use.

(3) Overlength:

(a) All loads or vehicles that exceed 60 feet (18.46 meters) in length but are less than 75 feet (3 meters) in length may travel on the KSC roadways system, but must be flagged on each corner of the equipment/vehicle and at the rearmost extension of the load. No escort required.

(b) All loads or vehicles that are between 75 feet and 85 feet in length shall be flagged at each corner of the vehicle and at the rearmost extension of the load. One user escort vehicle shall be required. The escort vehicle shall be in the rear of the convoy.

(c) All loads or vehicles that exceed 85 feet in length shall be flagged on each corner of the equipment/vehicle and at the rear-most extension of the load, and shall require two Security escort vehicles or two user escort vehicles. Security concurrence must be obtained prior to user's escorting. The escort vehicles shall be in front of and to the rear of the convoy.

(4) Weight:

(a) The following gross weight limitation chart applies to the KSC roadway system for most loads/equipment:

1. NASA Causeway overpass - 80,000 lbs.

2. NASA Causeway Indian River Bridge - 80,000 lbs.

3. NASA Causeway Banana River Bridge - 80,000 lbs.

4. Kennedy Parkway (SR-3) Haulover Canal Bridge - 60,000 lbs.

(b) For all KSC operational support equipment that exceeds the above weight limits, a request must be submitted to the Facilities Division for a one-time move, or a blanket or permanent waiver.

(c) Movement of over dimensional equipment/vehicles shall not be permitted unless each movement is covered by a written authorization in the form of a Work Order, Support

RELEASED - Printed documents may be obsolete; validate prior to use.

Request, Work Assignment, Shipping Order, etc. Each authorization shall constitute a "special permit" for the movement of such equipment/vehicles on KSC roads under Section 316.550 of the Florida Statutes. Prior to the actual move of such equipment/vehicles, J-BOSC Security (853-159) shall be contacted to ensure that the movement does not conflict with any other such movement. Movement during 0600-0800, 1500-1700 or 300-400, Monday through Friday, is prohibited. Exceptions shall be reviewed on a case-by-case basis.

b. Other Escort Requirements:

(1) Slow moving equipment/vehicles, as defined in FS 316.045(1), must be in compliance with Florida Statutes while traveling on KSC roadways. Slow moving vehicles shall have a “Slow Moving Vehicle” sign affixed to the rear of the equipment or vehicle. Slow moving vehicles shall not be permitted on KSC roadways during the hours of 0600-0800, and 1500-1700, and 300-400 hours, Monday through Friday.

(2) Escorting selected oversize items, flight hardware and mission critical astronauts on KSC roadways shall be the responsibility of J-BOSC Security. Mission Critical astronauts shall be escorted in the configuration outlined in J-BOSC Security mission unique Plans.

(3) Flight hardware is defined as an item or piece of equipment which, when installed or attached, becomes an integral part of the Orbiter, external tank, SRBs, or cargo at launch. Flight hardware for the purpose of scheduling a security escort, shall be that flight hardware (as defined) which is an element of the upcoming and the next subsequent launch. Security shall normally escort Transcan/Strongback moves, satellite moves, explosive or hazardous material moves which present a danger if a mishap occurred, External Tanks (ETs), Space Shuttle Main Engines (SSMEs), Forward Reaction Control Systems (FRCS), Orbiter Maneuvering System (OMS) pods, APU/HPU carts, Solid Rocket Booster (SRB) aft skirts, Crew Transport Vehicle (CTV), Orbiter Tail Cone and SRB segments (except when transferring a segment between the RPSF and VAB). Spent SRB segments shall be moved from CCAFS to KSC with one Lead J-BOSC Security Escort. Segments are transferred between the RPSF and VAB by the user/contractor.

RELEASED - Printed documents may be obsolete; validate prior to use.

(4) The user/contractor is expected to escort all other Shuttle Transportation System associated equipment, such as small payload elements or flight hardware that could fit into a standard size vehicle, non-oversize flown hardware, SRB segments between the RPSF and VAB, main chutes, forward skirts, nose caps, tail cone crates, 140, 50, and 300-ton cranes and Portable Purge Units (PPUs).

(5) Satellites or oversize satellite equipment escorted off-center to the Astrotech or Spacehab facilities require three Security units. Two positioned in front of the escort and one at the rear. Flight hardware escorted to Astrotech or Spacehab that is not oversize or does not need to travel against traffic shall be escorted by only two Security units.

(6) Late access experiments for STS missions shall be escorted by the user or J-BOSC Security, if determined to be mission critical and time critical. Determination as to who shall escort the late access experiments and the number of Escort Units shall be made by J-BOSC Security, taking into consideration the time of day, amount of traffic, route taken, and threat assessment.

19.5 CRASH REPORTING PROCEDURE

a. Any crash occurring on KSC property which involves a vehicle (as defined in this KNPR) and property damage or injuries must be immediately reported to J-BOSC Security by the fastest means available, in accordance with Florida Statutes. The driver of a vehicle involved in a traffic crash shall make every effect to move the vehicle to the side of the road to avoid blocking traffic.

b. A traffic crash investigator shall conduct an investigation in accordance with Florida Statutes and submit a report as required by the State of Florida and/or The Protective Services & Safeguards Office.

c. J-BOSC Security shall maintain traffic crash and violation records in accordance with appropriate NASA and State directives.

19.6 KSC TRAFFIC CITATION POINT ASSESSMENT SYSTEM

a. Any person who is charged with a violation of NASA and/or Florida Traffic Regulations shall be assessed points against his/her driving record in accordance with State of Florida Department of Highway Safety and Motor Vehicle Guidelines. KSC Traffic Citations issued for

RELEASED - Printed documents may be obsolete; validate prior to use.

"Non-moving Violations" must have all the driver/owner information recorded by the driver/owner and signed by the driver's supervisor in the space provided on the reverse of the form, before it is returned to J-BOSC Security. Failure to complete and return the citation within 7 hours as specified in this KNPR shall constitute a separate violation, and an additional point shall be assessed against the owner's driving record.

b. Points shall be automatically assessed by the J-BOSC Projects & Integration Office upon completion of the processing procedure for KSC Traffic Citations.

c. Points assessed as a result of the issuance of a KSC Traffic Citation shall be removed from a person's driving record, if an appeal is upheld in accordance with paragraph 408.7 below.

d. Points shall be assessed as a result of the issuance of a Florida Uniform Traffic Citation only after receipt of documentation from the Clerk of the Court showing that the person was found guilty during Court proceedings. No point shall be assessed if the charges are dismissed, or if found not guilty by the Court.

19.7 TRAFFIC APPEALS

a. Appeals of KSC Traffic Citations shall be the responsibility of the J-BOSC Security, Traffic Management Office. Appeals shall be reviewed by the KSC Traffic Appeals Board which is comprised of the following persons and shall convene the first week of each month:

(1) CHAIRPERSON - A permanent position to be held by the J-BOSC Security Traffic Management Administrator.

(2) MEMBER - A 6-month position to be held by a Security Representative from another contractor at KSC. Appointment shall be made by The Protective Services & Safeguards Office.

(3) MEMBER - A 6-month position to be held by a KSC Civil Service employee outside the Security Field. Appointment shall be made by The Protective Services & Safeguards Office.

(4) RECORDER/ADVISOR - A permanent position to be held by a Representative from the Projects and Integration Office. The position shall not have a vote, but shall act as Technical Advisor to the Board.

RELEASED - Printed documents may be obsolete; validate prior to use.

b. The KSC Traffic Appeals Board shall adjudicate all appeals which are based upon the issuance of a KSC Traffic Citation. The decision of the Board shall be final.

c. Persons who wish to appeal a KSC Traffic Citation issued to them must, within 10 days of the citation issue date, initiate a letter of appeal.

d. The letter shall state the facts of the incident (as seen by the appellant) and the reasons why the appellant feels the assessed points should be stricken from the record. Maps, diagrams, and pictures may be included. The letter shall be forwarded to the KSC Traffic Appeals Board, J-BOSC Security. The KSC Traffic Appeals Board shall notify the appellant in writing of the action taken by the Appeals Board. The KSC Traffic Appeals Board shall not consider those KSC Traffic Citations which are not completed by the appellant as outlined by this KNPR. No personal appearances or video tapes are allowed.

19.8 ASSIGNMENT OF RESERVED PARKING SPACES

a. Criteria for the assignment of reserved parking spaces are as follows:

(1) Civil Service Personnel: Each employee in grade GS-15 or above, or each Division Chief, is authorized a reserved parking space for his/her privately owned vehicle in the vicinity of his/her primary assigned office. An individual shall only be authorized one reserved parking space.

(2) Contractor Personnel: Each contractor employee located at the KSC who is at the management level in the local company organization that is equivalent to civil service grade GS-15 or above, as determined by the NASA Contracting Officer, is authorized a reserved parking space for his/her privately owned vehicle in the vicinity of his/her primary assigned office. An individual shall only be authorized one reserved parking space.

(3) Handicapped Personnel: Each handicapped civil service and contractor employee who has the proper KSC or State handicapped hang tag is authorized to park in designated handicapped spaces. Temporary KSC handicapped parking permits shall be requested through the Occupational Health Facility (OHF).

RELEASED - Printed documents may be obsolete; validate prior to use.

(4) Government-Owned/Leased Vehicles: Reserved parking space is authorized for Government-owned/leased vehicles, including those assigned to an organization, subject to the approval of the NASA Site Manager of the facility where the reserved space is requested.

(5) Vanpool Vehicles: Each civil service and contractor employee operating an authorized vanpool can request a reserved parking space for the van in the vicinity of his/her primary assigned office.

b. Use and Identification of Reserved Parking Spaces.

(1) All reserved spaces shall be marked as identified below. The location of marking (i.e. pavement, bumper block, curb, etc.) shall be determined by the J-BOSC Security Traffic Management Office.

(2) Spaces reserved for Government vehicles shall be marked using a numbered parking permit system, or an alternate method of marking the space by identifying the specific vehicle or category of vehicle (e.g., Government vehicle, mail truck, etc.).

(3) Vehicles with visible markings which identify them as KSC contractor-owned/leased vehicles shall utilize spaces reserved for Government vehicles subject to the limitations imposed on Government vehicles in subparagraph (2) above.

19.9 ASSIGNMENT RESPONSIBILITIES FOR RESERVED PARKING

a. The J-BOSC, Security Traffic Management Office, or designee, is responsible for:

(1) Managing existing vehicle parking facilities on KSC.

(2) Approving requests for reserved parking.

(3) Assigning reserved spaces/zones to authorized employees and offices.

(4) Preparing (prior to the parking facility's beneficial occupancy date) and maintaining a plan showing utilization of all parking areas. The plan shall show the following:

RELEASED - Printed documents may be obsolete; validate prior to use.

(a) Visitor parking spaces.

(b) Spaces reserved for privately owned vehicles.

(c) Spaces reserved for Government vehicles.

(d) Loading zones.

(e) Spaces reserved for special-purpose vehicles.

(f) Parking spaces for the handicapped.

(5) Implementing the parking area utilization plan including traffic flow markings, reserved space markings, and erection of signs.

b. NASA Contracting Officers or their designated representatives are responsible for reviewing parking requests submitted by contractor personnel for reserved parking spaces for their privately owned vehicles (except those requests based on physical handicap) to determine whether the contractor employee meets the criteria established for a reserved parking space.

c. Heads of primary organizations to which Government-owned/leased vehicles are assigned are responsible for submitting a request to the J-BOSC Security Traffic Management Office for reserved parking space for assigned Government-owned/leased vehicles, and for assuring that their respective contractors submit requests as indicated. **NOTE:** This type request is normally limited to emergency or special-purpose vehicles.

d. The Director, Spaceport Services is responsible for reviewing requests submitted by handicapped personnel for a temporary KSC handicapped hang tag which authorizes parking in handicapped parking spaces. A determination shall be made whether the employee's physical condition justifies a hang tag and if so, the length of time assigned.

e. The Director, Spaceport Services is responsible for the approval of parking requests and the assignment of reserved parking spaces for the parking area located in front of the KSC Headquarters Building; and approval of Senior Management Permits and hang tags for reserved parking spaces. Both temporary and permanent Senior Management permits are processed by this office.

RELEASED - Printed documents may be obsolete; validate prior to use.

f. NASA Site Management Personnel are responsible for identifying and approving reserve parking spaces at their facilities.

19.10 PROCEDURES FOR REQUESTING RESERVED PARKING PERMIT/HANGTAG

a. Handicapped Personnel

(1) Requests for a temporary KSC handicapped hang tag by temporarily handicapped personnel shall be submitted on KSC Form 13-116 (Physical Examination Request/Report) to the OHF.

(2) The OHF shall verify the handicap and issue a handicapped hang tag which authorizes parking in handicapped parking spaces. Hangtag shall be issued for a period not to exceed one year.

(3) Handicapped personnel with State-issued parking permits are authorized to park in designated handicapped parking spaces. Application procedures listed above do not apply.

b. Civil Service Personnel - Privately Owned Vehicle (POV).

(1) Requests by authorized civil service personnel shall be submitted on KSC Form 8-18 (Request for Reserved Parking /Hang Tag Request Form), to the J-BOSC Security Traffic Management Office.

(2) The J-BOSC Security, Traffic Management Office shall process the request and notify the requester of status and/or assignment upon completion of processing.

c. Contractor Personnel - Privately Owned Vehicle (POV).

(1) Requests by authorized contractor personnel shall be submitted on KSC Form 8-18 (Request for Reserved Parking Hang Tag Request Form).

(2) Requester's NASA Contracting Officer or designated representative shall show approval by signing the form and forwarding it to J-BOSC Security Traffic Management Office.

RELEASED - Printed documents may be obsolete; validate prior to use.

(3) The Reserve Parking Coordinator, J-BOSC Security Traffic Management Office, shall process the request and notify the requester of status and/or assignment upon completion of processing.

d. Vanpools.

(1) Requests for reserved parking space for a vanpool van shall be submitted on KSC Form 8-18, KSC Form 8-18 (Request for Reserved Parking Hang Tag Request Form) and forwarded to J-BOSC Security, Traffic Management Office for processing.

(2) Upon the completion of processing, the Reserve Parking Coordinator, J-BOSC Security Traffic Management Office, shall process the request and notify the requester of status and/or assignment.

e. The requester shall notify J-BOSC Security, Traffic Management Office, in writing, when a parking space is no longer required (i.e., termination, retirement, transfer from KSC or within KSC). This shall allow J-BOSC Security to delete, reassign or move the reserved parking space.

f. Special Requirements.

(1) Requests for assignment of reserved or temporary parking space for the parking area located in the front of the KSC Headquarters Building should be submitted to the Deputy Director for Business Operations for approval. It shall then be forwarded to the J-BOSC Security, Traffic Management Office for processing.

(2) Requests for assignment of reserved or temporary parking space only for the parking area located inside the fence line of the LCC Building fence should be submitted to the NASA/Director, Process Integration for coordination and processing. Requester must meet the criteria for assignment of reserved parking as stated in paragraph 408.8.a.

(3) Requests for assignment of a reserved or temporary parking space for those spaces located next to the OPF Annex and on the Space Shuttle tow route in the vicinity of the OPF should be submitted to the OPF NASA Site Manager for review and approval. Personnel approved for a reserved (by permit) space do not necessarily meet the criteria stated in paragraph 408.8.a.

RELEASED - Printed documents may be obsolete; validate prior to use.

These spaces are controlled (reserved) for operational, safety, fire, and security purposes so that owners of POVs/GOVs are able to be identified and located quickly.

(4) Other requests not covered by paragraphs a. through e. above shall be submitted by the requester to the J-BOSC Security Traffic Management Office for coordination.

g. Specialized Parking Permits/Hang Tags

(1) Senior Management Permits/Hang Tags are authorized for Senior Management personnel to allow them to park in designated parking spaces at facilities other than their primary work location.

(a) Requests shall be submitted on KSC Form 8-18 (Request for Reserved Parking Hang Tag Request Form), outlining the individual's management position and primary work location to Spaceport Services for approval.

(b) Upon approval, Spaceport Services shall forward the request to J-BOSC Security Traffic Management Office, for issuance.

(c) These permits shall be renewed annually; however, when the need for the permit no longer exists, it shall be forwarded to the J-BOSC Security Traffic Management Office for disposition.

(2) Temporary Senior Management Permits shall be maintained and issued by the Director, Spaceport Services to those individuals who require a parking permit for a short duration.

(3) LCC Parking Permits are authorized for individuals who have a need for parking access to the inner perimeter of the LCC as determined by the Director, Process Integration.

(a) Requests for these permits shall be sent to the Director, Process Integration for approval and issuance.

(b) The expiration of these permits shall be at the discretion of the Director, Process Integration; however, when the need for this permit no longer exist, it shall then be

RELEASED - Printed documents may be obsolete; validate prior to use.

returned to the Process Integration Office, for proper disposition.

(4) Temporary LCC Parking Permits shall be maintained and issued by the Director, Process Integration, for those individuals requiring a parking permit for a short duration.

(5) OPF Parking permits (as described in 408.10.f.(3)) are authorized for individuals with a need for parking next to the OPF Annex or for those spaces near the OPF that are located on the Space Shuttle tow route.

(a) Requests for issuance of these permits shall be sent to the NASA OPF Site Manager for approval and issuance.

(b) The NASA OPF Site Manager shall maintain a current listing of assignments by name, function, telephone number, and space number.

(c) Upon approval, the NASA OPF Site Manager shall forward the request to J-BOSC Security Traffic Management Office, for issuance.

(d) Permits shall be returned to the J-BOSC Security, Traffic Management Office when the need no longer exists.

(6) Official Vehicle Hang Tags are authorized when private, leased, and/or rental vehicles are utilized as Government vehicles, provided that proper justification is submitted. This hang tag authorizes personnel to park their personal vehicle in a generic parking space marked “Government Vehicle”.

(a) Hang Tags shall be requested by submitting KSC Form 8-18, Reserve Parking/Hang Tag Request Form to J-BOSC Security, Traffic Management Office for processing.

(b) Upon approval, the J-BOSC Security Traffic Management Office, shall issue the permit to the requesting individual.

(c) Official vehicle hang tags are valid for one year. Upon expiration, justification must be resubmitted for renewal as outlined in paragraph a. above.

RELEASED - Printed documents may be obsolete; validate prior to use.

(d) When the need for this permit no longer exists, or at the time of expiration, it must be forwarded to J-BOSC Security Traffic Management Office for disposition.

(7) Service Vehicle Hang Tags are authorized when Government vehicles or private vehicles are utilized as Government Vehicles and used as mobile workshops.

(a) Service Vehicle Hang Tags shall be requested by submitting a KSC Form 8-18 (Reserve Parking/Hang Tag Request Form) to the J-BOSC Security Traffic Management Office.

(b) Upon approval, the J-BOSC Security Traffic Management Office shall issue a hang tag to the individual requester.

(c) Service Vehicle Hang Tags are valid for one year. Upon expiration, the hang tag must be returned to J-BOSC Security.

(8) Intentional misuse of any of the specialized parking hang tags may cause loss of privileges, confiscation, and disciplinary action.

19.11 TRAFFIC MANAGEMENT REVIEW BOARD

a. Purpose. The KSC Traffic Management Review Board (TMRB) shall review proposals, plans, design engineering and specifications, and/or suggestions to modify and expand KSC's roads, parking areas, and automated and manual traffic control devices. The TMRB shall also review contracts that could impact the movement of any vehicular traffic on KSC, or areas under KSC jurisdiction.

b. Policy. It is KSC policy to establish and maintain the necessary capabilities to ensure that the management of traffic and traffic impacting activities on KSC affords all personnel the optimum level of service. This shall be accomplished by the KSC Traffic Management Review Board which shall evaluate and/or adjudicate new or existing situations arising from changes, modifications, or any activity identified as having the potential to impact KSC's traffic, roads, parking areas, etc.

c. The TMRB shall consist of:

RELEASED - Printed documents may be obsolete; validate prior to use.

Chairperson:	Protective Services & Safeguards Office
Vice-chair:	NASA Safety
Members:	NASA Facilities Representative
	SFOC Safety Representative
	J-BOSC Traffic Management, Administrator
	J-BOSC Security Engineer (Signalization)
	J-BOSC Roads & Grounds Representative
	J-BOSC Security Operations Representative
	J-BOSC Secretariat/Recorder
Others:	Representative from organizations identifying the situation.
	Other KSC organizations as required.

The TMRB shall consist of designated NASA/KSC representatives from the organizations having TMRB responsibilities. The member's organizations shall be identified in writing and be authorized to speak for their organizations regarding TMRB activity. The TMRB is authorized to limit participation to only those individuals having a proprietary interest in the matter under discussion.

d. The TMRB shall:

(1) Convene when traffic management issues are identified.

(2) Review the issue/concern and provide requirements and/or recommendations for action/corrections.

(3) Resolve organizational interface problems.

(4) Provide recommendations for advanced planning on traffic management changes.

e. Traffic Management Issues:

RELEASED - Printed documents may be obsolete; validate prior to use.

(1) Traffic management issues shall be presented in writing to any Board member by any employee having a traffic-related concern.

(2) All design engineering involving traffic management issues shall be reviewed by the Board for impacts.

(3) Traffic Management issues include, but are not limited to, the following situations:

(a) New roadway or facility construction (Plans and Specifications).

(b) Site Plan Reviews.

(c) Intersection configuration changes.

(d) Employee suggestions (traffic related).

(e) Pedestrian or vehicle safety issues.

(f) Roadway operations and maintenance programs.

(g) WAP reviews.

CHAPTER 20. VIOLATIONS OF LAW INCIDENT REPORTING

20.1 GENERAL

a. The Office of the Inspector General investigates all crimes concerning fraud against the U.S. Government, waste of Government resources, and abuse of Government authority or privilege. To report crimes of fraud, waste, and abuse phone 31-867-4714 or 1-800-44-9183.

b. The contract investigators and contract Security Patrol, under the technical direction of The Protective Services & Safeguards Office, shall investigate criminal matters normally handled by local police to include trespass, theft, drugs, and assault. In emergencies, dial 911. In all other cases, phone 31-867-11. See also Chapter 401.

c. Because time is critical when reporting and investigating incidents, all organizations to which this chapter applies shall take steps to ensure the timely reporting of the incidents covered by this chapter.

(1) In cases where a physical examination of a particular item or site is likely during the course of an investigation, the item or

RELEASED - Printed documents may be obsolete; validate prior to use.

site shall be preserved exactly as found, provided that this does not jeopardize safety or disclose classified information.

(2) When an incident may gravely affect the national security or preservation of critical national resources, the Center Chief of Security or the NASA/KSC Investigator may, as long as safety is not jeopardized, initiate the following:

(a) Order that the scene of the incident be protected to assure the preservation of evidence.

(b) Freeze conditions and configurations.

(c) Impound material.

(d) Conduct interviews.

(e) Order persons who are knowledgeable of the incident or investigation not to discuss it except as directed by the Center Chief of Security or NASA/KSC Investigator.

20.2 BEHAVIOR OF CLEARED PERSONS

a. Organizations to which this chapter applies shall report to The Protective Services & Safeguards Office, any incident which indicates that a person who is cleared for access to classified information or unescorted access to controlled areas may not be trustworthy or reliable. The Protective Services & Safeguards Office shall make a preliminary assessment of the information and may suspend access pending the completion of a thorough investigation and resolution of the matter.

b. Examples of reportable behavior include:

(1) Financial irresponsibility.

(2) Criminal conduct.

(3) Sexual misconduct.

(4) Mental or emotional illness.

(5) Alcohol abuse.

(6) Drug abuse.

RELEASED - Printed documents may be obsolete; validate prior to use.

(7) Security violations.

(8) Subversive activity.

20.3 OTHER REPORTABLE INCIDENTS

The protection of critical Government resources and the ability to maintain a secure environment for classified information or material is dependent on the identification and reporting of incidents. The following list of incidents shall be reported to The Protective Services & Safeguards Office or contractor security in a timely manner.

a. Evidence or suspicion of penetration of a security area.

b. Failure or unauthorized manipulation of an access control system (e.g., Electronic Security System).

c. Equipment malfunctions of a suspicious or unusual nature.

d. Damage to critical hardware or unapproved configuration changes.

e. Unplanned equipment activity.

f. Circumvention of approved Secure Configuration Management change procedures.

g. Incidents/activities as described in Appendix A, "Miscellaneous Controlled Activities."

CHAPTER 21. TRANSPORTATION AND MATERIAL SECURITY

21.1 GENERAL

This chapter of this KDP specifies the minimum safeguards and security measures to be taken in the protection of NASA and contractor assets during their storage and movement. These minimum standards do not limit users from instituting more stringent controls since hands-on operators often are aware of problems which may not be obvious to outsiders.

21.2 TYPES OF CARGO/MATERIAL

RELEASED - Printed documents may be obsolete; validate prior to use.

a. All Government and contractor assets while being stored, transported, or while in use require some level of protection. Priorities are established in accordance with importance to the mission, value, and specific nature of any item. The following list depicts levels of priorities:

Priority	Cargo/Material Item
1	Operationally critical Space Shuttle flight hardware; Space Shuttle flight hardware designated for a mission undergoing processing (including payloads).
	Other Space Shuttle manned flight hardware/payloads.
	Expendable vehicle flight hardware/payloads. Sensitive/classified items. Hazardous cargo/material.
	High-value/pilferable items; medical supplies (drugs listed as controlled substances); cash/check-handling activities.
3	Other cargo or material items, or the transportation or storage assets used with or by these items.

b. Some items are classified/prioritized by others. These items, such as nuclear material or classified hardware, require safeguards specified by the originator of the item. When prioritizing and planning utilization of security assets for these items, ensure that all requirements of the other authority are satisfied.

c. The transportation and storage of hazardous matter require special security support. Those items identified as hazardous or potentially hazardous shall be given special attention. All parties involved in the transportation or storage of hazardous material (or in response to emergencies) must be fully cognizant of the nature of the hazard.

21.3 RESPONSIBILITIES

RELEASED - Printed documents may be obsolete; validate prior to use.

a. The Chief, Protective Services and Safeguards Office (PSSO) is responsible for overall management of the security efforts involved in transportation and material security.

b. The Lead, Spaceport Security Operations is responsible for:

(1) Establishing and ensuring the implementation of all security measures for activities/operations under the cognizance of KSC.

(2) Delegating certain security planning and implementing functions to other NASA and contractor elements. Chapter 401, "Law Enforcement," requires directors of first line directorates or offices and contractors to appoint "Security/Law Enforcement points of contact" (Appendix C).

(3) Providing procedural requirements and assistance to NASA organizations and contractor points of contact (POCs) in designing certain security plans for all items.

(4) Maintaining liaison with all NASA and contractor organization POCs, keeping them informed of all security measures in use and providing procedural requirements when necessary.

c. Heads of primary organizations are responsible for ensuring that NASA and contractor organizations appoint a security/law enforcement POC to be responsible for the security of facilities, operations, and assets under their responsibility; and in addition to the responsibilities listed in Chapter 401, shall, as a minimum:

(1) Ensure that Standard Operating Procedures (SOPs) are developed and implemented for the following:

(a) Documentation of orders, manifests, and requisitions detailing what has been ordered, how items are to be transported, and where delivery shall be made.

(b) Maintenance of accountability and recording of disposition of cargo.

(c) Receipt, storage, and maintenance of cargo.

(d) Identifying and reporting shortages.

RELEASED - Printed documents may be obsolete; validate prior to use.

(e) Scheduled and nonscheduled audits of all transportation and supply accountability records.

(f) Training or arranging for training of personnel in loss prevention.

(g) Receipt for shipment of arms, munitions, pyrotechnics, ordnance, or other sensitive items.

(h) Security of items in shipment and storage.

(2) Ensure that vehicles, containers, shipping bins, etc., are properly marked (origin and destination), sealed, and locked where appropriate.

(3) Ensure that proper physical security measures are in place at receipt, shipping, and storage areas.

(4) Ensure the security of sensitive information concerning shipments.

(5) Coordinate with The Protective Services & Safeguards Office and J-BOSC Security for support when required.

d. J-BOSC Security shall:

(1) Provide assistance to the NASA PSSO and other organizations in fulfilling their storage and transportation security responsibilities.

(2) Provide uniformed, armed, security officers and security escorts when required.

(a) The storage and/or transportation of sensitive or classified items may require an armed security escort. The officers and supporting equipment for the security protection shall be supplied by J-BOSC Security at the direction of NASA PSSO. As requirements vary with each situation, specific plans shall be developed by the coordinated efforts of NASA PSSO and J-BOSC Security.

(b) Certain unusual or oversized items shall require traffic escorts from marked security vehicles in order to travel safely on the roadways. These shall be provided by J-

RELEASED - Printed documents may be obsolete; validate prior to use.

BOSC Security within the provisions of the following regulatory documents:

1. 45th Space Wing #15E-3-50, Joint Operating Procedure Between ESMC and KSC for Responsibilities and Interfaces for Scheduling, Transportation, and Convoying of Oversized Loads Between CCAFS and KSC.

2. KMI 600.1, "Movement of Overweight/Over dimensional Loads at KSC."

21.4 MINIMUM STANDARDS

a. Accountability for and protection of items in storage or in transit, in addition to those listed below, shall be maintained in accordance with procedures established by each cognizant NASA or contractor organization and approved by NASA PSSO. These procedures shall comply with NASA regulatory documents, the provisions of this KNPR, and any special accountability requirements levied for special controlled items, such as nuclear material. As a minimum, the following shall be complied with to prevent pilferage, theft, damage, destruction, or loss:

(1) Packing for Shipment.

(a) Physical Construction of Containers. Shipping containers must be strong enough to protect the load from damage and to hold together without breaking open under stress or rough handling. They must be constructed to show signs of any attempted forced entry.

(b) Physical Size of Containers. Small packages, which could be easily concealed, shall be packed in larger, master cartons.

(c) Sealing of Containers. Containers shall be securely sealed with tape, glue, and/or staples, and/or metal/steel straps and seals. Tape shall be at least 3 inches wide. Tape shall not be used if it can be lifted without creating noticeable damage. Tape shall be distinctively marked to permit quick detection of tampering. Appropriate warnings, similar to "IF TAPE IS BROKEN, DO NOT

RELEASED - Printed documents may be obsolete; validate prior to use.

GIVE RECEIPT WITHOUT EXAMINATION" shall be placed on containers.

(d) Package Markings. Consistent with current Department of Transportation rules, packages shall not be marked with the contents of the item being shipped. No indications as to the item or value shall appear on the outside of the shipping container. Packages shall be properly marked with any special handling requirements, such as "FRAGILE."

(e) Origin/Destination Markings. Packages shall be marked with the name and address of the consignee and the shipper's telephone number and name. All old or confusing handling and cautionary marks and symbols shall be removed or obliterated on reusable containers.

(f) Palletizing/Unitizing. Items which are susceptible to pilferage shall be palletized or unitized whenever possible. Boxes shall be stacked neatly and tightly. Supporting strapping, netting, or shrink-wrap plastic shall be utilized.

(g) Carriers. The loading and unloading of items to or from carrier trucks shall be observed. The bill of lading shall be checked for accuracy and completeness. A NASA/KSC provided seal shall be used for sealing containers.

(h) Sensitive Information. Only those persons who need to know shall have access to information concerning shipments, schedules, routes, and destinations of cargo.

(i) Documentation Checks. Procedures to double-check documentation for errors shall be developed.

(j) Two-Person Rule. Two workers shall always be employed for packaging sensitive or easily pilfered items.

(2) Receiving Procedures. Persons receiving shipments shall, as a minimum, accomplish the following:

(a) When receiving items, ensure that a bill of lading is properly completed with full addresses of shipper and consignee.

RELEASED - Printed documents may be obsolete; validate prior to use.

(b) Inspect cargo for proper address and markings. Remove or obliterate old or confusing markings.

(c) Inspect cargo for damage, abnormally light cartons, cartons which appear to have been repaired/rebuilt, etc., and note any discrepancies on the bill of lading.

(d) Count the number of pieces and ensure that the number agrees with the number called for on the bill of lading.

(e) Have the carrier sign the bill of lading with full last name and initial any notations of exception.

(f) Record the company name or carrier abbreviation, record and circle the number of pieces received, and sign and record the date on all copies of the bill of lading.

(g) Conduct spot checks on the loading docks. Monitor unloading procedures. Randomly select crews to unload cargo. Do not use the same crew to unload the same carrier time after time. Rotate supervisors on the docks. Do not let crew have their lunch or breaks in the unloading areas. Always have at least two persons on each crew.

(h) The driver of inbound loads should not be allowed in the unloading area. Inbound vehicles shall not park at the unloading area until ready to unload.

(i) Inspect all seals.

(j) Close and lock any partially loaded trucks at the close of business. Do not use a carrier-supplied lock.

(k) Inspect the interior of the truck before loading or unloading.

(l) Make periodic inspections of trash bins in the loading/unloading areas for concealed items.

(3) <u>Seals.</u>

RELEASED - Printed documents may be obsolete; validate prior to use.

(a) Use of Seals. Seals are not locks. Seals are intended to discourage theft, maintain accountability, and indicate tampering. Do not rely on a seal if a lock is needed.

(b) Storage of Seals. Un-issued seals shall be secured in a locked storage area, accessible only to designated supervisors and accounted for.

(c) Application of Seals. After verifying the contents of the containers, seals shall be applied by supervisory personnel.

(d) Recording of Seals. A log of all seals applied to loads or removed from inbound loads shall be maintained. This log shall show, as a minimum:

1. Seal number.

2. Date applied.

3. Unit applied to.

4. Person applying seal.

5. Load destination/origin.

(e) Discrepancies. If a seal is found to be broken, tampered with, or switched, a report shall be made by the discovering office and forwarded to the contractor and NASA PSSO within three business days. All details of the discrepancy, including the date and time discovered, location discovered, and person finding the problem, shall be included in this report.

(f) Seal Removal. Seals on inbound shipments shall be checked by a supervisor before removal.

(g) Legal Considerations. Title 18, U.S. Code, Section 117, states: "Whoever breaks the seal or lock of any railway car, vessel, aircraft, motor truck, wagon or other vehicle . . . containing interstate or foreign shipments of freight or express, or other property, or enters any such vehicle with intent in either case to commit larceny therein, shall be fined not more than $5,000, or imprisoned not more than 10 years, or both . . . ."

RELEASED - Printed documents may be obsolete; validate prior to use.

b. Physical Security Measures for Storage Areas/Structures. All standards for physical security as established in this KDP apply to facilities involved in the shipment and storage of Government cargo and material. Buildings and rooms used for the storage of Government property on the Kennedy Space Center and at off-Center KSC facilities worldwide must meet the following standards:

(1) Doors provide a degree of security comparable to that provided by the walls of the basic structure.

(2) Door hinge mounting screws are not exposed to the exterior of the facility. If screws are exposed, they shall be spot welded, peened, covered, or filled with material in a way so as to prevent easy removal. Nails shall not be used to mount hinges.

(3) Door hinge pins exposed to the exterior of the facility are designed or modified to prevent easy removal. If these hinge pins cannot be so modified, safety stud hinge pins shall be used.

(4) Doors to the exterior locked from the inside are secured with a deadbolt locking device, crossbar, or similar locking device resistant to jimmying and manipulation from the outside as opposed to a latch-style door lock.

(5) Windows have individual locking devices, and protected as described in paragraph b.6 below.

(6) All first-floor openings, except doors, in excess of 96 square inches (619.4 square centimeters) that are located less than 1 feet (3.7 meters) from the ground level shall be barred, grilled, or covered with chain link material in a way to preclude easy removal. Long, narrow openings with the shortest dimension measuring less than 6 inches (15. centimeters) are exempt from this requirement.

(7) Doors secured from the outside shall have locking devices conforming to the requirements of this KNPR and shall be part of the KSC lock system. In-door locks and pin-tumbler-type, key- operated padlocks and hasps shall be of a size and strength to provide proper security. Hasps shall not be mounted with nails.

RELEASED - Printed documents may be obsolete; validate prior to use.

(8) Walls, floors, and ceilings shall be constructed of at least 1/-inch plywood, 1-inch tongue-in-groove wall boards, or equivalent.

c. Personnel Security.

(1) The two-person rule applies to all loading/unloading operations and to the handling of sensitive cargo.

(2) Persons handling or having access to classified, sensitive, or otherwise secured items shall be cleared by appropriate authority prior to having access to these items.

(3) Knowledge of details concerning security planning, schedules, etc., shall be available only on a need-to-know basis.

d. Procedural Measures. Utilizing the requirements of this KDP and other NASA and Government documents, each organization involved in the transportation and storage of assets and each facility handling cargo, shall develop procedures to maintain accountability and to facilitate accurate auditing of all aspects of cargo processing.

e. Overseas Shipping and Receiving Areas. Special security plans for KSC controlled areas outside the continental U.S. shall be developed following detailed site surveys for each area by NASA PSSO and/or by the J-BOSC.

f. During Shipment.

(1) Route Selection. Route selection shall normally be made to accommodate safe, cost-effective transportation of a given item. If a specific threat against an item is known, then the route shall be selected to maximize the available protection and to diminish the adversaries' possible access.

(2) Alarm Devices. When appropriate, electronic surveillance of articles in shipment shall be made. The manner or devices utilized and the application of it shall depend upon the specific cargo, the carrier, and any known threat. NASA PSSO shall be notified whenever electronic surveillance or other alarm devices are utilized on shipments.

(3) Use of Seals. See paragraph 410.4.a.(3) above.

(4) Use of Escorts.

RELEASED - Printed documents may be obsolete; validate prior to use.

(a) Shipper Escorts. Use of carrier-supplied security escorts for NASA/KSC shipments shall be made only at the direction of, or with the approval of, NASA PSSO. All procedures and specifications for the operation of the carrier-supplied escorts shall be approved by NASA PSSO.

(b) J-BOSC Patrol Officers. J-BOSC Patrol Officers shall provide escort for Government property on KSC within the provisions of the J-BOSC contract and as specified in this KNPR. Their escort of items outside the confines of KSC shall be made only upon the direction of NASA PSSO.

(c) Legal Considerations. Escort procedures shall consider the legal considerations present in a specific transportation operation. Some of these are jurisdiction, Department of Transportation regulations, and use of force limitations.

(d) Instructions for Guards/Escorts. Instructions for guards for shipments made under NASA cognizance shall be developed by the J-BOSC and approved by NASA PSSO.

g. Transit/Temporary Holding Areas.

(1) On KSC. The transit/holding areas on KSC are governed by the provisions of this KDP and other NASA and Government publications.

(2) Off KSC. Security during temporary stops off KSC is the responsibility of the consignee for normal, noncritical/sensitive items. For critical/sensitive items for which KSC has assumed security responsibility while the items are in transit off the Center, contingency plans shall be developed by the Protective Services & Safeguards Office for temporary holding areas while the shipment is in transit. In these cases when KSC retains security responsibility, the NASA PSSO developed shipment security plan shall include provisions for, as a minimum:

(a) Primary and alternate routes of travel.

RELEASED - Printed documents may be obsolete; validate prior to use.

(b) Possible holding areas in route.

(c) Contacts within each community (country, state, county, and municipality) law enforcement authorities who would be notified, should the shipment be temporarily held within their area.

(d) Local area threat situation.

h. Temporary Removal of Government Property From KSC. All handling and removal of government property from KSC shall be in accordance with the provisions of KNPR 4000.1. As a minimum, NASA Form 89, "Property Pass Request and Removal Permit," or other appropriate documentation, shall be utilized.

i. Lost and Found. J-BOSC Security shall maintain a lost and found service in accordance with appropriate Government regulations and as directed by The Protective Services & Safeguards Office.

21.5 NON-OFFICIAL DELIVERIES

Non-official deliveries (i.e., food, flowers, greetings, etc.) are not permitted on KSC. Only those delivery service organizations recognized by NASA as requiring official access to the restricted area in support of the Space Center, are permitted on the Center.

CHAPTER 22. REGISTERED KEY AND LOCK SYSTEM (RKLS) LOCKSMITH SERVICES

22.1 PURPOSE

This chapter explains the responsibilities and services, and establishes requirements for obtaining and controlling registered locks, padlocks, and keys. It covers KSC's implementation of the KSC Key Accountability System (KKAS), the Registered Lock and Key System control procedures, Key Custodian responsibilities training, and supplemental locksmith services.

22. RESPONSIBILITIES

a. The Lead, NASA Security Operations is responsible for appointing a KSC Key Control Officer.

b. The Key Control Officer is responsible for:

(1) Representing the Protective Services & Safeguards Office in all matters regarding Registered Key Control.

RELEASED - Printed documents may be obsolete; validate prior to use.

(2) Identifying training requirements and concurring in training programs established to support the KCCs and alternates.

(3) Evaluating lost key incidents and reviewing investigations involving the Registered Key Control System.

(4) Coordinating security requirements for changes, modifications, additions, and deletions of lock requirements that are outside the responsibility of the organizational KCC.

(5) Directing actions to be taken after the review of incident reports/investigations.

c. Heads of primary organizations are responsible for:

(1) Ensuring compliance with the provisions of this chapter.

(2) Appointing, in writing, primary and (as determined) alternate Key Control Custodians (KCCs) and providing them with the authority to approve and/or disapprove key and lock requests.

d. KCCs (Primary) are responsible for:

(1) Reviewing and approving all key/lock requests.

(2) Forwarding requests to the J-BOSC Locksmith Office.

(3) Turning in all keys and locks to the J-BOSC Locksmith Office when no longer required.

(4) Reporting all lost or misplaced keys and locks to the appropriate organizational security office.

(5) Acting as the central point-of-contact for the organization/facility with the J-BOSC Locksmith Office.

(6) Assisting in surveys and audits of the Registered Key Control System under their cognizance.

(7) Being cognizant of all key and lock activities in their area of control.

e. KCCs (Alternates) are responsible for:

RELEASED - Printed documents may be obsolete; validate prior to use.

(1) Assisting the requester in filling out key and lock requests.

(2) Forwarding properly completed requests to the primary KCC.

(3) Turning in keys and locks to the Primary KCC.

(4) Reporting lost keys and locks to the Primary KCC.

(5) Assisting in surveys and audits of the Registered Key Control System under their control.

(6) Interfacing with the J-BOSC Locksmith in the absence of the Primary KCC.

f. The Director, Procurement Office is responsible for incorporating this chapter into applicable contracts.

22.3 GENERAL

a. It is a KSC policy to protect Government property in the most practical and economic manner. Unless specifically exempted by the Installation Security Officer, all lockable facilities/areas containing Government or other high value property shall be equipped with approved locks. These facilities/areas shall be locked during any period that they are unoccupied.

b. The "KSC Registered Lock and Key System" is a master key system utilizing registered locks and padlocks with removable and interchangeable cores. Each lock or padlock core is stamped to include the series to which it is assigned. The location is maintained by the J-BOSC Locksmith Office.

c. A "KSC Registered Key" is a key marked "U.S. Government, Do Not Duplicate." It is stamped to indicate the lock series and key number.

d. The "KSC Key Accountability System" (KKAS) is an automated data processing (ADP) program, maintained by the J-BOSC Locksmith Office, and is designed to maintain control and accountability of the KSC Registered Key and Lock System.

e. The J-BOSC Locksmith Office shall:

(1) Service and repair vaults, safes, door locks, and padlocks with three-position combination locks.

RELEASED - Printed documents may be obsolete; validate prior to use.

(2) Provide "BEST" Lock Company seven-pin padlock cores, cylindrical locksets, mortise locksets, rim locksets, and tubular locks.

(3) Cut keys and replacements (vehicle, desk, file, storage, cabinet, control panel, etc.).

(4) Combinate and recombinate lock cores.

(5) Activate and deactivate storage containers and assist in changing safe combinations.

(6) Provide preventive maintenance and real-time response to the aforementioned hardware.

(7) Maintain the automated KKAS.

(8) Support audits and surveys of KCCs, holders of keys/locks, and the KKAS, as required.

(9) Maintain a listing of certified/trained KCCs.

22.4 KEY CONTROL CUSTODIANS (KCC) AND ALTERNATES

a. The KCC, also commonly known as a Key Coordinator, is the central point-of-contact within the organization or facility, who shall authenticate the need for key or lock service (change, addition, deletion, etc.). The Primary KCC (PKCC) serves as the official point-of-contact with the J-BOSC Locksmith Office. Alternates (assistants) are designated based upon organizational needs. The alternates shall interface with the PKCC, who shall be cognizant of the organizational needs. Only in the absence of the PKCC, shall the KCC contact the Locksmith Office.

b. Assignment of KCCs and alternates shall be in writing from the cognizant contractor or KSC directorate (head of organization). At a minimum, the KCC and alternates shall be Personnel Reliability Program (PRP) certified when controlling access to facilities/assets requiring personnel to be PRP certified. Written notification shall be provided to The Protective Services & Safeguards Office which shall, in turn, provide the J-BOSC Locksmith Office with the notification. Notification shall include:

RELEASED - Printed documents may be obsolete; validate prior to use.

(1) Full name.

(2) Primary or alternate custodian.

(3) Office symbol/building/room number.

(4) Phone number/alternate.

(5) Areas of responsibility.

(6) PRP areas controlled.

(7) PRP approved/pending date.

22.5 KEY AND LOCK ACCOUNTABILITY/CONTROL

a. Key and Lock Issue.

(1) Requests for issue of registered locks, padlocks, or keys must be presented on KSC Form 0-36, "Locksmith Services Request," to the organizational/facility KCC/Alternate.

Note: These keys are Government property; and therefore, each individual must sign the 0-36 noting issuance. These keys shall not be loaned, transferred, thrown away, or given away. When no longer required, the proper procedure for turning in a key is detailed in paragraph b. below.

(2) Upon verifying that the request is authentic, and if approved, the KCC signs the Form 0-36 and forwards it to the J-BOSC Locksmith Office for processing.

(3) After processing the request, the Locksmith Office notifies the individual who shall accept receipt for the key that is ready for pickup. At the time the individual picks up the key, KKAS is updated reflecting the assignment of that key. Primary/Alternate KCCs shall not receipt or pick up keys that shall be assigned to other individuals. Deviation from these requirements must be approved by the KSC Key Control Officer.

b. Key and Lock Turn-in.

(1) All registered keys and padlocks no longer required shall be returned to the J-BOSC Locksmith Office through the organizational/facility KCC.

RELEASED - Printed documents may be obsolete; validate prior to use.

(2) All registered key or locks must be surrendered to the KCC upon termination or transfer of the individual key holder.

(3) All turn-ins are required to be transferred to the J-BOSC Locksmith Office within 5 working days.

(4) The J-BOSC Locksmith and KCC shall maintain a permanent record of turn-ins for a period of 3 years.

c. Lost and/or Misplaced Keys or Locks. The unauthorized tampering with, removal or damaging of a KSC registered lock or padlock, and/or the tampering with, loss, or duplication of a registered key shall be investigated and referred to the proper authority for administrative or disciplinary action.

(1) Loss of registered keys, locks, etc., shall be verbally reported to the KCC immediately, but not later than the first duty hour of the day, if the loss occurred during nonduty hours. In all cases, after the verbal report, a written report of the lost key incident shall be provided to the KCC.

(2) The KCC shall ensure that KSC Form 0-174 (reporting a lost registered key) is completed on all lost keys and shall provide the organizational security office with full details concerning the loss. The KSC Form 0-174 shall be provided to the security office along with a request for an inquiry or investigation into the loss.

(3) The organizational security element shall investigate each lost key report and forward the results to the KSC Key Control Officer for review. In addition to determining pertinent facts surrounding the loss, the inquiry must determine the estimated value of equipment, property, and valuables being protected by the lock/key series involved. The organizational security office must then make a recommendation to the KSC KCO concerning whether or not a recore is warranted.

(4) When the loss of keys issued under a particular series exceeds 10 percent of the number issued, a key/lock change or recore shall be directed. Key and lock changes shall be directed at any time if investigation determines the need.

22.6 KSC LOCKSMITH SERVICES

RELEASED - Printed documents may be obsolete; validate prior to use.

a. Requesting Routine Access. Neither the KSC Patrol nor the J-BOSC Locksmith routinely unlocks areas/rooms because someone has forgotten their key. Individuals requiring access must first contact the area occupants or the KCC. Those names, if not known, are available from the J-BOSC Locksmith Office, by providing the lock series number that is stamped on the core.

b. Emergency Access.

(1) Master keys for registered locks are maintained by the KSC Patrol for use when an emergency condition exists. The Joint Communications Control Center, through whom the request shall be made, can be contacted at 867-11.

(2) Master keys for registered locks in KSC facilities located on Cape Canaveral Air Force Station (CCAFS) are maintained by J-BOSC JCCC and are for use only during an emergency. The JCCC can be contacted at 853-11.

c. Routine and Emergency Locksmith Shop Service. The J-BOSC Locksmith Office is available for routine telephone and walk-in service, Monday through Friday. Emergency support shall be given appropriate response and attention, as required by circumstance.

22.7 KEY SECURITY/CONTROL

Master keys constitute the greatest vulnerability to the KSC Registered Key Control Program. The loss of any one jeopardizes the total system. Therefore, the following restrictions are placed on master keys:

a. Master keys shall be limited to minimum numbers.

b. Master keys are subject to audit/inventory at any time.

c. Master keys shall not be issued for convenience. All requests for master keys (except sub-masters) shall require KSC Key Control Officer's approval.

22.8 AUDITS/ACCOUNTABILITY

All Registered Key Control accounts are subject to audit periodically or as an independent action directed by the Key Control Officer. Audits may take place as an adjunct to other scheduled security inspections or as a stand-alone audit.

RELEASED - Printed documents may be obsolete; validate prior to use.

22.9 KSC KEY ACCOUNTABILITY SYSTEM (KKAS)

a. The KKAS is an automated data processing system which shall be operated by the J-BOSC Locksmith Office. It shall contain all key assignments for NASA/KSC and those NASA facilities at other locations such as CCAFS and PAFB. Personnel data and individual's facility access (by key) information shall be contained in the database. Access to this information shall be strictly controlled to those having a need-to-know. Although not classified, the intelligence value of the information, if compromised, could cause a potential impact to the safety and security of KSC personnel and resources.

b. Access to the database shall be limited to:

(1) J-BOSC Locksmith Office personnel.

(2) KSC Key Control Officer or the designated representative.

(3) Those individuals identified in writing by the Key Control Officer who have an official need for access.

c. Requests for information from the database shall be limited to:

(1) J-BOSC Locksmith Office personnel.

(2) Protective Services & Safeguards Office personnel.

(3) KCCs.

(4) Security personnel conducting inquiries or investigations, or responding to emergencies where such information is required.

(5) Those individuals identified in writing by the Key Control Officer who have an official need for the requested information.

22.10 TRAINING

a. Locksmith Certification: Each Locksmith employed by the J-BOSC Locksmith Office shall participate in a formal training program designed to maintain his/her proficiency. This training program shall include keeping pace with "state-of-the-art" lock/key hardware and maintaining proficiency in both installation and by-pass techniques. The training must also include all phases of classified container service, drilling and

RELEASED - Printed documents may be obsolete; validate prior to use.

by-pass techniques. This training shall be on-going and shall be recertified to the KSC Key Control Officer every 3 years.

b. KCC Training: Each Primary/Alternate KCC, upon assignment, shall receive certification training as conducted by the J-BOSC. Training shall include, but not be limited to, the following:

(1) KCC authority/responsibility.

(2) Documentation (requests, trouble calls, etc.).

(3) KKAS operation.

(4) Investigations.

(5) Audits.

(6) Criteria for issue/turn-in.

(7) Lost/misplaced locks/keys.

(8) Protective Services & Safeguards Office responsibilities.

(9) Organizational responsibilities.

(10) Locksmith support.

22.11 KEY AUDIT AGENT

A Key Audit Agent shall be appointed, in writing, by the Joint-Base Operations Support Contractor, Resource Protection Branch Manager. The appointed person shall be responsible to the KSC Key Control Office for the operation and general function of the KSC Lock and Key System. Specific functions shall include, but not be limited to, the following:

a. Determining location and accountability procedures of all locks and keys given a facility or key account.

b. Determining the status of all keys currently in use.

c. Ensuring that all key storage containers are used properly, in accordance with all directives and instructions.

d. Inspection of key retention devices and key rings and key tags for serviceability.

RELEASED - Printed documents may be obsolete; validate prior to use.

e. Publishing a quarterly KEY NEWS bulletin for Key Custodian distribution.

f. Conduct quarterly Key Custodian certification classes.

g. Work closely with the Locksmith Services Office in developing lock and key procedures for KSC.

h. Covering all other assignments relating to key control as designated by the KSC Key Control Officer.

CHAPTER 23. CONTROL OF WEAPONS

23.1 GENERAL

This chapter establishes control over the introduction and possession of weapons on KSC. It also prescribes the qualifications necessary before any individual is authorized to possess/use a weapon (firearm) on KSC or areas under KSC jurisdiction.

23.2 APPLICABILITY

This chapter applies to all individuals possessing or introducing weapons on the KSC, except Law Enforcement Officers (city, county, state, or federal, departments or agencies); military members in the performance of their duties, Cape Canaveral Air Force Station contract guard force in the performance of their duties, and individuals, groups, or representatives of agencies specifically authorized by the Center Chief of Security.

23.3 POLICY

The introduction and possession of weapons on KSC is prohibited.

23.4 DEFINITIONS

a. Weapons:

(1) Authorized: Government issued firearms and ammunition, as approved by the Center Chief of Security.

(2) Unauthorized: Items listed in paragraph 41.9 and any privately owned firearms, with the exception of those firearms granted a waiver in accordance with paragraph 41.8.

RELEASED - Printed documents may be obsolete; validate prior to use.

b. Concealed Firearms: A firearm carried in such a manner as to preclude knowledge of its presence by direct observation. Concealed weapons are usually covered by a coat or jacket at all times.

c. Unconcealed Firearms: A firearm carried in such a manner that knowledge of its presence can be obtained by casual or direct observation.

23.5 AUTHORITY TO CARRY FIREARMS

The authority to carry firearms is granted under the National Aeronautics and Space Act of 1958, (4 U.S. Code 456).

23.6 RESPONSIBILITIES

a. The Center Chief of Security (CCS) is responsible for the control of weapons on KSC. Specific responsibilities are:

(1) Providing procedural requirements to the KSC Protective Services & Safeguards Office for the proper enforcement of this directive.

(2) Appointing a NASA KSC Firearms Custodian (government employee) and one or more Firearms Instructors.

(3) Approving the appointment of the J-BOSC Firearms Instructor/Range master.

(4) Ensuring that all KSC personnel that have been identified to carry weapons in the performance of their duties receive and pass an approved course of training.

(5) Ensuring that all KSC Protective Services (J-BOSC) personnel that have been identified to carry weapons in the performance of their duties receive and pass an approved course of training.

(6) Issuing NASA Forms 699a, “Certification to Carry Concealed Weapons;” or NASA Form 699b, "Certification to Carry Unconcealed Weapons," to individuals that have been certified by the Firearms Instructor/Range master.

(7) Identify the prescribed course of fire that shall be used for firearms qualification and the intervals when that training shall take place.

RELEASED - Printed documents may be obsolete; validate prior to use.

(8) Ensuring a training program for all security force personnel assigned to NASA STS recovery operations, to include firearms requirements in foreign countries, is available.

b. The Procurement Officer is responsible for ensuring that any contract entered into, wherein the requirement for the use of weapons exists, shall contain a statement of work which includes the requirements established by this Issuance.

c. NASA KSC Employees and Employees of NASA Contractors shall comply with the provisions, conditions, and limitations, of this chapter regarding the carrying, use, and storage of weapons.

d. KSC Security Personnel authorized to carry firearms on KSC shall:

(1) Qualify on a recognized course of fire prescribed by the Center Chief of Security.

(2) Have in their immediate possession NASA Form 699a or 699b when carrying firearms.

(3) Only possess firearms on KSC while on actual hours of duty.

(4) Be knowledgeable of the USE OF DEADLY FORCE and deadly force criteria."

(5) Never have been convicted of a misdemeanor charge of Domestic Violence.

e. The Firearms Instructor/Range master (NASA KSC government employee or contractor employee) shall:

(1) Train personnel in the safe handling of firearms.

(2) Supervise firing and range operations.

(3) Supervise all firing for qualification.

(4) Prepare written certification for each employee successfully completing the required training, and qualification, with their assigned weapon(s).

(5) Maintain the training and firearms qualification historical records on applicable personnel.

RELEASED - Printed documents may be obsolete; validate prior to use.

(6) Forward firearm certifications to the Center Chief of Security.

(7) Remain proficient, while assigned to the position of Firearms Instructor/Range master, by obtaining continuing professional education in the firearms/weapons discipline.

(8) Be certified as a Weapons Armorer, for all assigned Government weapons.

f. The Firearms Custodian shall:

(1) Keep current records on all firearms in the custody of NASA/KSC and/or NASA/KSC Contractors. These records include the date and method of acquisition and complete identifying data (manufacturer, caliber, model, serial number, etc.).

(2) Provide storage for all firearms and ammunition in containers meeting NASA requirements for confidential material at a minimum.

(3) Ensure all weapons are unloaded prior to storage.

NOTE: Weapons shall never be stored in the same receptacle as money, drugs, or classified material.

(4) Maintain a receipting system for the issue, transfer, and return, of firearms to the custodian.

23.7 CONTROL, ISSUANCE, AND CARRYING OF FIREARMS BY KSC SECURITY PERSONNEL

a. Protective force equipment shall enhance the ability of KSC's security personnel to effectively, efficiently, and safely perform routine duties, and to prevent adversaries from accomplishing their objectives. Duty weapons are:

(1) Primary Weapon: The 9-mm or .40 caliber Glock semiautomatic pistol.

(2) Secondary Weapon: A 9-mm submachine gun, 1-gauge shotgun, or a HK-33 rifle is available and shall be issued based on the type of duty and level of protection to be afforded.

RELEASED - Printed documents may be obsolete; validate prior to use.

b. Procedures for issuance, transfer, and return of weapons and ammunition to the Firearms Custodian shall incorporate reasonable and prudent safety standards for the protection of all personnel.

Only weapons and ammunition approved for use on KSC shall be used in the performance of official duties.

c. NPD 1600.2, "NASA Security Policy," provides the direction and authorization to the Center Chief of Security and designated security personnel of that office, and to employees of NASA contractors and subcontractors engaged in the protection of property owned by the United States or contracted to the United States, to carry firearms while in the conduct of their official duty.

d. KSC Security Personnel are required to successfully complete a designated course of fire. The course of fire is derived from federal and state requirements, (security personnel on KSC, depending upon their law enforcement/security status, are required to meet different firearms qualifications). A custom tailored course of fire is developed by the Range master to accommodate all mandatory firearms requirements and is subsequently approved by the Center Chief of Security. These courses of fire are reviewed on an annual basis to ensure any changes in requirements are reflected in the qualifications.

23.8 POSSESSION OF WEAPONS BY KSC EMPLOYEES AND REQUESTS FOR WAIVERS

Possession of unauthorized weapons by KSC employees is prohibited. There is no longer a waiver process for possessing personal firearms on KSC.

23.9 PROHIBITED WEAPONS AND ITEMS

a. All KSC employees are prohibited from possessing or introducing unauthorized weapons onto KSC property.

b. KSC employees observing violations of the weapons (firearms) policy, or becoming aware of the presence of unauthorized and/or prohibited weapons, on KSC, should notify the Joint Communications Control Center (JCCC), at 867-11.

c. J-BOSC Security Forces (contractor) and Protective Services & Safeguards Office credentialed Agents shall take the necessary action

RELEASED - Printed documents may be obsolete; validate prior to use.

to bar, intercept, remove, neutralize, confiscate, or otherwise eliminate unauthorized weapons from KSC.

(1) Weapons or ammunition found in vehicles during spot checks inside the perimeter of KSC or found in parked vehicles, shall be confiscated. The owners shall be advised that privately owned weapons and ammunition are not permitted on KSC and may be picked up upon exiting. A property receipt shall be filled out on all confiscations. All weapons shall be held at Patrol Headquarters (K6-496) until returned to the owner.

(2) If an individual voluntarily surrenders a weapon while attempting to enter KSC, he or she shall be denied access until the following steps can be completed:

(a) The weapon shall be taken, and safed, by a Security Supervisor.

(b) A property receipt shall be issued to the owner.

(c) The weapon shall be transported to the Equipment Room at Patrol Headquarters.

(d) The property receipt shall be destroyed once the weapon is returned to the owner.

d. The following items are prohibited on KSC:

(1) Personal firearms.

(2) Personal ammunition.

(3) Air rifles or pistols.

(4) Switch blade knives.

(5) Throwing knives.

(6) Black jacks or saps.

(7) Metal knuckles.

(8) Martial arts offensive or defensive weapons.

(9) Incendiary or pyrotechnic devices.

RELEASED - Printed documents may be obsolete; validate prior to use.

(10) Explosives (including fireworks).

(11) Any device/item known, or intended, to inflict injury or death or cause property damage, or any device/item specifically prohibited by city, county, state, or federal, law, statute, or regulation, etc.

(1) Any TASER weapon.

e. If the status of an unlisted weapon or item is questionable, it shall be referred to the Center Chief of Security for a further analysis and determination.

CHAPTER 24. KSC FLAG POLICY

24.1 GENERAL

The purpose of this chapter is to provide the requirements necessary to implement and maintain a consistent policy governing the flying of the United States flag on KSC.

24.2 SCOPE

This chapter applies to NASA, contractors and tenants on KSC which display the National Colors on exterior staffs. It establishes the KSC National Flag Retirement Program. It also provides a procedure by which deceased active, resident employees may be honored by the Center's flags being flown at half staff and the employees' next of kin receiving a flag flown at KSC, at or following the funeral. Deceased retired employees may be honored as described herein only if specifically approved by the Center Director.

24.3 AUTHORITY

The authority for this policy is derived from Public Law 94-344, "Flag of United States - Display Rules," Presidential Proclamation 3044, "Display of the Flag of the United States of America at Half-Staff Upon the Death of Certain Officials and Formal Officials (as amended)," and NPD 100., "Displaying the United States Flag at Half-Staff."

24.4 RESPONSIBILITIES

a. The Center Director, under the authority of NPD 100, shall appoint the KSC Flag Protocol Officer (FPO).

RELEASED - Printed documents may be obsolete; validate prior to use.

b. The Director of Spaceport Services under the authority of the Associate Administrator for Security Management and Safeguards (Code X, NASA Headquarters) shall:

1. Approve, or disapprove, the Center's honoring deceased active employees.

2. Direct the Flag Protocol Officer (FPO) to implement the policy and procedures contained herein.

3. Inform the Center Director when a deceased active employee is so honored.

c. Senior Managers for NASA, contractors and tenants shall notify the FPO in case of the death of a active KSC employee. Notification may be made by calling either the Joint Communications Control Center at 867-11, or the Protective Services & Safeguards Office at 867-461.

d. The FPO shall coordinate all matters involving the flags of the United States on KSC. This includes, but is not limited to:

1. Direct the J-BOSC Protective Services, Projects and Integration Office, 861-5657, to coordinate with KSC contractors and tenants to have the United States flag flown at half staff at their respective facilities.

2. Request publication of weekly KSC Bulletin notices and in the Daily News, as appropriate, to inform the Center's employees for whom, and when the flag was/shall be flown at half staff.

3. Notify the Associate Administrator for Management Systems and Facilities, when and for whom the KSC flags were flown at half-staff.

4. Manage the KSC National Flag Retirement Program.

e. J-BOSC Security shall maintain a supply of flags of the United States, previously flown over KSC, to be cleaned, folded, and presented to the next of kin of deceased active KSC employees, or as directed by the FPO. The Property Custodian shall ensure that with each flag, are the exclusive dates when the flag flew, and what missions were launched/landed during the flag's service.

RELEASED - Printed documents may be obsolete; validate prior to use.

f. NASA KSC welcomes tenants of KSC who fly the National Colors outside their facilities to participate in the KSC National Flag Retirement Program. Under this voluntary program, the tenant shall provide their worn/tattered flags to the J-BOSC Security Property Custodian, who processes them as in the proceeding paragraph, thus ensuring the dignified and honorable disposition of the flag.

24.5 PROCEDURES

a. The documents listed above in Section 413.3 - Authority, contains the procedures which KSC shall follow in flying the flag of the United States, with the following additional provisions:

1. The flag of the United States may also be flown at half staff on the day of a deceased active KSC employee's funeral, or as directed by the Center Director.

2. When the flag of the United States is flown at half staff, no other flag shall be flown on it's or adjacent flag poles.

3. At KSC, all flags of the United States shall be flown at either full staff or half staff, simultaneously.

4. Whenever the flag of the United States is flown at full staff, flags below it shall be positioned so that when the flag of the United States lies fallow, it shall not touch the flag below it.

b. The sequence of events for honoring deceased active KSC employees is:

1. The deceased employees management notifies the J-BOSC Security or the FPO of the death of an active KSC employee.

2. The FPO briefs the Director of Spaceport Services on the death and receives permission to honor the employee with the KSC flags being flown at half staff on the day of the funeral, or as directed by the Center Director.

3. The FPO procures a KSC flown flag, along with it's history, from the J-BOSC Security, Property Custodian and gives it to the employee's Senior Manager.

RELEASED - Printed documents may be obsolete; validate prior to use.

4. Normally, the presentation of the flag to the next of kin shall be made by the employee's Senior Manager, or their representative.

5. The FPO ensures that an entry is made as soon as it is possible in the KSC Weekly Bulletin and Daily News when and for whom the flag of the United States was/shall be flown at half staff at KSC.

CHAPTER 25. KSC CHILD CARE DEVELOPMENT CENTER PROGRAM

25.1 GENERAL

This document establishes KSC's procedural requirements for the development and implementation of a Child Care Program in compliance with the Crime Control Act of 1990 with respect to the KSC Child Care Development Center (KSC-CDC) and screening of current and prospective Child Care Service Providers.

25.2 RESPONSIBILITIES

a. The Protective Service and Safeguards Office shall be responsible for:

(1) Serving as the point of contact with the Procurement Office for policies and procedures relating to personnel security investigations of Child Care Service Providers at the KSC-CDC.

(2) Ensuring that all existing and newly hired Child Care Service Providers are the subject of a National Agency Check (NAC)(FBI Fingerprints and Name Check).

(3) Local Law Enforcement checks shall be conducted by the Personnel Security Support Office (PSSO) and shall cover areas of residence for the past 5 years. Law Enforcement checks shall also be conducted on any residences outside of the local area.

(4) Evaluating the results of the NAC and local records check.

(5) Maintaining a security file on all Child Care Service Providers. Placing all Child Care Service Providers in a "Monitored" status.

(6) Annually, based on Child Care Service Provider's hire date, local Law Enforcement, Brevard County Court records, and

RELEASED - Printed documents may be obsolete; validate prior to use.

drivers license checks shall be conducted.

(7) Providing any adverse information resulting from the NAC or Local Law Enforcement checks, in writing, concerning Child Care Service Providers to the Director, Procurement/KSC-Exchange Operations Manager for a determination of suitability for employment.

(8) Providing KSC-CDC with required forms (SF85P, “Questionnaire for Public Trust Positions, “SF87s, “Fingerprint Cards,” and the NASA 531, “Name Check Request”).

(9) Routing all correspondence and information pertaining to and for KSC-CDC through KSC-Exchange Operations Manager.

b. The Procurement Office is responsible for:

(1) Acting as point of contact between KSC-CDC and NASA Protective Services and Safeguards Office.

(2) Making suitability for employment determinations concerning adverse information obtained on Child Care Service Providers.

c. The Director of the Child Care facility (KSC-CDC) is responsible for:

(1) Notifying the Protective Services & Safeguards Office when hiring Child Care Service Providers and initiating security investigations.

(2) Maintaining a current listing of all individuals who come in contact with the children at the KSC-CDC either in a teaching or non-teaching capacity.

(3) Providing in accordance with the Draft NASA Federal Personnel Manual (FPM) Supplement to implement the “Crime Control Act of 1990,” direct line-of-sight supervision to those Child Care Service Providers whose background investigations have not been completed.

(4) Annually, submitting (5 days prior to the employment anniversary “Date of Hire”) for each Child Care Service Provider, a KSC Form 4-649 NS and the EHS-14, “Caretaker Background Screening Information” form.

RELEASED - Printed documents may be obsolete; validate prior to use.

(5) Notifying the Protective Services & Safeguards Office of the termination of any Child Care Service Provider.

25.3 ADVERSE INFORMATION

a. Adverse or derogatory information resulting from criminal history background checks shall be summarized by PSSO and evaluated by Protective Services and Safeguards Office.

b. A copy of adverse information along with a copy of the Subject Interview shall be sent to Director of Procurement/KSC-Exchange Operations Manager for a determination of suitability for employment.

c. OP shall notify the Protective Services and Safeguards Office, in writing within 30 days of their final determination of suitability for employment.

25.4 PERIODIC REINVESTIGATIONS

a. On an annual basis, local records checks shall be conducted by PSSO. These checks shall include Brevard County Court records, and State of Florida Driver's License check.

b. These checks shall be conducted on the anniversary of the "Date of Hire" for a Child Care Service Provider.

CHAPTER 26. FEDERAL EMPLOYEE SECURITY PROGRAM (FESP)

27.1 GENERAL

The Center Director delegates to the CCS authority to grant security clearances to employees under his jurisdiction subject to the eligibility standards.

The Federal Employees Security Program insures that:

a. All new civil service employees are the subject of a Personnel Security Investigation.

b. All civil service employees requiring access to classified information are investigated and adjudicated to the appropriate security clearance level (Top Secret, Secret, or Confidential) and that their position sensitivity level reflects their level of access to classified information. Investigations are updated in accordance with Office of Personnel

RELEASED - Printed documents may be obsolete; validate prior to use.

Management (OPM) requirements.

c. All civil service employees are investigated based on their position sensitivity level as it relates to their job functions and responsibilities. This position sensitivity designation is dependent of any requirement for access to classified information. Investigations are updated in accordance with OPM requirements.

27.2 POSITION SENSITVITY LEVELS

All civil service positions are designated at one of four position sensitivity levels. They are Nonsensitive (NS), Noncritical Sensitive (NCS), Critical Sensitive (CS), and Special Sensitive (SS). The position sensitivity level is a reflection of the security clearance (Confidential, Secret, Top Secret) required by a position and/or the duties and responsibilities (positions of trust, potential damage to efficiency of the service) associated with the position.

27.3 RESPONSIBILITIES

a. The FESP Manager, Protective Services and Safeguards Office, is responsible for:

(1) Ensuring that civil employees are investigated and adjudicated in accordance with the Government issuance's referenced in the list of references.

(2) Receiving and approving requests for security clearances and reviewing and changing, as necessary, the position sensitivity level to ensure that it adequately reflects the level of approved access to classified information.

(3) Serving as primary point of contact with the Workforce & Diversity Management Office for policies and procedures relating to the FESP.

b. The Director, Workforce & Diversity Management Office is responsible for:

(1) Coordinating investigative requirements for new hire civil service employees with the FESP Manager.

(2) Designating position sensitivity levels for each civil service position based on duties and responsibilities (not involving access to classified information).

RELEASED - Printed documents may be obsolete; validate prior to use.

(3) Making suitability determinations for all civil service employees.

Note: Review and disposition of adverse OPM reports of investigation shall be completed within ninety days in accordance with OPM requirements. The FESP Manager shall be advised of disposition in order to forward a response to OPM.

27.4 NASA PRE-EMPLOYMENT SCREENING

The Protective Services and Safeguards Office conducts pre-employment screening on potential NASA new hires. The pre-employment screening shall include criminal, education, credit, driving record checks, employment verifications, and reference checks. The results of pre-employment screenings are provided to the Personnel Office.

27.5 PERIODIC REINVESTIGATIONS

a. Special Sensitive and Critical Sensitive Positions. Civil service employees in these positions shall be subject to reinvestigation 5 years after placement, and every succeeding 5 years.

b. Noncritical Sensitive Position. Civil service employees in these positions shall be subject to reinvestigation 10 years after placement and every succeeding 10 years.

c. Nonsensitive Positions. Civil service employees in these positions are not subject to reinvestigation.

27.6 SECURITY CLEARANCES

a. A security clearance is an approval for access to classified national security information. Security clearances are granted by authorized federal organizations based on an appropriate level of investigation of an individual. Security clearances grant access to a level of classified information (Confidential, Secret, or Top Secret) for a specific purpose.

b. A security clearance is terminated when an employee no longer requires access to classified information or ends his/her employment with the issuing Federal agency. For example, when a civil service employee leaves another government agency and joins NASA his/her security clearance with the other agency is no longer active and the individual is not authorized access to classified information. If the employee requires access to classified information as part of his/her new job at NASA, NASA shall take appropriate action to grant a

RELEASED - Printed documents may be obsolete; validate prior to use.

security clearance.

c. KSC shall not honor a security clearance granted by another agency for access to classified information under KSC's control, unless there is a relationship between that agency and NASA and a basis for doing so. For example, an employee may be cleared for an assignment in the military reserves; but the clearance is invalid at KSC because there is no relationship between the reserve unit and KSC. On the other hand, KSC has a relationship with the Defense Industrial Security Clearance Office (DISCO) and frequently honors clearances of defense contractors. However, if the individual's work for KSC is not under a classified contract, the clearance shall not be accepted since there is no basis for doing so.

d. While security clearances do not transfer from one agency to another, the results of background investigations, which are the basis for granting clearances, are available to all federal agencies. If the investigation is adequate in scope and is not outdated, a previous investigation may be used for granting a security clearance by NASA.

27.7 SECURITY CLEARANCES FOR CIVIL SERVANTS

a. NASA employees shall be granted security clearances only when a demonstrated need exists for the performance of their duties.

b. A NASA Form 1630, "Request for Access to Classified National Security Information," shall be submitted to the Protective Service Office/The Protective Services & Safeguards Office, and used to document the justification of each security clearance request. The form must be prepared and certified by the employee's immediate supervisor, reviewed by a designated management official (division chief, or higher, depending on the employee's organizational position), and approved by the Installation Security Officer (Chief, Protective Services and Safeguards Office).

c. If an employee's personnel security folder does not contain the results of an adequate previous background investigation commensurate with the level of clearance requested, the employee shall be provided with security forms to complete and submit to Protective Services and Safeguards Office.

e. When clearances are no longer required, employees shall be notified through their supervisors that their security clearances are being

RELEASED - Printed documents may be obsolete; validate prior to use.

administratively withdrawn without prejudice to the individual.

f. A security clearance recertification must be submitted annually, or whenever a person changes positions. Failure to provide an annual recertification to Protective Services & Safeguards Office shall result in administrative withdrawal of an employee's security clearance.

g. Before a clearance is granted, the employee must attend required security education courses. He/she must also sign a Standard Form 31, "Classified Information Nondisclosure Agreement." At the time the employee receives the security clearance his/her supervisor shall brief the employee on his/her specific classified duties. The briefing shall be documented on NASA Form 838, "Employee Security Orientation/Indoctrination Record,"

27.8 CERTIFYING SECURITY CLEARANCES FROM KSC

NASA personnel on travel status who require access to classified information at a defense contractor or other Government agency may have their security clearance certified to that organization. A KSC Form 0-1NS, "Clearance Verification, Telegram Format," shall be prepared by the employee's office an forwarded to Protective Services and Safeguards Office for processing.

27.9 CERTIFYING SECURITY CLEARANCES TO KSC

a. NASA participates in the National Industrial Security Program. The Defense Industrial Security Clearance Office (DISCO) grants personnel security clearances to defense contractors which shall be honored at KSC when contractor employees are working under a classified contract and have classified work to perform at KSC. Contractor employees should consult their respective company security offices for procedural requirements regarding clearances.

b. KSC shall honor clearances of employees of other Government agencies who are conducting classified work at KSC.

c. Cleared employees of defense contractors and other federal agencies should send their visit notices and clearance verification to:

NASA Visitor Record Center
ATTN: VRC
Kennedy Space Center, FL 3899

27.10 CO-OPERATIVE (CO-OP) EDUCATION STUDENTS

RELEASED - Printed documents may be obsolete; validate prior to use.

a. Initially, Co-op students entering on duty shall be processed in by Personnel and Security in the same manner as new NASA employees.

b. When a Co-op student goes on Leave Without Pay (LWOP) status to return to school, he/she shall return his/her KSC badge to the Personnel Security Support Office (PSSO) at the Headquarters Building, Room 1503. c. When a Co-op student returns to duty, the Co-op shall obtain his/her badge from PSSO at the Headquarters Building.

CHAPTER 28. PERSONNEL RELIABILITY PROGRAM (PRP)

28.1 GENERAL

The NASA Personnel Reliability Program (PRP) ensures that personnel assigned to mission critical positions/duties relating to the Space Shuttle and other critical space systems, including the Space Station, designated Expendable Launch Vehicles (ELV's), designated payloads, Shuttle Carrier Aircraft and other designated resources that provide access to space meet suitability screening requirements prior to unescorted access to areas where the Space Shuttle and/or any of the other systems are located. The Space Shuttle and other systems are "mission critical space system." "Mission critical positions/duties" are those positions/duties which if performed in a faulty, negligent or malicious manner, could jeopardize these systems or delay a mission.

28.2 RESPONSIBILITIES

The Center Director is responsible for designating KSC mission critical system areas, and designating the following management officials responsible with the following tasks:

a. The KSC PRP Manager, Protective Services & Safeguards Office, is responsible for:

(1) Administering the KSC Personnel Reliability Program.

(2) Approving PRP certification of civilian and contractor employees.

(3) Referring cases to the Center Chief of Security (CCS), Protective Services & Safeguards Office, which based on the Adjudication Guidelines, contain unreasonable issues, thus requiring temporary suspension of PRP until further

RELEASED - Printed documents may be obsolete; validate prior to use.

investigation can be conducted and issues resolved.

(4) Referring cases to the Personnel Reliability Board (PRB) which contain significant issues that were unable to be resolved by the PRP Manager or ISO.

(5) Ensuring that the individuals certified under the PRP remain current in their update screening and withdrawing PRP certifications from those individuals who fail to submit their forms by the date instructed or who no longer have a requirement for unescorted access to mission critical space systems areas.

(6) Serving as primary point of contact with the KSC civilian and contractor personnel offices for policies and procedures relating to the PRP.

b. The Personnel Security Support Office (PSSO) is responsible for:

(1) Notifying employees, appropriate contractor security offices, or administration offices when an employee's certification for PRP requires reinvestigation. Appropriate forms and instructions are provided for the reinvestigation.

(2) Reviewing forms submitted for Interim PRP, PRP, or recertification for accuracy and completeness and comparing submitted forms with previous forms submitted for any new information revealed, or information which may have been omitted. Any discrepant or derogatory information revealed at this time is brought to the attention of the PRP Manager for the requirements concerning interviews, medical, employer's evaluation, etc. Forms are then suspended and inquires made of the appropriate agencies (e.g., FBI, state and local law enforcement, Motor Vehicles) and files are suspension until response are received.

(3) Summarizing investigative data mentioned in 503.b(2) and bringing cases with discrepant or derogatory to the PRP Manager for final adjudication.

(4) Acting for the KSC PRP Manager in approving PRP certification or recertification on any employee's case which is clear of discrepant or derogatory information.

RELEASED - Printed documents may be obsolete; validate prior to use.

(5) PSSO has direct accountability to the NASA Protective Services & Safeguards Office. Due to the sensitive nature of the information dealt with on a daily basis, the employees staffing the PSSO have met the minimum requirements of a favorable Background Investigation (BI). Dissemination of any of this information to anyone outside of the Protective Services & Safeguards Office is ground for immediate dismissal.

c. The Chief, Occupational Health Branch, is responsible for reviewing case files involving medical issues and rendering medical opinions regarding mental stability and/or physical reliability for consideration by the Board.

d. The Director, Procurement, is responsible for taking necessary action to direct heads of prime contractor organizations to:

(1) Establish internal administrative procedures which ensure that all contractor and subcontractor personnel occupying Mission Critical Positions as defined in this KNPR, or who require unescorted access to Mission Critical Space Systems Areas (all areas controlled under the KSC Area Permit System and other designated facilities, areas, operations, or flight hardware) are identified and submitted for investigation and certification under the NASA Personnel Reliability Program.

(2) Conduct periodic reviews at least annually of contractor and subcontractor positions and make certain that all Mission Critical Positions have been identified under the NASA Personnel Reliability Program. To aid contractor organizations in these reviews, the Protective Services & Safeguards Office shall provide each primary contractor organization with a listing of personnel who are badged for access to KSC but who do not possess a certification under the NASA PRP Program. Contractor organizations should carefully review these listings to ensure that none of the personnel identified are in Mission Critical Positions. These listings shall be provided to contractor organizations on a semi-annual basis. The contractor organizations review should include all persons employed under NASA contract including those persons who do not require access to KSC.

(3) Provide information, as requested by NASA, on any matter pertaining to the contractor organizations implementation of the

RELEASED - Printed documents may be obsolete; validate prior to use.

requirements and procedures contained in this KNPR.

(4) Indicate on adverse reports provided to the Protective Services & Safeguards Office, in accordance with the requirements of this KNPR, whether the individual occupies a Mission Critical Position.

(5) Assign, employ, or retain personnel in Mission Critical Positions, or use personnel to perform any mission critical duty, only if the individuals have been certified under Mission Critical Space Systems Personnel Reliability Program. (Note: Real-time operational situations may require non PRP certified “expert technicians” to visit KSC and perform mission critical work. Other situations may require the real-time delivery, installation and checkout of computer or test equipment. It is recognized that in an operational environment it is impossible to anticipate all situations. As a rule, every effort should be made to identify in advance, persons who may be required to perform the duties of a mission critical position and submit these persons for PRP certification. In real-time situations where visiting technicians are not PRP certified, work controls, to include escort and observation by technically knowledgeable KSC personnel, proper work authorizations, review and sign-off by quality assurance personnel, etc., shall have to suffice. The need for real-time expediencies and the utilization of non-PRP certified to perform mission critical work should be understood and approved by management.)

(6) Provide requested information when submitting individuals for certification to a Mission Critical Position and when requesting unescorted access.

(7) Require that supervisors brief PRP candidates and re-brief PRP personnel on the needs and intent of PRP.

e. The PRP Board is responsible for:

(1) Reviewing individual cases referred to the Board for certification under the Mission Critical Space System Personnel Reliability Program and/or for authorizing or denying unescorted access to KSCAP areas.

(2) Reviewing and designation of positions as mission critical and designating, or removing the designation of, a position as

RELEASED - Printed documents may be obsolete; validate prior to use.

mission critical for cases that come before the Board.

f. Supervisors are responsible for:

(1) Identifying and designating those positions, and the incumbent employee for each, within their organization which meet the definition of a mission critical position.

(2) Ensuring that only personnel who have been certified under Mission Critical Space Systems Personnel Reliability Program are assigned to mission critical positions/duties within their organization.

(3) Reviewing for reliability and nominating personnel whose duties require certification under the PRP.

(4) Certifying that the PRP Candidate holds current licenses, skill training certificates, and other documentation issued as required by applicable directives.

(5) Monitoring and continually evaluating personnel for steady, reliable performance and notifying the certifying official if changes occur which may compromise the safety and reliability of mission critical space systems.

(6) Briefing PRP candidates and rebriefing PRP personnel on the needs and intent of the PRP.

28.3 MISSION CRITICAL SPACE SYSTEMS AREAS (MCSSA)

"Director of each NASA Installation shall designate mission critical space systems areas." At KSC, the Protective Services & Safeguards Office is responsible for preparing and submitting to the Center Director, a listing of proposed MCSSAs.

28.4 OTHER AREA DESIGNATION PERSONNEL SCREENING REQUIREMENTS

a. NASA SECURITY AREAS. NHB 160.3 authorizes the Center Director to designate Security Areas (Restricted, Limited and Closed Areas) for the protection of government property and classified national security information. Facilities designated as Limited Areas for protection of flight hardware and/or other NASA resources require personnel with unescorted access to such areas, to be the subject of a favorably completed National Agency Check. At KSC, all Limited Areas

RELEASED - Printed documents may be obsolete; validate prior to use.

identified for the protection of flight hardware shall be designated as "mission critical space system areas" under the PRP and certification under the PRP shall meet the personnel screening requirements for Limited Areas. Limited and Closed Areas created for the protection of classified national security information shall require the appropriate security clearance level for unescorted access.

b. NASA RESOURCE PROTECTION (NRP) PROGRAM CATEGORY A & B ASSETS. NHB 160.3 requires KSC to designate NRP Category A (Mission Critical) and Category B (Mission Essential) Assets. Personnel requiring unescorted access to NRP Category A and/or B facilities must be the subject of a favorably completed National Agency Check. At KSC, all NRP Category A & B Assets shall be designated by the Center Director, KSC, as "mission critical space systems areas" under the PRP and certification under the PRP shall meet the personnel screening requirements for NRP Category A & B Assets.

c. KSC AREA PERMIT SYSTEM. All areas and flight hardware proximity codes identified under the KSC Area Permit System shall be designated as "mission critical space systems areas" by the Center Director. Issuance of a KSC Area Permit or a non-escorted Temporary Area Authorization to an individual is evidence of favorable certification under the NASA PRP.

28.5 AUTHORIZED REQUESTERS

Initially, PRP certification must be requested by one of the persons or organizations identified below. Thereafter, the same requester shall be notified when rescreening is required for recertification of PRP. The requesters are expected to submit the forms or information identified in paragraph 503.8 below, both for initial PRP requests and for subsequent recertification. The following are authorized to request PRP certifications:

a. NASA KSC civil service supervisors for their employees, or their designated civil service administrative office.

b. Authorized badging officials for employees of their organizations, contractors, and subcontractors.

c. Contacts for other visitors to KSC.

28.6 ACCEPTANCE OF OTHER PROGRAMS

a. Usually, the following shall be considered to have met the screening and evaluation requirements of this chapter:

RELEASED - Printed documents may be obsolete; validate prior to use.

(1) Flight crews and payload specialists who are covered by other regulations which require screening and evaluation commensurate with, or exceeding, that required by this chapter.

(2) Persons certified by NASA Headquarters, other NASA centers, or other agencies under the NASA Mission Critical Space Systems Personnel Reliability Program.

(3) Others who can prove screening under federal law or regulation commensurate with, or exceeding, that required by this chapter. In addition, they must prove the results of the screening have been evaluated with the same intent and considerations as set forth in this chapter. Clearance for access to classified material is not deemed to be adequate.

(4) Foreign Representatives who have a favorably completed National Agency Check (NAC) and have a Foreign National Security Questionnaire (KSC Form 0-181) or KSC Badge and Area Permit Investigative Data Form (KSC Form 0-90) on file, may be authorized unescorted access to mission critical space systems areas, but only to those areas for which they have operational need, and excluding those areas which protect the Space Shuttle or classified national defense information.

b. Persons who are given PRP certification pursuant to this paragraph do not need to submit forms required by paragraph 503.6. Instead, the organization which has screened and evaluated them, and which has the approval of the Protective Services and Safeguards Office, must provide the following information, in writing, for each person:

(1) Full name.

(2) Date and place of birth.

(3) Social security number. Passport, visa or alien registration numbers may be used in lieu of a social security number for aliens.

(4) The name of the screening program and a certification that the results of screening have been favorably evaluated.

(5) An expiration for the certification, not to exceed three years.

RELEASED - Printed documents may be obsolete; validate prior to use.

c. This information must be sent to the PSSO at the address in paragraph 503.8b below.

d. The organization shall be notified when the certification is about to expire. It shall be given an opportunity to renew it by rescreening and re-evaluating the person and providing a new certification.

28.7 VERIFYING PRP CERTIFICATIONS TO OTHER INSTALLATIONS

a. Every person who has unescorted access to KSC mission critical space systems areas is certified under the PRP. With the exception of those who are given unescorted access pursuant to paragraph 503.4 the PRP certifications have been granted by KSC. KSC's PRP certifications are acceptable to other NASA centers and to some other Government installations, such as, Vandenberg AFB, and may be required for other access privileges there. Personnel who are PRP-certified by KSC and who need their certification verified to another installation must use the following procedure:

(1) Prepare a letter to the installation on your organization's letterhead stationery.

(2) Address the letter to the office which maintains the installation's records of PRP certifications. Your point of contact at the installation should be able to provide the address.

(3) In the correspondence, include the full names, dates of birth, places of birth, and social security numbers of those individuals whose certifications need to be transmitted.

(4) Send the letter to PSSO Personnel Security Support Office. When time is short, the letter may be hand-carried to Room 1503, KSC Headquarters Building.

b. The PSSO shall verify the certifications, add their expiration dates, endorse your letter, and mail it to the other installation.

c. Once a person's certification has been verified, it should not be necessary to send it again to the same installation until it is renewed. Certifications that require renewal should be re-sent as needed.

28.8 FORMS AND PROCEDURES

RELEASED - Printed documents may be obsolete; validate prior to use.

a. The following forms are routinely used in the PRP for conducting a National Agency Check and/or rescreening. Samples and instructions for filling out these forms are provided by PSSO:

(1) KSC Form 0-87, “Request for Investigation and Unescorted Access Badge.”

(2) KSC Form 0-90, “KSC Badge & Area Permit Investigative Data Badge.”

(3) NASA Form 531, “Name Check Request.”

(4) SF-87, “Fingerprint Chart for Federal Employees” or FD-58, “Fingerprint Chart for Federal Employees” or SF-87, Fingerprint Chart for Non-Federal Employees.

b. Forms should be mailed or hand carried to:

Personnel Security Support Office
PSSO
Rm. 1503, HQ Bldg.
Kennedy Space Center, FL 3899

c. Forms which are incomplete, incorrect, or improperly executed shall not be processed and shall be returned. For initial submissions, the requester shall be notified when the forms have been accepted for processing. He/she shall be informed when unescorted access to mission critical space systems areas is initially authorized but shall not, when it is renewed.

d. PRP shall be administratively revoked on those individuals whose forms for renewal are not submitted within the given time frame. The requester shall be notified of the revocation and a request made to return the KSC Area Permit and PACAS badges by that date since the badges shall become inactive on the revocation date. If renewal forms are turned in after the revocation date an additional form shall be required for the Visitor Records Center, a new KSC Form 0-94, Kennedy Space Center Area Permit Application. This form can be mailed or hand-carried to:

Visitor Record Center

RELEASED - Printed documents may be obsolete; validate prior to use.

VRC
Rm. 1470, HQ Bldg.
Kennedy Space Center, FL 3899

28.9 SPECIFIC CRITERIA

Results of screening shall be evaluated to determine if authorizing unescorted access to mission critical space systems areas is clearly consistent with the preservation of national resources, government property and facilities, and a safe working environment. In addition to the requirements of Appendix A, evidence of any of the following conditions is reason to question a person's reliability and may be used to deny unescorted access to mission critical space system areas:

a. Negligence, inadequacy, or delinquency in duty performance.

b. Any significant physical or mental impairment, character disorder, or aberrant behavior substantiated by medical authority that might jeopardize national resources, government property and facilities, or a safe working environment.

c. Behavior patterns that demonstrate or suggest a contemptuous attitude toward the law or Federal, State or local regulations.

d. Behavior that indicates a disregard for national resources, government property and facilities, and a safe working environment.

28.10 DISPOSITION OF CASES WITH ADVERSE INFOMATION

a. In those cases where evaluation fails to clearly support the granting of PRP certification, the PRP Manager shall take appropriate investigative or other actions to resolve the adverse issues involved. If the adverse issues are of such a nature that they cannot be resolved, the PRP Manger shall prepare the case for submission to the Personnel Reliability Board. The PRP Board may deny or approve PRP certification and may set conditions on any area or system accesses which it approves.

b. If a case has potentially disqualifying information and the person has unescorted access to mission critical space systems areas, the PRP Manager, with concurrence of the Center Chief of Security, may temporarily suspend PRP certification.

28.11 REPORTING ADVERSE INFORMATION

RELEASED - Printed documents may be obsolete; validate prior to use.

a. Individuals with PRP are required to report any adverse information/incidents such as arrests due to alcohol, drugs, etc. to their supervisor/management within 7 hours of the incident.

b. Supervisors/Management are required to provide a written report of adverse information to the NASA KSC Protective Services and Safeguards Office PRP Program Manager.

The Adverse Information Report should contain the following information:

(1) Subject's name
(2) Social Security Number
(3) Date and Place of Birth
(4) Clearance level/Date
(5) Address of Subject
(6) Subject's physical worksite
(7) Mission critical status
(8) Descriptions and details of adverse information

28.12 INTERIM PRP

a. Interim PRP can be granted to new civil service employees who have had a favorable pre-employment screening; or are transferring from another federal agency in which a favorable investigation was completed within the last five years.

b. Resident contractor organizations can request Interim PRP for new employees after the company has performed a contractor pre-employment screening. The pre-employment screening shall include all of the checks required by the NASA Internal Security Office (i.e., a check of the criminal history records, previous employment, residences, education, verification of professional licenses (if applicable), and a DD 14). The contractor shall then forward the completed pre-employment screening, NAC forms (see paragraph 503.8) and KSC Form 0-18NS, "Request for Interim Unescorted Access," to the PSSO. After a review of all information received a determination for Interim PRP shall be made. The contractor organization shall be notified if IUA cannot be granted.

c. Construction employees performing working in limited areas can provide NAC form (see paragraph 503.8) to the Contracting Officer for submission to the Protective Services and Safeguards Office. Investigation activities shall take approximately 7-10 days.

RELEASED - Printed documents may be obsolete; validate prior to use.

Note: In addition to the routine information requested on the NAC forms, the driver's license number is required on the top of the KSC Form 0-90, and the contract number and "Request for IUA" is needed on the KSC Form 0-87. The Contracting Officer shall be notified if Interim PRP cannot be granted.

29.13 PERSONNEL RELIABILITY BOARD (PRB)

a. The PRB shall:

(1) Certify the individual as meeting the requirements of the Mission Critical Space Systems Personnel Reliability Program; or,
(2) Deny Certification of PRP based on the available information.
(3) Conditionally grant PRP and allow unescorted access to areas under the KSCAP Program; or
(4) Request additional information and delay the decision until the information is received.

b. In cases where the PRB fails to certify the individual as reliability or conditionally authorizes, the PRB Secretary (PRP Program Manager) shall furnish reasonable notice of the PRB's decision to the affected individual and his/her employer. This notice shall include a statement of the PRB's decision, and the basis thereof (to the extent allowed under the Privacy Act). This notice shall also advise that upon written request filed with the PRB Secretary, the PRB shall reconsider its decision. Further, if the subject is a subcontractor employee, the prime contractor shall be advised of the disposition of its request.

c. The PRB, during the reconsideration process, shall allow the individual and one representative of his/her choosing to appear before the PRB. Pertinent rebuttal or explanations of the issue(s) in question shall be permitted by the PRB at this time,

d. The PRB, when an appeal is requested, shall provide the Center Director with the documentation generated during the PRB's proceedings. The appeal to the Center Director is a document review process only and does not involve personal presentations.

CHAPTER 29. AUTOMATED INFORMATION PERSONNEL SECURITY PROGRAM

29.1 GENERAL

To ensure that Government and contractor personnel associated with NASA

RELEASED - Printed documents may be obsolete; validate prior to use.

Automated Information Resources are investigated to the level required by their position.

29.2 RESPONSIBILITIES

a. The Information Management Office is responsible for implementation of the NASA Automated Information Security (AIS) Program at KSC, to include identification of the criteria for determining which positions require investigation under the AIS Program and the level of investigation required.

b. The Protective Services and Safeguards Office is responsible for conducting personnel security investigations in support of the AIS Program.

APPENDIX A. MISCELLANEOUS CONTROLLED ACTIVITIES

The following miscellaneous activities are controlled, as stated:

a. Alcohol. The possession or consumption of alcohol in areas under KSC cognizance is restricted, except those areas approved by Senior Management. Employees and their guests may not consume alcoholic beverages (except at official functions sponsored by NASA) within the controlled area of KSC. Employees and their guests may possess and consume alcohol at KARS Park I and II, and also at KSC Visitor's Center when they are not on duty.

b. Contraband Drugs. All illegal drugs are prohibited from introduction onto the KSC.

c. Illegal Activity. All activities defined as illegal through local ordinance. State statute, or by Federal legislation are prohibited on KSC.

d. Personal Trailers, Recreational Vehicles, and Trailered Boats. Personal trailers, recreational vehicles, and trailered boats are prohibited from access onto KSC. Exceptions to this may be made on a case-by-case basis by the Center Chief of Security. Badged employees who use their badges to transverse the controlled area while towing a personal trailer, towing or driving a recreational vehicle, or towing a trailered boat are misusing their badge.

RELEASED - Printed documents may be obsolete; validate prior to use.