NASA 10SECR (15-115, 80 FR 246, pp. 79937-79947)

SYSTEM NAME: Security Records System.

SECURITY CLASSIFICATION: None.

SYSTEM LOCATION:

The centralized data system is located at Location 9. Records are also located at Locations 1 through 9 and Locations 11, 12, and 14. The locations are set forth in Appendix A.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This system maintains information on Civil Servant Employees, applicants, NASA committee members, NASA consultants, NASA experts, NASA Resident Research Associates, guest workers, contractor employees, detailees, visitors, correspondents (written and telephonic), Faculty Fellows, Intergovernmental Personnel Mobility Act (IPA) Employees, Grantees, Cooperative Employees, and Remote Users of NASA Non-Public Information Technology Resources. This system also maintains information on all non-U.S. citizens, to include Lawful Permanent Residents seeking access to NASA facilities, resources, laboratories, contractor sites, Federally Funded Research and Development Centers or NASA sponsored events for unclassified purposes to include employees of NASA or NASA contractors; prospective NASA or NASA contractor employees; employees of other U.S. Government agencies or their contractors; foreign students at U.S. institutions; officials or other persons employed by foreign governments or other foreign institutions who may or may not be involved in cooperation with NASA under international agreements; foreign media representatives; and representatives or agents of foreign national governments seeking access to NASA facilities, to include high-level protocol visits; or international relations.

CATEGORIES OF RECORDS IN THE SYSTEM:

Personnel Security Records, Personal Identity Records including NASA visitor files, Emergency Data Records, Criminal Matters, Traffic Management Records, and Access Management Records. Specific records fields include, but are not limited to: Name, former names, date of birth, place of birth, social security number, home address, phone numbers, citizenship, traffic infraction, security violation, security incident, security violation discipline status and action taken.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

18 U.S.C. §793–799, Espionage and Information Control Statutes;

18 U.S.C. §2151–2157, Sabotage Statutes;

18 U.S.C. §202–208, Bribery, Graft, and Conflicts of Interest;

18 U.S.C. §3056, Powers, authorities, and duties of United States Secret Service;

18 U.S.C. §371, Conspiracy Statute;

40 U.S.C. §1441, Responsibilities regarding efficiency, security, and privacy of Federal computer systems;

44 U.S.C. §3101, Records management by agency heads; general duties;

50 U.S.C., §Internal Security Act of 1950;

51 U.S.C. §20101 National and Commercial Space Programs

42 U.S.C. §2011 et seq., Atomic Energy Act of 1954, as amended;

Executive Order 9397, as amended, Numbering System for Federal Accounts Relating to Individual Persons;

Executive Order 13526, as amended, Classified National Security Information;

Executive Order 12968, as amended, Access to Classified Information;

Executive Order 10865, Safeguarding Classified Information Within Industry;

Executive Order 10450, Security Requirements for Government Employees;

Pub. L. 81–733, Summary suspension of employment of civilian officers and employees;

Pub. L. 107–347, Federal Information Security Management Act 2002;

HSPD 12, Policy for a Common Identification Standard for Federal Employees and Contractors;

14 CFR parts 1203 through 1203b, NASA Information Security Program;

14 CFR 1213; NASA Release of Information to News and Information Media;

15 CFR 744; EAR Control Policy: End-user and End-use Based;

22 CFR 62, Exchange Visitor Program;

22 CFR 120-130; Foreign Relations Export Control;

41 CFR Chapter 101 Federal Property Management Regulation.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Any disclosures of information will be compatible with the purpose for which the Agency collected the information. The records and information in these records may be disclosed:

1. To the Department of Justice (DOJ) when: (a) The agency or any component thereof; (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the DOJ has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by DOJ is therefore deemed by the agency to be for a purpose compatible with the purpose for which the agency collected the records.

2. To a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to

represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

3. To an Agency in order to provide a basis for determining preliminary visa eligibility.

4. To a staff member of the Executive Office of the President in response to an inquiry from the White House.

5. To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. §§ 2904 and 2906.

6. To agency contractors, grantees, or volunteers who have been engaged to assist the agency in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. § 552a.

7. To other Federal agencies and relevant contractor facilities to determine eligibility of individuals to access classified National Security information.

8. To any official investigative or judicial source from which information is requested in the course of an investigation, to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.

9. To the news media or the general public, factual information the disclosure of which would be in the public interest and which would not constitute an unwarranted invasion of personal privacy, consistent with Freedom of Information Act standards.

10. To a Federal, State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947 as amended, the CIA Act of 1949 as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.

11. In order to notify an employee's next-of-kin or contractor in the event of a mishap involving that employee or contractor.

12. To notify another Federal agency when, or verify whether, a PIV card is valid.

13. To provide relevant information to an internal or external organization or element thereof conducting audit activities of a NASA contractor or subcontractor.

14. To a NASA contractor, subcontractor, grantee, or other Government organization information developed in an investigation or administrative inquiry concerning a violation of a Federal or state statute or regulation on the part of an officer or employee of the contractor, subcontractor, grantee, or other Government organization.

15. To foreign governments or international organizations if required by treaties, international conventions, or executive agreements.

16. To members of a NASA Advisory Committee or Committees and interagency boards charged with responsibilities pertaining to international visits and assignments and/or national

security when authorized by the individual or to the extent the committee(s) is so authorized and such disclosure is required by law.

17. To the following individuals for the purpose of providing information on traffic accidents, personal injuries, or the loss or damage of property: (a) Individuals involved in such incidents; (b) persons injured in such incidents; (c) owners of property damaged, lost or stolen in such incidents; and/or (d) these individuals' duly verified insurance companies, personal representatives, employers, and/or attorneys. The release of information under these circumstances should only occur when it will not: (a) interfere with ongoing law enforcement proceedings, (b) risk the health or safety of an individual, or (c) reveal the identity of an informant or witness that has received an explicit assurance of confidentiality. Social security numbers should not be released under these circumstances unless the social security number belongs to the individual requester.'' The intent of this use is to facilitate information flow to parties who need the information to adjudicate a claim.

18. To the Transportation Security Administration, with consent of the individual on whom the records are maintained, to establish eligibility for the TSA Pre✓ program.

19. In accordance with NASA standard routine uses as set forth in Appendix B.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system are maintained electronically and in hard-copy documents.

RETRIEVABILITY:

Records are retrieved from the system by individual's name, file number, badge number, decal number, payroll number, Agency-specific unique personal identification code, and/or Social Security Number.

SAFEGUARDS:

Electronic records are maintained on secure NASA servers and protected in accordance with all Federal standards and those established in NASA regulations at 14 CFR 1212.605. Additionally, server and data management environments employ infrastructure encryption technologies both in data transmission and at rest on servers. Approved security plans are in place for information systems containing the records in accordance with the Federal Information Security Management Act of 2002 (FISMA) and OMB Circular A-130, Management of Federal Information Resources (OA-9999-M-MSF-2712, OA-9999-M-MSF-2707, IE-999-M-MSF-1654). Only authorized personnel requiring information in the official discharge of their duties are authorized access to records through approved access or authentication methods. Access to electronic records is achieved only by utilizing NASA agency managed authentication mechanisms. Non-electronic records are secured in access-controlled rooms with electronic security countermeasures and agency managed, PIV enabled, physical authentication mechanisms.

RETENTION AND DISPOSAL:

The Personnel Security Records are maintained in Agency files and destroyed upon notification of the death or within 5 years after separation or transfer of employee or within 5 years after contract relationship expires, whichever is applicable in accordance with NASA Records Retention Schedules (NRRS), Schedule 1 Item 103. The foreign national files are maintained in Agency files and destroyed in accordance with NRRS, Schedule 1 Item 35.

The Personal Identity Records are maintained in Agency files and destroyed upon notification of the death or within 5 years after separation or transfer of employee or within 5 years after contract relationship expires, whichever is applicable in accordance with NRRS, Schedule 1 Item 103. Visitor files are maintained and destroyed in accordance with NRRS, Schedule 1 Item 114.

The Emergency Data Records are maintained in Agency files and destroyed when superseded or obsolete in accordance with NRRS 1, Item 100B.

The Criminal Matter Records are maintained in Agency files and destroyed in accordance with NRRS 1, Schedule 97.5, Items A and B.

The Traffic Management Records are maintained in Agency files and destroyed in accordance with NRRS 1, Schedule 97.5, Item C.

SYSTEM MANAGER(S) AND ADDRESS:

System Manager: Deputy Assistant Administrator of the Office of Protective Services, Location 1. Subsystem Managers: The Chief of Security/Protective Services at each subsystem location at locations 1 through 9 and locations 11, 12, and 14. Locations are as set forth in Appendix A.

NOTIFICATION PROCEDURE:

Information may be obtained from the cognizant system or subsystem manager listed above. Requests must contain the following identifying data concerning the requestor: First, middle, and last name; date of birth; Social Security Number; period and place of employment with NASA, if applicable.

RECORD ACCESS PROCEDURES:

Personnel Security Records compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to

classified information have been exempted by the Administrator under 5 U.S.C. 552a(k)(5) from the access provisions of the Act.

Personal Identity Records: Requests from individuals should be addressed to the same address as stated in the Notification section above.

Emergency Data Records: Requests from individuals should be addressed to the same address as stated in the Notification section above.

Criminal Matter Records compiled for civil or criminal law enforcement purposes have been exempted by the Administrator under 5 U.S.C. 552a(k)(2) from the access provision of the Act.

Traffic Management Records: Requests from individuals should be addressed to the same address as stated in the Notification section above.

CONTESTING RECORD PROCEDURES:

For Personnel Security Records and Criminal Matters Records, see Record Access Procedures, above. For Personal Identity Records, Emergency Data Records, and Traffic Management Records, the NASA rules for access to records and for contesting contents and appealing initial determinations by the individual concerned appear at 14 CFR part 1212.

RECORD SOURCE CATEGORIES:

Information is obtained from a variety of sources including the employee, contractor, or applicant via use of the Standard Form (SF) SF–85, SF–85P, or SF–86 and personal interviews; employers' and former employers' records; FBI criminal history records and other databases; financial institutions and credit reports; medical records and health care providers; educational institutions; interviews of witnesses such as neighbors, friends, coworkers, business associates, teachers, landlords, or family members; tax records; and other public records. Security violation

information is obtained from a variety of sources, such as guard reports, security inspections, witnesses, supervisor's reports, audit reports.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Personnel Security Records compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a confidential source, are exempt from the following sections of the Privacy Act of 1974, 5 U.S.C. 552a(c)(3) relating to access to the disclosure accounting; (d) relating to access to the records; (e)(1) relating to the type of information maintained in the records; (e)(4)(G), (H) and (I) relating to publishing in the annual system notice information as to agency procedures for access and correction and information as to the categories of sources of records; and (f) relating to developing agency rules for gaining access and making corrections. The determination to exempt the Personnel Security Records portion of the Security Records System has been made by the Administrator of NASA in accordance with 5 U.S.C. 552a(k)(5) and Subpart 5 of the NASA regulations appearing in 14 CFR part 1212.

Criminal Matter Records to the extent they constitute investigatory material compiled for law enforcement purposes are exempt from the following sections of the Privacy Act of 1974, 5 U.S.C. 552a(c)(3) relating to access to the disclosure accounting; (d) relating to access to the records; (e)(1) relating to the type of information maintained in the records; (e)(4)(G), (H) and (I) relating to publishing in the annual system notice information as to agency procedures for access and correction and information as to the categories of sources of records; and (f) relating to developing agency rules for gaining access and making corrections. The determination to exempt the Criminal Matter Records portion of the Security Records System has been made by the

Administrator of NASA in accordance with 5 U.S.C. 552a(k)(2) and subpart 5 of the NASA regulations appearing in 14 CFR part 1212.

Records subject to the provisions of 5 U.S.C. 552(b)(1) required by Executive Order to be kept secret in the interest of national defense or foreign policy are exempt from the following sections of the Privacy Act of 1974, 5 U.S.C. 552a:(c)(3) relating to access to the disclosure accounting; (d) relating to the access to the records; (e)(1) relating to the type of information maintained in the records; (e)(4)(G), (H) and (I) relating to publishing in the annual system notice information as to agency procedures for access and correction and information as to the categories of sources of records; and (f) relating to developing agency rules for gaining access and making corrections.

The determination to exempt this portion of the Security Records System has been made by the Administrator of NASA in accordance with 5 U.S.C. 552a(k)(1) and subpart 5 of the NASA regulations appearing in 14 CFR part 1212.