PIA Analysis Worksheet and Summary Template

The template for an information technology (IT) system Privacy Impact Assessment (PIA) Analysis Worksheet and Summary Template begins on the following page. The Template covers the four major categories of information required for inclusion into the PIA: system characterization, information sharing practices, Web site practices, and security controls.

NASA 10 SECR

NASA
SECURITY
RECORDS
SYSTEM

Date: July 20, 2006

The PIA determines what kind of information in identifiable form (IIF), if any, is contained within a system, what is done with that information, and how that information is protected. Systems with IIF are subject to an extensive list of requirements based on privacy laws, regulations, and guidance.

Identifying Numbers (Use N/A for items that are Not Applicable)

Application Name (generally the name that the system is accessed by. www.nasa.gov, when Web enabled, for example):	NASA Security Records System
Application Owner: (Person who is responsible for funding)	Director, Security Management Division, Office of Security and Program Protection Phone Number: 202-358-2010
System Manager (Responsible for system technical operation)	Tim Baldridge Phone Number: 256-544-5314
NASA Cognizant Official: (NASA individual responsible for management of daily operations)	Will Morrison Phone Number: 202-358-2010
Activity/Purpose of Application:	The purposes of this system of records are to: 1. Document security violations and supervisory actions taken. 2. Ensure the safety and security of NASA facilities, systems, or information, and Agency occupants and users. 3. Enable contact with an employee's next-of-kin in the event of a mishap involving the employee. 4. Complete the NASA identity proofing and registration process. 5. Create data records in the Personal Identity Verification (PIV) Identity Management System (IDMS). 6. Issue PIV cards to verify that individuals entering federal facilities, using federal information resources, or accessing classified information are authorized to do so. 7. Track and control issued PIV cards.
Mission Program/Project Supported:	The NASA Security Records Systems supports the Office of Security and Program Protection, as well as the Office of the Chief Information Officer
IT Security Plan Number:	MSFC-0401654

System Location (Center or contractor office building, room, city, and state): Center: George G. Marshall Space Flight Center
Street Address: Bldg 4200/IS50 - Redstone Arsenal
City Huntsville ST AL ZIP 35812

Privacy Act System of Records (SOR) Number: NASA 10 SECR

OMB Information Collection Approval Number and Expiration Date: SF 85 – OMB No. 3206-0005
SF 86 - OMB No. 3206-0007

Other Identifying Number(s): None

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
System Characterization and Data Categorization					
1	**Has/Have any of the major changes listed in the Comments column occurred to the system since April 2003 or the conduct of the last PIA?** **If yes, please check which change(s) have occurred.**	X	☐	☐	☐ Conversions ☐ Anonymous to Non-Anonymous ☐ Significant System Management Changes ☐ Significant Merging ☐ New Public Access ☐ Commercial Sources X Internal Flow or Collection ☐ New Interagency Use ☐ Alteration in Character of Data
2	**Does/Will the system contain Federal records?**	X	☐	☐	
3	**If the system contains/will contain Federal records, under which disposition authority item in the NASA Records Retention Schedules or the General Records Schedules are/will the records be retained and disposed of or archived?**				Schedule Item: NRRS 1/103, 2/4B2, 6/11B, and GRS 18/22a.
4	**Do the records in the system pertain to active programs/projects?**	☐	X	☐	
5	**Are the records Vital records for the organization?**	X	☐	☐	
6	**Are backup files (tapes or other media) being stored off-site?** If yes, please indicate in the comment field where backups are located.	X	☐	☐	Backup storage location: Alternate facility located on Redstone Arsenal, Huntsville, AL.

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
System Characterization and Data Categorization					
7	**Does/Will the system collect and/or *contain (store)* information in identifiable form (IIF) within any database(s), record(s), file(s) or Web site(s) hosted by this system?** Note: If yes, check all that apply in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category. Please note: This question seeks to identify all personal information contained within the system. This includes any IIF, whether or not it is subject to the *Privacy Act*, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the *Privacy Act* or other legislation. . **[Autofill all relevant questions with N/A.]**	X	☐	☐	**Personal Information:** X Name X Date of birth X Social Security Number (or other number originated by a government that specifically identifies an individual) X Photographic identifiers (e.g., photograph image, x-rays, and video) X Driver's license X Biometric identifiers (e.g., fingerprint and voiceprint) ☐ Mother's maiden name X Vehicle identifiers (e.g., license plates) X Mailing address X Phone numbers (e.g., phone, fax, and cell) ☐ Medical records numbers ☐ Medical notes ☐ Financial account information and/or numbers (e.g., checking account number and Personal Identification Numbers [PIN]) X Certificates (e.g., birth, death, and marriage) X Legal documents or notes (e.g., divorce decree, criminal records, or other) ☐ Device identifiers (e.g., pacemaker, hearing aid, or other) ☐ Web Uniform Resource Locators (URL) X E-mail address ☐ Education records ☐ Military status and/or records ☐ Employment status and/or records X Foreign activities and/or interests X Other: Hair & eye color; Citizenship; certificates (visa, et al.) (See also Attachment A.)
8	**Indicate all the categories of individuals about whom IIF is or will be collected.**			☐	X Employees X Public citizens ☐ Patients X Business partners/contacts (federal, state, local agencies) X Vendors/Suppliers/Contractors X Other – Foreign Nationals

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
System Characterization and Data Categorization					
9	**Are records on the system (or will records on the system be) retrieved by one or more data elements?** Note: If yes, specify in the Comments column data elements will be used in retrieving the records (i.e., using a record number, name, social security number, or other data element or record locator methodology). If the category of personal information is not listed, please check "Other" and identify the category.	X	☐	☐	**Personal Information:** X Name X Social Security Number (or other number originated by a government that specifically identifies an individual) ☐ Photographic identifiers (e.g., photograph image, x-rays, and video) X Driver's license ☐ Biometric identifiers (e.g., fingerprint and voiceprint) ☐ Mother's maiden name X Vehicle identifiers (e.g., license plates) ☐ Mailing address X Phone numbers (e.g., phone, fax, and cell) ☐ Medical records numbers ☐ Medical notes ☐ Financial account information and/or numbers (e.g., checking account number and Personal Identification Numbers [PIN]) ☐ Certificates (e.g., birth, death, and marriage) ☐ Legal documents or notes (e.g., divorce decree, criminal records, or other) ☐ Device identifiers (e.g., pacemaker, hearing aid, or other) ☐ Web Uniform Resource Locators (URL) X E-mail address ☐ Education records ☐ Military status and/or records X Employment status and/or records ☐ Foreign activities and/or interests X Other: Citizenship; certificates (visa, et al.)
10	**Are/Will records on 10 or more individuals containing IIF [be] maintained, stored or transmitted/passed through this system?**	X	☐	☐	
11	**Is the system (or will it be) subject to the *Privacy Act*?** Note: If the answer to questions 7, 9, and 10 were yes, the system will likely be subject to the *Privacy Act*. System owners should contact their Center PAM for assistance with this question if they are uncertain of the applicability of the *Privacy Act*.	X	☐	☐	Autofill"yes" when yes is marked for 7 and 9; "no," if 7 and 9 are marked "no."
12	**Has a *Privacy Act* System of Record (SOR) Notice been published in the Federal Register for this system?** Note: If no, explain why not in the Comments column.	X	☐	☐	☐ No IIF is contained in the system. ☐ IIF is in the system, but records are not retrieved by IIF. ☐ Should have published an SOR, but was unaware of the requirement. ☐ System is required to have an SOR but is not yet procured or operational. ☐ Other:_____
13	**If a SOR Notice has been published, have major changes to the system occurred since publication of the SOR?**	X	☐	☐	Revised SORN is being processed concurrently with this PIA.
Information Sharing Practices					
14	**Is the IIF in the system voluntarily submitted (or will it be)?**	X	☐	☐	

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
15	**Does/Will the system *collect* IIF directly from individuals?** Note: If yes, identify in the Comments column the IIF the system collects or will collect directly from individuals. If the category of personal information is not listed, please check "Other" and identify the category.	X	☐	☐	**Personal Information:** X Name X Social Security Number (or other number originated by a government that specifically identifies an individual) X Photographic identifiers (e.g., photograph image, x-rays, and video) X Driver's license X Biometric identifiers (e.g., fingerprint and voiceprint) ☐ Mother's maiden name X Vehicle identifiers (e.g., license plates) X Mailing address X Phone numbers (e.g., phone, fax, and cell) ☐ Medical records numbers ☐ Medical notes ☐ Financial account information and/or numbers (e.g., checking account number and Personal Identification Numbers [PIN]) X Certificates (e.g., birth, death, and marriage) X Legal documents or notes (e.g., divorce decree, criminal records, or other) ☐ Device identifiers (e.g., pacemaker, hearing aid, or other) ☐ Web Uniform Resource Locators (URL) X E-mail address ☐ Education records ☐ Military status and/or records X Employment status and/or records X Foreign activities and/or interests X Other: Hair and eye color, Citizenship; citizenship certificates (visa, et al.),
16	**Does/Will the system *collect* IIF from *other resources* (i.e., databases, Web sites, etc.)?** Note: If yes, specify the resource(s) and IIF in the Comments column.	X	☐	☐	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, co-workers, 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.
17	**Does/Will the system *populate* data for *other resources* (i.e., do databases, Web sites, or other resources rely on this system's data)?** Note: If yes, specify resource(s) and purpose for each instance in the Comments column.	X	☐	☐	X Resource: _NASA Account Management System (NAMS), providing minimal identify and clearance information for control of user access to NASA IT systems. ☐ Resource: _____
18	**Does/Will the system *share* or *disclose* IIF with agencies external to NASA, or other people or organizations outside NASA?** Note: If yes, specify with whom and for what purposes, and identify which data elements in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.	X	☐	☐	With whom and for what purposes: X Federal law enforcement X State law enforcement X Local – law enforcement X Congress – Official Inquiries X White House – Official Inquiries X Routine uses as specified in the Security Records Privacy Act System of Notice (10SECR)

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
19	**If the IIF in the system is or will be matched against IIF in one or more other computer systems internal or external to NASA, are (or will there be) computer data matching agreement(s) in place?** **If yes**, indicate in the Comments column internal or external and the system(s) with data which are matched.	☐	☐	X	Location of other systems involved in matching: ☐ Internal NASA ☐ External to NASA Other systems involved: _____ _____ If answered "No," auto fill 20 with N/A.
20	**If data matching activities will occur, will the IIF be de-identified, aggregated, or otherwise made anonymous?** Note: If yes, please describe this use in the Comments column.	☐	☐	X	☐ De-identified ☐ Aggregated ☐ Other
21	**Is there a process, either planned or in place, to notify organizations or systems that are dependent upon the IIF contained in this system when changes occur (i.e., revisions to IIF, when the system encounters a major change, or is replaced)?**	X	☐	☐	
22	**Is there a process, either planned or in place, to notify and obtain consent from the individuals whose IIF is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of the original collection)?**	X	☐	☐	Should any changes occur, individuals will be notified by an updated SORN in the Federal Register.
23	**Is there/Will there be a process in place for individuals to choose how their IIF data is used?** Note: If yes, please describe the process for allowing individuals choice in the Comments column.	☐	X	☐	Process:_____ _____ _____ _____
24	**Is there/Will there be a complaint process in place for individuals who believe their IIF has been inappropriately obtained, used, or disclosed, or that the IIF is inaccurate?** Note: If yes, please describe briefly the notification process in the Comments column.	X	☐	☐	Process:_Individuals may address information corrections via procedures provided in 14 CFR 1212. _____ _____
25	**Are there or will there be processes in place for periodic reviews of IIF contained in the system to ensure the data's integrity, availability, accuracy, and relevancy?** Note: If yes, please describe briefly the review process in the Comments column.	X	☐	☐	Information accuracy is reviewed every 5 years upon PIV card re-issuance.

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
26	**Are there/Will there be rules of conduct in place for access to IIF on the system?** Note: If yes, identify in the Comments column all users with access to IIF on the system and for what purposes they use the IIF.	X	☐	☐	X Users X Administrators X Developers X Contractors For what purposes: The routine performance of their assigned duties. Rules of conduct specified in Section 5.24 of NPR 1600.1 NASA Security Program Procedural Requirements.
27	**Is there a process in place to log routine and non-routine disclosures and/or unauthorized access?** **If yes**, check in the Comments column which kind of disclosures are logged.	X	☐	☐	Disclosures logged: X Routine X Non-routine ☐ Public Internet_____
	Web site Host – Question Sets				
28	**Does/Will the system host a Web site?** Note: **If yes**, identify what type of site the system hosts in the Comments column. **If no**, check "No" for all remaining questions in the "Web Site Host Question Sets" section and answer questions starting with the "Administrative Controls" section beginning with question 42.	X	☐	☐	Type of site: ☐ Public Internet_____ X Internal NASA _____ ☐ Both_____
29	**Is the Web site (or will it be) accessible by the public or other entities (i.e., federal, state, and local agencies, contractors, third-party administrators, etc.)?**	☐	X	☐	
30	**Is the Agency Web site privacy policy statement posted (or will it be posted) on the Web site?**	X	☐	☐	
31	**Is the Web site's privacy policy in machine-readable format, such as Platform for Privacy Preferences (P3P)?** Note: If no, please describe in the Comments column your timeline to implement P3P requirements for this system.	☐	X	☐	Planned implementation P3P requirements 10/30/2006

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
32	**Does the Web site employ (or will it employ) persistent tracking technologies?** Note: If yes, identify types of cookies in the Comments column. If persistent tracking technologies are in place, please indicate the official who authorized the use of the persistent tracking technology.	☐	X	☐	☐ Session Cookies ☐ Persistent Cookies ☐ Web bugs ☐ Web beacons ☐ Other (Describe): _____ Authorizing Official: Authorizing Date:
33	**Does/Will the Web site collect or maintain personal information from or about children under the age of 13?**	☐	X	☐	If marked "No," autofill "N/A" in next question.
34	**If the Web site does/will collect or maintain personal information from or about children under the age of 13, please indicate what information and how the information is collected.**			X	☐ Actively directly from the child ☐ Passively through cookies ☐ Both of the above What Information collected: _____ _____ _____
35	**If the Web site does/will collect or maintain personal information from or about children under the age of 13, is the information shared with any non-NASA organizations, grantees, universities, etc.** Note: If yes, also identify the non-NASA organizations in the comments field	☐	☐	X	Information is shared with: _____ _____ _____ If "no," autofill "N/A" in items 36 & 37.
36	**If the Web site does/will collect or maintain personal information from or about children under the age of 13, specify in the comments field what method is used for obtaining parental consent.**			X	Method used for obtaining parental consent (please check all that apply) ☐ No consent is obtained ☐ Simple email ☐ email accompanied by digital signature ☐ signed form from the parent via postal mail or facsimile ☐ accepting and verifying a credit card number in connection with a transaction ☐ taking calls from parents, through a toll-free telephone number staffed by trained personnel

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
37	**Does/Will the Web site *collect* IIF electronically from any individuals?** Note: If yes, identify what IIF the system collects in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.	X	☐	☐	**Personal Information:** X Name X Date of birth X Social Security Number (or other number originated by a government that specifically identifies an individual) ☐ Photographic identifiers (e.g., photograph image, x-rays, and video) X Driver's license ☐ Biometric identifiers (e.g., fingerprint and voiceprint) ☐ Mother's maiden name X Vehicle identifiers (e.g., license plates) X Mailing address X Phone numbers (e.g., phone, fax, and cell) ☐ Medical records numbers ☐ Medical notes ☐ Financial account information and/or numbers (e.g., checking account number and Personal Identification Numbers [PIN]) ☐ Certificates (e.g., birth, death, and marriage) ☐ Legal documents or notes (e.g., divorce decree, criminal records, or other) ☐ Device identifiers (e.g., pacemaker, hearing aid, or other) ☐ Web Uniform Resource Locators (URL) X E-mail address ☐ Education records ☐ Military status and/or records ☐ Employment status and/or records ☐ Foreign activities and/or interests X Other: Hair & eye color; Citizenship (See also Attachment A.)
38	**Does/Will the Web site provide a PDF form to be completed with IIF from any individuals and then mailed or otherwise provided to NASA?** Note: If yes, identify what IIF the PDF form collects in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.	☐	X	☐	**Personal Information:** ☐ Name ☐ Date of birth ☐ Social Security Number (or other number originated by a government that specifically identifies an individual) ☐ Photographic identifiers (e.g., photograph image, x-rays, and video) ☐ Driver's license ☐ Biometric identifiers (e.g., fingerprint and voiceprint) ☐ Mother's maiden name ☐ Vehicle identifiers (e.g., license plates) ☐ Mailing address ☐ Phone numbers (e.g., phone, fax, and cell) ☐ Medical records numbers ☐ Medical notes ☐ Financial account information and/or numbers (e.g., checking account number and Personal Identification Numbers [PIN]) ☐ Certificates (e.g., birth, death, and marriage) ☐ Legal documents or notes (e.g., divorce decree, criminal records, or other) ☐ Device identifiers (e.g., pacemaker, hearing aid, or other) ☐ Web Uniform Resource Locators (URL) ☐ E-mail address ☐ Education records ☐ Military status and/or records ☐ Employment status and/or records ☐ Foreign activities and/or interests ☐ Other:_____

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
39	**Does/Will the Web site *share* IIF with organizations external to NASA, or other people or organizations outside NASA?** Note: If yes, specify with whom and for what purposes.	☐	X	☐	
40	**Are rules of conduct in place (or will they be in place) for access to IIF on the Web site?** Note: If yes, identify in the Comments column all categories of users with access to IIF on the system, and for what purposes the IIF is used.	X	☐	☐	X Users X Administrators X Developers X Contractors For what purposes: Official duties.
41	**Does (or will) the Web site contain links to sites external to the Center that owns and/or operates the system?** Note: If yes, note in the Comments column whether the system provides a disclaimer notice for users that follow external links to Web sites not owned or operated by the Center.	☐	X	☐	☐ Disclaimer notice for all external links
	Administrative Controls				
42	**Have there been major changes to the system since it was last certified and accredited?** Note: If the system is under development and not yet certified and accredited at the time of this PIA, please describe in the Comments column the plan and timeline for conducting a certification and accreditation (C&A) for this system.	☐	X	☐	
43	**Have personnel (system owners, managers, operators, contractors and/or program managers) using the system been (or will they be) trained and made aware of their responsibilities for protecting the IIF being collected and maintained?**	X	☐	☐	
44	**Who has /will have access to the IIF on the system?** Note: Check all that apply in the Comments column.				X Users X Administrators X Developers X Contractors ☐ Other
45	**If contractors operate or use the system, do the contracts include clauses ensuring adherence to privacy provisions and practices?**	X	☐	☐	Numerous contracts across the agency access the database containing the IIF. FAR PA Clause 52.224-1 & 2 are germane.

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
46	**Are methods in place to ensure that access to IIF is restricted to only those required to perform their official duties?** Note: If yes, please specify method(s) in the Comments column.	X	☐	☐	Each individual accessing the system must be approved either by the system program administrator, or the system manager, and controlled by user ID's and passwords
47	**Are there policies or guidelines in place for the retention and destruction of IIF within the application/system?** Note: If yes, please provide some detail about these policies/practices in the Comments column.	X	☐	☐	
	Technical Controls				
48	**Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system (or will there be)?**	X	☐	☐	
49	**Are any of the password controls listed in the Comments column in place (or will they be)?** Note: Check all that apply in the Comments column.	X	☐	☐	X Passwords expire after a set period of time. X Accounts are locked after a set period of inactivity. X Minimum length of passwords is eight characters. X Passwords must be a combination of uppercase, lowercase, and special characters. X Accounts are locked after a set number of incorrect attempts.
50	**Is there (or will there be) a process in place to monitor and respond to privacy and/or security incidents?**	X	☐	☐	
	Physical Controls				
51	**Are physical access controls in place (or will they be)**	X	☐	☐	
	- END -				

_____	July 20, 2006
Signature of Application Official	***Date***
Phillip A. Bounds	Acting Director, Security Management Division
Print Name	***Title/Position***

NASA HQ, Office of Security and Program Protection
Center and Office/Department

300 E. Street, SW
Street Address

9Q80
Street Address

Washington, DC 20546-0001
City, State and Zip Code

202-358-2010	**202-358-3238**
Phone Number	***Fax Number***

*** Please go to the next page and complete the PIA Summary. This Summary will be made publicly available at http://www.NASA.gov/pia.***

Privacy Impact Assessment (PIA) Summary

Date of this Submission (MM/DD/YYYY): July 20, 2006

NASA Center: NASA Headquarters

Application Name: NASA Security Records System

Is this application or information collection new or is an existing one being modified? Existing

Does this application collect, maintain, and/or disseminate information in identifiable form (IIF)? Yes

Mission Program/Project Supported: NASA Office of Security and Program Protection /
NASA Office of the Chief Information Officer

Identifying Numbers (Use N/A, where appropriate)

Privacy Act System of Records Number: NASA 10 SECR

OMB Information Collection Approval Number and Expiration Date: SF 85 – OMB No. 3206-0005, SF 86 - OMB No. 3206-0007
Other Identifying Number(s): N/A

Description

1. Provide an overview of the application or collection and indicate the legislation authorizing this activity.

   The National Aeronautics and Space Administration Security Records System is a Privacy Act system of records to document, track, manage, analyze, and/or report on individuals accessing NASA resources. Routine uses of this system of records will be to determine eligibility to access classified national security information; to maintain a record of identification documentation provided to NASA as proof of an individual's identity; to establish contact with an employee's next-of-kin in the event of a mishap involving the employee; to provide personal identifying data to Federal, State, local or foreign law enforcement representatives seeking confirmation of identity of persons under investigation.

   Authority for this activity is derived from: 42 U.S.C. 2451, et seq., the National Aeronautics and Space Act of 1958, as amended; Espionage and Information Control Statutes, 18 U.S.C. 793-799; Sabotage Statutes, 18 U.S.C. 2151--2157; Conspiracy Statute, 18 U.S.C. 371; 18 U.S.C. 202-208, 3056; Internal Security Act of 1950; Atomic Energy Act of 1954, as amended; Executive Order 12958, 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; 5 U.S.C. 552a, Privacy Act of 1974; E-Government Act of 2002; Federal Information Security Management Act 2002 41 CFR Chapter 101; 14 CFR parts 1203-1203b; 44 U.S.C. 3101; and Homeland Security Presidential Directive 12; Federal Information Processing Standard 201: Policy for a Common Identification Standard for Federal Employees and Contractors.

   (See Federal Register System of Record Notice (SORN) NASA 10 SECR)

2. Describe the information the agency will collect, maintain, or disseminate and how the agency will use the information. In this description, indicate whether the information contains IIF and whether submission is voluntary or mandatory.

   Records in this system include information about the individuals seeking access to NASA resources. Information about an individual may include, but is not limited to: name, home address, place of birth and citizenship, U.S. visitor/travel document numbers, employment information, Tax Identification Numbers (Social Security Number), description of the individual (height, weight, hair color, et al.) Submission of requested information is voluntary.

   The records in this system of records are intended for the sole use of the U.S. Government and its contractors who support U.S. Government operations, policies, laws and regulations, as well as State, local and foreign law enforcement representatives seeking confirmation of identity of persons under investigation.

   The Agency will use the information to conduct and document security violations and supervisory actions; ensure the safety and security of NASA facilities, systems, or information, and Agency occupants and users; enable contact with an employee's next-of-kin in the event of a mishap involving the employee; complete the NASA identity proofing and registration process; create data records in the Personal Identity Verification (PIV) Identity Management System (IDMS); issue PIV cards to verify that individuals entering federal facilities, using federal information resources, or accessing classified information are authorized to do so; track and control issued PIV cards.

   Although fingerprints are collected, they are at once electronically transmitted to the Federal Bureau of Investigation (FBI) as part of a background investigative package in accordance with 42USC14616. Further, as required by FIPS-201 (Personal Identity Verification (PIV) of Federal Employees and Contractors), the fingerprints are encoded on the PIV card and held in an encrypted container. Immediately upon fulfilling these two requirements, NASA purges the collected fingerprints from the system. Thus, NASA does not maintain any fingerprints in any database, or any other system. Should a PIV card become lost, or damaged, biometrics must be recaptured because they are not stored in any NASA system.

   See Federal Register System of Record Notice (SORN) NASA 10 SECR and Attachment A to this PIA.

3. Is submission of the IIF mandatory?

No. Submission of requested information is voluntary. Failure to submit requested information could result in NASA's inability to fulfill Agency requirements as set forth in Federal Information Processing Standards Publication 201 (FIPS-201), and could result in the individual's request for access to NASA physical and/or Information Technology resources being turn down.

4. Explain how the IIF collected, maintained, and/or disseminated is the minimum necessary to accomplish the purpose for this effort.

   The information is collected directly from the individual. To achieve the objectives of the system, only the IIF information necessary to positively identify an individual; perform national criminal database checks; identify emergency notification information; and to maintain a history of traffic incidents on NASA facilities is obtained from individuals. This information may be shared with other Federal, State, local and foreign government agencies only as authorized by applicable laws and regulations.

   See Federal Register System of Record Notice (SORN) NASA 10 SECR

5. Is a Privacy Act notice provided to the individual at the time information is collected? Yes
   If yes, provide or attach the Privacy Act Statement. If notice is not provided, why not? The Privacy Act notice is currently being revised to ensure greater adequacy.

   Privacy Act Notice

   General - Pursuant to the, Privacy Act of 1974, as amended (5 U.S.C. 552a), and the National Aeronautics and Space Act, 42 U,S.C. § 2451 et seq., the following information is being solicited and collected for use in conjunction with the NASA Security Records System know as NASA 10SECR.

   Authority - The National Aeronautics and Space Act (42 U.S.C. 2455, Section 304(a)).

   Purposes and Uses - The primary use of information collected on this form will be for the issuance of NASA badges. In addition, state, local, or Congressional offices which have a need to know in connection with program oversight or when relevant to civil, criminal, administrative, or regulatory investigations or proceedings. Additional uses are set forth and published in 10SECR at 49 FR 39742 (Dec. 13, 1999) and the standard uses as listed in Appendix B.

   Effect of Nondisclosure - Failure to provide your Social Security Number (SSN) will result in NASA's inability to issue an Agency identification badge, as required under NPD 1600 "NASA Security Policy." This may result in your disqualification from performing particular work or duty assignments, or from the position that you currently hold. Disclosure of your SSN is MANDATORY in order to obtain a NASA badge. Executive Order 9397 authorizes the use of the SSN to distinguish between you and other people who may have identical names and birth dates. The SSN will be used to match the person completing this form with the correct individual master record currently maintained in NASA 10SECR.

6. Explain why the IIF is being collected, maintained, or disseminated.

   Records are being collected and maintained pursuant to Homeland Security Presidential Directive 12 to provide positive identification of individuals who access NASA physical and information technology resources, to include NASA Headquarters, Field Offices, National Laboratories, Federally Funded Research and Development Centers, Contractor Sites, components facilities (NASA Management Office, Wallops Flight Facility, White Sands Test Facility, White Sands Complex, Independent Validation & Verification Facility, Michoud Assembly Center, Moffett Federal Airfield, Goldstone Deep Space Communications Complex, Goddard Institute for Space Studies, National Scientific Balloon Facility, Plum Brook Station).

   The IIF information is only disseminated to other government agencies as authorized by applicable laws and regulations for purposes outlined below and provided in the Routine Uses of the SORN.

   (See Federal Register System of Record Notice (SORN) for NASA 10 SECR.)

7. Identify with whom the agency will share the IIF.

   Routine uses of the records containing IIF are as follows:

   A record from this system may be disclosed to:

   - To the Department of Justice when: (a) the agency or any component thereof; or (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 by DOJ is therefore deemed by the agency to be for a purpose compatible with the purpose for which the agency collected the records.
   - 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.
   - Except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, or otherwise, responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order

issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutorial responsibility of the receiving entity.

- To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.
- To a staff member of the Executive Office of the President in response to an inquiry from the White House.
- 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.
- 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.
- To other Federal agencies and relevant contractor facilities to determine eligibility of individuals to access classified National Security information.
- To any source or potential source from which information is requested in the course of an investigation concerning the retention of an employee or other personnel action (other than hiring), or the retention of a security clearance, contract, grant, license, or other benefit, 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.
- 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.
- To a Federal State, local, foreign, or tribal or other public authority the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative personnel or regulatory action.
- 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.
- 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.
- To notify another federal agency when, or verify whether a PIV card is longer valid.

See Federal Register System of Record Notice (SORN) NASA 10 SECR

8. Describe how the IIF will be obtained, from whom it will be collected, what the suppliers of information and the subjects will be told about the information collection, and how this message will be conveyed to them (e.g., written notice, electronic notice if a Web-based collection, etc.). Describe any opportunities for consent provided to individuals regarding what information is collected and how the information will be shared.

   The IIF will be solicited directly from the individual. The individual will be advised of the authority and purposes for collecting this information as stated in 1-5 above. The information may be provided in written form, usually by the use of an approved OMB Standard Form (e.g., SF-85, SF-85P or SF-86). Individuals grant consent to the collection by providing the requested information.

   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, co-workers, 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.

9. State whether personal information will be collected from children under age 13 on the Internet and, if so, how parental or guardian approval will be obtained. (Reference: *Children's Online Privacy Protection Act of 1998*)

   Information will not be collected from children.

10. Describe how the IIF will be secured.

    The IIF will be secured using procedures set forth in NIST SP 800-18, NIST SP 800-53 and NIST SP 800-30.

11. Describe plans for retention and destruction of IIF.

    NASA Records Retention Schedule (NRRS) 1/Item 103, NRRS 2/Item 4B2, NRRS 6/Item 11B, and General Records Schedule 18/Item 22a provide for the retention of the records for a period not to exceed 5-years from termination date. At that point, the records will be removed from the system, and all media with the data either overwritten or destroyed.

12. Identify whether a system of records is being created under section 552a of Title 5, United States Code (the *Privacy Act)*, or identify the existing Privacy Act system of records notice under which the records will be maintained.

    NASA 10 SECR is being updated.

13. Identify the procedures individuals must follow to gain access to their own information:

Individuals should follow the Record Access Procedures specified in NASA 10SECR. Specifically, 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 in NASA 10SECR.

Emergency Data Records: Requests from individuals should be addressed to the same address as stated in the Notification section in NASA 10SECR.

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 in NASA 10SECR.

14. What are the procedures for correcting information?

Procedures are specified in 14 CFR.1212.

15. Do individuals have the right to consent to particular uses of the information?

Through the NASA Systems of Record Notice (NASA 10 SECR) published in the Federal Register and the Privacy Act Statement provided at the time data are collected, NASA has informed individuals of the purpose of its collection. By providing the information, the individual concurs with the uses of the information as published in the Federal Register and this PIA. Individuals are not given the ability to determine individual uses for the information collected.

16. Data Protection Controls

General Program Controls

- NASA has detailed badge/card issuance procedures which has been approved by the headquarters Office of Security and Program Protection (OSPP), and distributed to each Center/facility issuing badges/cards.
- The applicant appears in-person at least once before the issuance of a badge/credential.
- The identity proofing, registration and issuance process adheres to the principle of separation of duties to ensure that no single individual has the capability to issue a credential without the cooperation of another authorized person.
- NASA issues badges/credentials only through systems whose reliability has been established by the agency and so documented and approved in writing.
- A comprehensive PIA is conducted on systems containing personal information in identifiable (IIF) form for implementing PIV, consistent the E-Government Act.
- NASA has generated a SORN identifying the type of information collected, the purpose of the collection, how the information is protected, and the complete set of uses of the credential and related information during the life of the credential.
- NASA assures that systems containing IIF for the purpose of enabling the implementation of PIV are handled in full compliance with the Privacy Act.
- NASA ensures that only personnel with a legitimate need for access to IIF are authorized to access the IIF, including but not limited to information and databases maintained for registration and credential issuance.
- NASA coordinates with appropriate department or agency officials to define consequences for violating privacy policies of the PIV program.
- NASA has categorized the system risk level (as specified in FIPS 199) and utilizes security controls described in NIST SP800-53, Recommend Security Controls for Federal Information Systems, to accomplish privacy goals, where applicable.

What are the controls on data exchange and integrity of the credential?

The agency follows all applicable government-wide standards for controlling and protecting information systems (see NIST SP800-53). Specific controls are described below.

System security: The controls include network security and limited access to system and physical facilities. Program controls include protecting data through the use of FIPS validated cryptographic algorithms in transit, processing and at rest.

Networks: The IT infrastructure that supports security programs is described in detail in associated IT Security Plans. All data exchange takes place over encrypted data communication networks that are designed and managed specifically to meet the needs of the Security program. Private networks and or encryption technologies are used during the electronic transfer of information to ensure “eavesdropping” is not allowed and that data is sent only to its intended destination and to an authorized user, by an authorized user.

Data Transmission: All data transmissions associated with IIF are protected by NIST SP 800-37 & NIST SP 800-53 approved procedures.

Data Storage Facilities: Facilities and equipment are secured by limiting physical access to the workspace and system, and by requiring an appropriate verification of identity for logical access to the system.

Equipment: User Identification: PIV cardholders are authenticated to access the PIV system using, at a minimum, two-factor authentication based on their role and responsibility. A required component (first factor) of this authentication is the PIV card itself. In combination with the PIV, the second factor of this authentication requires a personal ID number (PIN), and/or biometric (e.g., fingerprint).

- User Groups: System/application users have varying levels of responsibility and are only allowed to access information and features of the system appropriate for their level of job responsibility and security clearance. These rights are determined by the identification provided when authenticating (i.e., user identification) to the system as described above.
- Network Firewall: Equipment and software are deployed to prevent intrusion into sensitive networks and computers.
- Encryption: Sensitive data are protected by rendering it unreadable to anyone other than those with the correct keys to reverse the encrypted data.
- Access Control: Access to data is PIN protected.
- Audit Trails: Attempts to access sensitive data are recorded for forensic purposes if an unauthorized individual attempts to access the information contained within the system.
- Recoverability: The system is designed to continue to function in the event that a disaster or disruption of service should occur.
- Physical Security: Measures are employed to protect enrollment equipment, facilities, material, and information systems that are part of the PIV program. These measures include: locks, ID badges, fire protection, redundant power and climate control to protect IT equipment that are part of the PIV program.
- An Information Assurance and Security plan containing all technical measures and operational procedures consistent with federal law, FIPS 201, related Special Publications and agency policy.
- System users/operators are officially designated as agents of the specific NASA facility and complete a training process associated with their specific role in the PIV process.

Separation of Duties Controls: As specified by NIST SP 800-79, duties associated with the issuance of badges/credentials meeting FIPS-201 requirements are separated to insure roles do not overlap.

- Security of ID credential issued to an employee or contractor is achieved by full compliance with the mandatory requirements of the Federal Information Processing Standard Publication 201 (FIPS Pub 201), Personal Identity Verification of Federal Employees and Contractors. Specific safeguards include:
  - Card issuing authority limited to providers with official accreditation pursuant to NIST Special Publication 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations
  - Cards use at least one visual tamper proof feature such as holograms, watermarks, etc.
  - Card data is encrypted and stored on the card
  - Employees are alerted to importance of protecting card
  - Card expiration within 5 years from issuance
  - Return of cards to agency when no longer needed (or upon employee/contractor separation from the agency)
  - Deactivation of card within 18 hours (the latest) of employee/contractor separation, loss of card, or expiration
  - Removal of all IIF associated with the cardholder from the system upon deactivation.
  - Specialized role-based training for all persons involved in the PIV process

Who will have access to the information?

Individuals listed in questions 18 and 40 of this PIA who include authorized information technology (IT) personnel or contractors (pursuant to an appropriate routine use) who handle the operations and maintenance of the system will have limited access to the system to support the credentialing activity as well as trouble shoot technical system issues encountered on a day-to-day basis. Additionally, as authorized by Section (b) (1) of the Privacy Act, disclosures may be made to officers and employees of the Agency which maintains the record who have a need for the record in the performance of their duties.

Are written procedures in place identifying who may access the system?

All NASA employees and assigned contractor staff with access to security systems containing IIF will receive appropriate privacy and security training, and have any necessary background investigations and/or security clearances for access to sensitive, privacy or classified information or secured facilities. Personnel will only have access to IIF information as part of their official duties within NASA and must first be approved by the Center Chief of Security prior to being granted access.

What technical and/or operational controls are in place to prevent misuse of data by those having access?

By design, and for security and privacy reasons, no enrollment data is stored at or by the enrollment workstation or center. The enrollment record can only be viewed or retrieved by a NASA enrollment official or PIV issuer who is trained and authorized to perform enrollment activities. The ability to retrieve or view an employee's enrollment record is controlled by user authentication, which ensures only those with a need to access the data and who possess proper training can retrieve or view enrollment information. In addition to this access control, physical privacy protections will be used. These physical protections include the use of "Privacy Screens" that prevent passers-by from viewing enrollment record information that may be displayed on the enrollment center workstation. Additionally, the enrollment center's physical security controls will be enforced to ensure that only NASA employment officer or PIV issuer with a need for access can enter the enrollment center and view personal information displayed on screens.

17. What decisions were made concerning this system as a result of conducting this assessment?

The storage location for system backup files is under reconsideration.
Update Privacy Act Statement provided to individuals at the time of information collection.

Contingent on the elements listed above and the satisfaction of all applicable Directives, OMB Guidance, and NIST standards and requirements, the privacy controls related to the system this PIA covers is considered adequate.

_____
Phillip A. Bounds
Acting Director, Security Management Division,
NASA HQ Office of Security and Program Protection

Date ___July 20 , 2006_____

Concur:

_____
Patti F. Stockman
NASA Privacy Act Officer

Date: _____

Concur:

_____
Scott Santiago
Deputy CIO for IT Security

Date: _____

Approved for Publication:

_____
John W. McManus
Acting, Chief Information Officer

Date: _____