Privacy Impact Assessment

Name of Project: NARS-5/Center Information Processing System (CIPS)/Space Information System (SIS)
Project's Unique ID: AAC

Legal Authority(ies): 44 U.S.C. 2108,2110, and 2907

Purpose of this System/Application:
NARS-5, CIPS, and SIS are three of several National Archives and Records Administration (NARA) applications housed at the Department of Veteran's Affairs (VA) Austin Automation Center (AAC) located in Austin, TX.

NARS-5. NARS-5 is an automated system for the control of records in Federal Records Centers (FRCs). NARS-5 is designed to document and control the retirement, processing, storage, and servicing of records in the physical custody of the Federal Records Centers (FRCs), that are pending accession into the National Archives or disposition in any other manner prescribed by law. The system is intended to: 1) ensure the orderly accessing and subsequent retrieval of records, 2) facilitate timely review of disposition of records, and 3) provide various statistical profiles of records holdings for more cost-effective control and planning.

Center Information Processing System (CIPS). The primary function of the CIPS system is to allow FRC customers - various departments and agencies of the federal government - to submit reference requests electronically to the FRC via a web-based interface or dial-up connection to retrieve records created by their offices that are stored at the FRC.

Space Information System (SIS). SIS is a management and tracking application used to control the shelf space at the various FRCs. It is directly related to the acceptance and storage of transfers (i.e., groups of records belonging to federal government agencies and stored by NARA). NARS-5 provides the information about the records and the SIS application allocates and tracks specific shelf space for the records.

Section 1: Information to be Collected

1. Describe the information (data elements and fields) available in the system in the following categories:

This system contains two general categories of information about individuals:

- Employees: Information about NARA Federal Record Center (FRC) employees who access the system to perform their jobs.
- External Users: Information about Federal Government employees who use the system to request access to Federal records stored in a NARA operated FRC.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?

The information that is collected includes: name, official title, mailing address of employee's official duty station, office telephone and fax number and email address.

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.

Yes. The data that is collected about individuals is used to authorize access to the system. The system stores the users name, password, and information regarding the user's ability to conduct transactions and access data.

2. Is there another source for the data? Explain how that source is or is not used?

No.

Section 3: Intended Use of this Information

1. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?
No.

2. Will the new data be placed in the individual's record?

N/A

3. Can the system make determinations about employees/the public that would not be possible without the new data?

N/A

4. How will the new data be verified for relevance and accuracy?

N/A

5. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

N/A

6. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

N/A

7. Generally, how will the data be retrieved by the user?
The user logs into the system and is validated through password control. Log in controls limit the data viewable by the user. The user retrieves data through a set of predefined reports and queries that are contained within the application.
The data is retrievable by user name. In addition each user has a unique password; however, this number is not considered a personnel identifier outside of this system.

8. Is the data retrievable by a personal identifier such as a name, SSN or other unique identifier? If yes, explain and list the identifiers that will be used to retrieve information on an individual.

N/A - The system maintains information about records stored at the FRCs, not information on individuals.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Data in the system is used to determine the physical location of paper records in an FRC. Any reports will be used to locate boxes within the stacks, to identify the location from which a box was pulled and to provide information concerning the office (internal or external) to which a box was sent.

10. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain.

No

11. Will this system be used to identify, locate, and monitor individuals? If yes, describe the business purpose for the capability and the controls established explain.

No

12. What kinds of information are collected as a function of the monitoring of individuals?

N/A

13. What controls will be used to prevent unauthorized monitoring?

The AAC has in place a set of extensive controls to prevent unauthorized monitoring. These controls are documented in the Report on Controls placed in Operation and Tests of Operating Effectiveness (SAS 70) dated September 5,2006. This report was completed by Independent Auditor KPMG (copy available upon request).

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?

N/A

Section 4: Sharing of Collected Information

1. Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?

AAC System Administrators, authorized Federal employee users, managers, on-site system administrators and developers.
The data in the system (except user information) is considered public information and is available to any requester. The NARS-5 data itself does not contain any information that would be protected from public disclosure pursuant to the provisions of the Privacy Act or FOIA.

2. How is access to the data by a user determined and by whom? Are criteria, procedures, controls, and responsibilities regarding access

documented? If so, where are they documented (e.g., concept of operations document, etc.).

Routine users access the data through a log in procedure. Routine users must enter a unique identifier and password. The password is changed every 90 days. Three incorrect log in attempts will disable the log in user until recertified. Non-routine users request data on an ad hoc basis to through the Office of Regional Records Services via letter, fax, phone or email.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

Users are restricted to data appropriate to their needs. For example, an agency user would only view data that is relevant to their agency; a FRC user would view data relevant to the specific record center.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those who have been granted access (please list processes and training materials)?
The AAC has in place a set of extensive controls to prevent unauthorized monitoring. These controls are documented in the Report on Controls placed in Operation and Tests of Operating Effectiveness (SAS 70) dated September 5,2006. This report was completed by Independent Auditor KPMG (copy available upon request).

5. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

The system is mature and is not undergoing any changes at this time. NARA has contracted with the Department of Veterans Affairs - Austin Automation Center (AAC) for operation and maintenance. The AAC has extensive contract clauses inserted in contracts to ensure proper handling of the data.

6. Do other NARA systems provide, receive or share data in the system? If yes, list the system and describe which data is shared. If no, continue to question 7.

Data is not received from other NARA systems.

Several NARA organizations receive reports containing data extracted from this application. Since the data is not restricted, we have not established formal

Interchange Security Agreements, and, therefore, cannot identify the specific systems, if any, that use this data.

7. Have the NARA systems described in item 6 received an approved Security Certification and Privacy Impact Assessment?

N/A

8. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

The NARS5/CIPS/SIS system owner, individual users and AAC administrator and staff are responsible for managing and securing any personal data that resides in the system.

9. Will other agencies share data or have access to the data in this system (Federal, State, Local, or Other)? If so list the agency and the official responsible for proper use of the data, and explain how the data will be used.

Many Federal agencies receive automated reports that contain data extracts of data from this system, however, the data that is provided does not contain any privacy restricted information.

Section 5: Opportunities for Individuals to Decline Providing Information

1. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?

N/A. Individual users must provide their unique login information to gain access to the system.

2. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

N/A

Section 6: Security of Collected Information

1. How will data be verified for accuracy, timeliness, and completeness? What steps or procedures are taken to ensure the data is current? Name the document that outlines these procedures (e.g., data models, etc.).

Centers Information Processing System Users Manual provides instructions for requesting access CIPS. All users must be revalidated annually and passwords must be changed every 90 days.

2. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The system operates at the Department of Veteran's Affairs (DVA) Austin Automation Center (AAC). Users access the system from many sites, however, all data is retained at the AAC.

3. What are the retention periods of data in this system?

NARS-5/CIPS/SIS data is scheduled in NARA Records Disposition Schedule, FILES 203 Appendix 13.

NARS-5 System		
	Automated accession control system used for administrative tracking and control of accessions into, movement within, and disposal or transfer of records from a records center. The system also provides statistical information and "space available" information through the "Space Information System" (SIS) subsystem (See file no. 1326-2[d]).	
1326-1	Forms and reports, documenting input actions to NARS-5, such as: NA Form 13116, Records Center Holdings Control Input; NA Form 13117, Mass Data Change Worksheet; Disposal Accomplished Report (Report 88); and Disposal Change Report (Report 89).	• If used as input source documentation for RCPBS: Cut off at end of fiscal year. Destroy when 3 years old. (N1-64-05-9, item 1) • Otherwise:

		Cut off annually. Destroy when 1 year old or when no longer needed for administrative purposes, whichever is sooner. (N1-64-87-1)
1326-2	NARS-5 output reports.	
	a. Feeder reports used to prepare summary reports, including One Time/Special Inquiry Reports: Reports 04, 05, 08, 09, 10, 15, 16, 17, 18, 35, 36, 44, and 45.	Destroy when no longer needed to prepare the summary report or 3 months after close of fiscal year. (N1-64-87-1)
	b. Edit reports of input errors, including Transaction Validity Error Report (Report 19), Transaction Logical Error Report (Report 20), and SIS Error Cycles 2 and 3 reports.	Destroy after corrections have been made to the transaction file. (N1-64-87-1)
	c. NARS-5 periodic reports.	
	(1) Monthly reports: Accession Number Master List (Report 01); Record Group Profile (Summary) Listing (Report 02); and Records Center Profile (Summary) Listing (Report 03).	Destroy when superseded. (N1-64-87-1)
	(2) Semiannual and annual (FY) reports: Record Group Profile (Summary) Listing (Report 02); Records Center Profile (Summary) Listing (Report 03); Stack Sequence Report (Report 06); Location Report (Report 07); Annual Report of Holdings and Disposals by Record Group (Report 24); Retention Report (Report 37); and Auditors Report (Report 43).	Cut off annually and destroy when 1 year old or when no longer needed for administrative purposes, whichever is longer. (N1-64-87-1)
	(3) NARS-5 history reports: Withdrawal Report (Report 11) and Withdrawal Report 2 (Report 21).	Destroy when no longer needed for reference purposes. (N1-64-87-1)
	(4) NARS-5 edit files: IVF Update	Destroy when superseded. (N1-

	Report (Report 28) and Disposal Authority Master List.	64-87-1)
	(5) Disposal pull list: Copy of Disposal Approved Report (Report 22), annotated with signed certification indicating that disposal records were removed from the shelves and, where required, that the destruction of the records was witnessed; and Disposal Concurrence Report (Report 23).	Cut off at the end of fiscal year in which the disposal is accomplished. Destroy when 10 years old. (N1-64-87-1)
	d. Space Information System (SIS): Reserve Master Listings, Available Space by Location Report, and Available Space by Volume Report.	Destroy when superseded. (N1-64-87-1)
1326-3	Automated Files.	
	a. Program and documentation files consisting of machine instructions designed to add or retrieve information to or from specific data systems and related written documentation files.	
	(1) Files maintained at records centers.	Overwrite when modified or destroy when no longer in use. (N1-64-87-1)
	(2) Files maintained by NHTR.	Destroy when modified or 5 years after program is no longer in use. (N1-64-87-1)
	b. Intermediate input-output files consisting of data that is manipulated, sorted, or moved from one computer run to a subsequent run and is used in the process of updating a master file.	Delete after information has been transferred to the master file and verified. (GRS 20, item 1b)
	c. Master Files maintained by NHTR.	
	(1) Report 21 and Withdrawal Report 2.	Destroy when 25 years old. (N1-64-87-1)
	(2) NARS-5 Master File.	Cut off at end of fiscal year.

		Delete or overwrite when 3 years old or when no longer needed for administrative use, whichever is sooner. (N1-64-95-2, item 2b)

4. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented? Cite the disposition instructions for records that have an approved records disposition in accordance with, FILES 203. If the records are unscheduled that cannot be destroyed or purged until the schedule is approved.

Disposition instructions are contained in NARA Files 203.

5. Is the system using technologies in ways that the Agency has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, describe.

No

6. How does the use of this technology affect public/employee privacy?

The public does not use this system. Federal agency and FRC employees must provide their name, address, phone number, and email address in order to gain access to the system.

7. Does the system meet both NARA's IT security requirements as well as the procedures required by federal law and policy?

Yes

8. Has a risk assessment been performed for this system? If so, and risks were identified, what controls or procedures were enacted to safeguard the information?

The VA Austin Automation Center assesses the risks of NARA systems executing at their facility on an annual basis. The overall system risk was identified as Medium-Low. The versions of operating system and system specific related software are outdated and it is no longer readily possible to apply patches and updates. These risks will be addressed in conjunction with the deployment of the ARCIS application which is targeted for the 2008 – 2009 time frame. The TASK

application will be replaced at that time.

9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.

The VA conducts monthly vulnerability scans on all hardware supporting NARA applications, as well as their overall network. Open vulnerabilities are compiled and analyzed on a quarterly basis and a subset of NIST 800-53 controls are tested annually. Additionally, a SAS70 audit which includes a review of system security practices is conducted on an annual basis and reported to NARA.

10. Identify a point of contact for any additional questions from users regarding the security of the system.

Linda Ferro
NHV – St Louis
Email: linda.ferro@nara.gov
Phone: 314.801.0957

Section 7: Is this a system of records covered by the Privacy Act?

1. Under which Privacy Act systems of records notice does the system operate? Provide number and name.

N/A. There is no information in this system that is covered by the Privacy Act.

2. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

N/A

Conclusions and Analysis

1. Did any pertinent issues arise during the drafting of this Assessment?

No.

2. If so, what changes were made to the system/application to compensate?

N/A

The Following Officials Have Approved this PIA

_____ (Signature) 9/4/08 (Date)
David M. Weinberg, NR
Director, Federal Records Center Program
8601 Adelphi Road, Room 3600
College Park, MD 20740-6001
301.837.7167

_____ (Signature) 9/10/08 (Date)
Gary M. Stern, NGC
Senior Agency Official for Privacy
8601 Adelphi Rd, Room 3110
College Park, MD
301.837.2024

_____ (Signature) 9/11/08 (Date)
Martha Morphy, NH
Chief Information Officer
8601 Adelphi Rd, Room 4400
College Park, MD
301.837.1992