Privacy Impact Assessment

Name of Project: TASK Tracking System
Project's Unique ID: AITC - TASK

Legal Authority(ies): 44 U.S.C. 2907

Purpose of this System/Application:

The TASK system is one of several National Archives and Records Administration (NARA) applications housed at the Department of Veteran's Affairs (VA) Austin Information Technology Center (AITC) located in Austin, TX.

TASK is a labor management and tracking application used to align and monitor the specific work tasks to hours expended. The TASK system provides statistical summaries concerning the production rates of specific tasks, automates the production of quantity statistics for individual employees' performance ratings, provides summaries concerning the personnel costs to perform specific tasks and projects in the centers, and provides feeder dates for various budget and productivity reports.

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 information about Federal Records Center employees who use the system to perform their jobs.

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

Employees: Information about NARA Federal Record Center (FRC) employees, including assigned user name and unique password.

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 is used to provide statistical summaries concerning the production rates of specific tasks, automates the production of quantity statistics for individual employees' performance ratings, provides summaries concerning the personnel costs to perform specific tasks and projects in the centers.

In addition data about the TASK users is collected to validate 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.

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.

Yes. Data is retrievable by name.

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

Reports on individuals can be produced that show the type and amount of work produced for a specific period of time. These reports are used by FRC managers to evaluate employee performance against critical elements and performance standards.

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

No. There is no public use of the system.

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 AITC 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). A SAS 70 audit was also completed in 2008, with final report to NARA pending.

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

The system is not web based.

<u>Section 4: Sharing of Collected Information</u>

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

AITC System Administrators, FRC Managers and FRC system administrators have access to the TASK data. Users have access to data necessary to perform work related functions.

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.).

AITC System Administrators. AITC System Administrators have access to all data. The AITC 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). A SAS 70 audit was also completed in 2008, with final report to NARA pending.

FRC Managers and System Administrators. FRC Managers and System Administrators can only access data for employees assigned to their specific organization. Controls are maintained within the application.

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

See question 2, above.

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 AITC 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). A SAS 70 audit was also completed in 2008, with final report to NARA pending.

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 for operation and maintenance. The AITC 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.

No.

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?

N/A

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.

No.

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?

Individuals cannot decline to provide information. It is a requirement of employment to provide the staff members legal name.

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

No negative determinations can be made by the system. Due process procedures are in accordance with NARA personnel policies and procedures.

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.).

Each new user must be approved by an FRC Manager. FRC Managers review the data for accuracy. There is no document that outlines this procedure.

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 (AITC). Users access the system from many sites; however, all data is retained at the AITC.

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

1316	**TASK System**	
	Automated data base and related records created for administrative purposes to show individual, unit, and center productivity measurements. The TASK system also serves as a feeder system to the Automated Statistical Summary. (See file no. 1317.)	
1316-1	Input forms.	
	a. Short-term: Organization Master Entries, Master Transaction Entries, Batch Cards, and Employee Master Transaction Entry.	Destroy after information has been keyed onto disk file and verification is complete. (N1-64-87-1)
	b. Long-term: Productivity Record and Batch Card and TASK Daily Work Log.	• 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: Destroy when 6 months old or when no longer needed for administrative purposes, whichever is shorter. (N1-64-87-1)
1316-2	Output reports.	
	a. Employee performance measurements,	Destroy 3 years after the date of

	including General Performance Appraisal System (GPAS) reports supporting employee performance appraisal files; and individual monthly and yearly reports. (See also file no. 305.)	appraisal or when no longer needed. (N1-64-87-1)
	b. Individual Weekly Summary Report.	Destroy when Individual Monthly Summary Report has been verified. (N1-64-87-1)
	c. Feeder reports used to prepare summary reports, including Microfilm Job Summary, Weekly Summary, Monthly Summary, and Center Statistical Summary.	Destroy when no longer needed to prepare the summary report, or 3 months after close of fiscal year. (N1-64-87-1)
	d. Weekly Productivity Reconciliation Validation Edit Report.	Destroy after corrections have been made to the transaction file. (N1-64-87-1)
1316-3	Automated files.	
	a. Program and documentation files containing 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 system is no longer is use. (N1-64-87-1)
	(2) Files maintained by the Regional Operations Branch (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. TASK system master file.	
	(1) Files maintained at records centers.	Destroy when system is

		modified OR no longer in use. (N1-64-87-1)
	(2) Files maintained by NHTR.	Destroy 2 years after close of fiscal year. (N1-64-87-1)

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 the NARA Records Schedule, which is a supplement to the policy directive, FILES 203: NARA Files Maintenance and Records Disposition Manual.

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?
N/A

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.

This system operates under NARA 22, Employee Related Files.

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

There are no modifications of the system or the Privacy Act system of records notice at this time.

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

See Attached Approval Page

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

Martha Morphy (Signature) 9/11/08 (Date)

Martha Morphy, NH
Chief Information Officer
8601 Adelphi Rd, Room 4400
College Park, MD
301.837.1992