Privacy Impact Assessment (PIA)

Name of Project: Case Analysis Tracking System

Project's Unique ID: CATS

Legal Authority(ies):	**44 USC 1502, et seq.**

Purpose of this System/Application: The Case Analysis Tracking System (CATS) is an MS Access database used to administer correspondence requests for civilian records at the National Personnel Records Center (NPRC). CATS maintains the request itself, but it does not include the actual civilian records.

Section 1: Information to be Collected

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

Employees		Available data in the system with respect to NARA employees is limited to First Name, Last Name, CAT Account User ID and NARANet User ID. NARA email address is not stored in CATS, are used to log-in and user identification numbers that is CATS specific.
External Users		N/A.
Audit trail information (including employee log-in information)		Audit trail information is available in the system that includes user log-in information, searches, and other actions.
Other (describe)		Although there are no external users of the system, there is data in the system specific to former federal employees. This data details the "Subject of Record" when an external request is made for an Official Personnel Folder (OPF) or Employee Medical File (EMF). This data includes name, date of birth, last four of social security number of the Subject of Record, as well as the date of request. Additionally, there is information in the system that describes what entity makes the correspondence request. This is either the agency name (when the request is made by a federal agency), or described as a "public request" when made by the subject of record or other authorized third party.

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

NARA operational records		None. There is no data in the system garnered from NARA operational records.
External users		There are no external users of the system.
Employees		The NARA employees who have accounts are assigned them when they work on the team that processes these requests at Valmeyer or at the Archives Drive customer call center. User account information (Same as the Employees entry above) is limited to a log-in identifier obtained when the user's CATS account is created.
Other Federal agencies (list agency)		None. There are no other Federal agencies that use the system.
State and local agencies (list agency)		N/A.
Other third party source		Requests for records are submitted via a paper request. The paper request includes the specific details of the request. That paper request is handled by NARA employees, as they are the only users of the system. The NARA employee, in turn, enters the details of the paper request into the system.

Section 2: Why the Information is Being Collected

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

Yes.

The employee user account and user identification is necessary to authenticate into the system.

The external subject of record name, date of birth, and last four of the social security number is necessary to process the request.

The date information is necessary for logging, case tracking/management, and auditing purposes.

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. The system only includes the details of the records request, not the records themselves.

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

No. There is no new data.

3. Can the system make determinations about employees/the public that would not be possible without the new data?
No.
There are no determinations made about employees or the public.

4. How will the new data be verified for relevance and accuracy?
No.
There is no new data.

5. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
The system employs safeguards and processes to protect the data from unauthorized access. Supervisor approval is required for account creation. The system employs role-based security associated with individual accounts. Additionally, access is predicated upon successfully logging into a NARANet machine with an authenticated PIV card.

6. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.
N/A.
No processes are consolidated.

7. Generally, how will the data be retrieved by the user?
Supervisors/Managers, Management Assistants/Analysts, and Customer Service Technicians retrieve data from the system through various database queries/commands.
Supervisors/Managers retrieve statistical information to manage work. Supervisors also retrieve collections of unassigned requests (known as "Batches") and assign those requests to subordinate personnel for execution. The batches are printed out in hardcopy and then assigned to subordinate personnel.

Customer Service Technicians retrieve data in order to provide progress updates on case management.

Management Assistants/Analysts extract information from the system in order to make work transactions in another system as a part of the monthly billing process.

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. Supervisors/Managers and Customer Service Technicians can retrieve information by the name, data of birth, or last four of the social security number for Subject of Record.

This data is only the records request itself, it is not the actual record.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?
There are no reports produced on individuals.

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?
Role based security includes a single administrator role with complete read/write access to the entire CATS system and fifteen (15) additional user roles with limited read/write access to the CATS system dependent on user responsibilities.

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)?
Users, managers, and system administrators have access to the data in the system. All personnel are NARA employees. Their access is determined through a management approval process and the system employs role-based security.

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.). Are safeguards in place to terminate access to the data by the user?

The system employs role-based security associated with individual accounts. Those roles are determined through a management approval process.

Supervisors/Managers retrieve statistical information to manage work. Supervisors will also retrieve collections of unassigned requests (known as "Batches") and assign those requests to subordinate personnel for execution. The batches are printed out in hardcopy and then assigned to subordinate personnel.

Customer Service Technicians retrieve data in order to provide progress updates on case management.

Management Assistants/Analysts extract information from the system in order to make work transactions in another system as a part of the monthly billing process.

Each month the Information System Security Officer requests that the System Owner perform a Privileged User Account review and send a detailed verification of for each person's access to ensure any unnecessary access is revoked.

A similar Non-Privileged User Account review and verification is performed annually to ensure any unnecessary access is revoked.

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

Access is limited to the user's assigned role.

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)? How will these controls be monitored and verified?

The system employs role-based security to prevent the misuse of the data. There is an annual audit in place to review assigned roles. There are no contractors that use this system.

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?

No.

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.

Archives Records Center Information System (ARCIS) receives data from this system via a human interface (i.e. there is no automated data link). This data details agencies that have submitted requests and the number of requests submitted. There is no personal information exchanged.

NARA Performance Metric System (PMRS) receives data from this system via a data link. This data includes numbers and dates of requests. There is no personal information exchanged.

7. Have the NARA systems described in item 6 received an approved Security Certification and Privacy Impact Assessment?
ARCIS and PMRS both contain PII and their PIA was last reviewed in September 2018. These are Enterprise level systems with an approved ATO.

8. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?
The Senior Agency Official for Privacy and Chief Privacy Officer are responsible for protecting the privacy rights of the public and employees.

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?
This is not applicable, as CATS does not contain the records themselves, only the requests made for those records.

2. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
CATS does not make determinations about people.

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.).
N/A.
The data in the system is only as accurate as the request that was made.

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 is operated at more than one NPRC site, but both sites access the same system over the NARANet. Consistent use of the system and data integrity is achieved by all users at both NPRC sites accessing the same data tables that are located on the NPRC Valmeyer Annex servers.

3. What are the retention periods of data in this system?
GENERAL RECORDS SCHEDULE 4.1: Records Management Records.

Item 010 - Tracking and control records. Temporary. Destroy when no longer needed. DAA-GRS-2013-0002-0016.

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.
The records request in the CATS system is maintained indefinitely. If deleted, it would be a manual process using the Windows delete commands.

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?
The system is an MS Access database hosted on NARANet. As such, the system meets NARA's IT security requirements as well as the procedures required by the federal law and policy.

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?
As this system is an MS Access database, a risk assessment has not been performed. However, this system is slated for replacement by an enterprise customer relationship management tool to eliminate

the risks inherent in Access databases.

9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.
Security scans are completed by NARA IT Security monthly. An "Admin Account Attestation", a document that confirms that the System Owner is aware of the users with elevated privileges on their account, is also completed on a monthly basis. An audit of user accounts is completed annually.

10. Identify a point of contact for any additional questions from users regarding the security of the system.
The points of contact are:
Karen Mellott (System Owner)
Karen.Mellott@nara.gov
618-935-3005

Joseph Stewart (Technical Point of Contact)
Joseph.Stewart@nara.gov
314-801-0602

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.

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.

See Attached Approval Page

Once the Privacy Impact Assessment (PIA) is completed and the signature approval page is signed, please provide copies of the PIA to the following:

IT Security Manager
Privacy Act Officer

The Following Officials Have Approved this PIA	
System Manager (Project Manager)	
KAREN MELLOTT Digitally signed by KAREN MELLOTT Date: 2021.08.03 11:21:27 -05'00' (Signature)	(Date)
Name: Karen Mellott	
Title: CATS System Owner	
Contact information: 1411 Boulder Blvd, Valmeyer, IL 62295, 618-935-3005, Karen.Mellott@nara.gov	
Senior Agency Official for Privacy (or designee)	
GARY STERN Digitally signed by GARY STERN Date: 2021.07.14 15:25:20 -04'00' (Signature)	(Date)
Name: Gary M. Stern	
Title: General Counsel	
Contact information: 8601 Adelphi Road, Room 3110, College Park, MD 20740-6001 301-837-3026, Garym.Stern@nara.gov	
Chief Information Officer (or designee)	
SWARNALI HALDAR Digitally signed by SWARNALI HALDAR Date: 2022.04.15 07:49:10 -04'00' (Signature)	(Date)
Name: Swarnali Haldar	
Title: Executive for Information Services/CIO (I)	
Contact information: 8601 Adelphi Road, Room 4415, College Park, MD 20740-6001 301-837-1583, Swarnali.Haldar@nara.gov	