



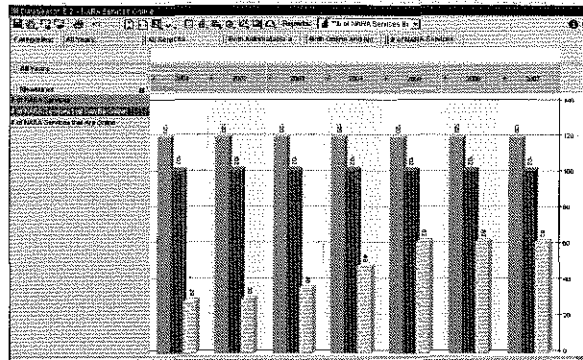
---

Performance Measurement and Reporting System (PMRS)

# Privacy Impact Assessment

September 12, 2013

---



Prepared for:

**National Archives and Records Administration**  
Performance and Accountability Staff  
8601 Adelphi Road  
College Park, MD 20740-6001

---

**CACI**

1100 North Glebe Rd.  
Arlington, VA 22201  
(703) 841-7800

*Last Updated: September 18, 2013*  
*h:\privacy\pia's\pmrs privacy impact assessment 2013-09-12.docx*

# Table of Contents

---

<b>1. Overview of PMRS</b>	<b>1</b>
1.1 A DATA WAREHOUSE.....	1
1.2 PARTS OF PMRS RELEVANT TO PRIVACY .....	2
1.3 BORDERLINE CASES NOT DISCUSSED FURTHER .....	3
<b>2. Employee Data</b>	<b>4</b>
2.1 EMPLOYEE INFORMATION BEING COLLECTED.....	4
2.2 WHY THE EMPLOYEE INFORMATION IS BEING COLLECTED .....	10
2.3 INTENDED USE OF THIS INFORMATION .....	10
2.4 SHARING OF COLLECTED INFORMATION.....	12
2.5 OPPORTUNITIES FOR INDIVIDUALS TO DECLINE PROVIDING INFORMATION .....	13
2.6 SECURITY OF COLLECTED INFORMATION .....	13
<b>3. Written Requests &amp; FOIAs in the Unit Logs</b>	<b>15</b>
3.1 WRITTEN REQUEST AND FOIA INFORMATION BEING COLLECTED IN THE UNIT LOGS .....	16
3.2 WHY THE WRITTEN REQUEST AND FOIA INFORMATION IS BEING COLLECTED .....	16
3.3 INTENDED USE OF THIS INFORMATION .....	16
3.4 SHARING OF COLLECTED INFORMATION.....	17
3.5 OPPORTUNITIES FOR INDIVIDUALS TO DECLINE PROVIDING INFORMATION .....	17
3.6 SECURITY OF COLLECTED INFORMATION .....	17
<b>4. Written Requests &amp; FOIAs in the PMRS Web Application</b>	<b>18</b>
4.1 WRITTEN REQUEST AND FOIA INFORMATION BEING COLLECTED IN THE WEB APPLICATION.....	19
4.2 WHY THE WRITTEN REQUEST AND FOIA INFORMATION IS BEING COLLECTED .....	20
4.3 INTENDED USE OF THIS INFORMATION .....	20
4.4 SHARING OF COLLECTED INFORMATION.....	20
4.5 OPPORTUNITIES FOR INDIVIDUALS TO DECLINE PROVIDING INFORMATION .....	20
4.6 SECURITY OF COLLECTED INFORMATION .....	20
<b>5. Is this a System of Record Covered by the Privacy Act?</b>	<b>21</b>
<b>6. Conclusions and Analysis</b>	<b>21</b>
6.1 DID ANY PERTINENT ISSUES ARISE DURING THE DRAFTING OF THIS ASSESSMENT?.....	21
6.2 IF SO, WHAT CHANGES WERE MADE TO THE SYSTEM/APPLICATION TO COMPENSATE? .....	21
<b>7. Approvals</b>	<b>21</b>

---



## Update History

<b>Date</b>	<b>Version</b>	<b>Description</b>	<b>Author</b>
Aug 22, 2008	1.0	Initial	S. Beste
May 19, 2010	1.1	No substantive changes. Minor grammatical and IT technical changes were made. For instance, all the Access databases referred to have been migrated to Access 2007, so their file names end in ".accdb" vice "*.mdb". All citations herein were correspondingly updated.	S. Beste
Apr 29, 2011	1.2	No substantive changes. Organization codes have been changed to reflect the NARA reorganization in the spring of 2011. The document was converted to Word 2007 format.	S. Beste
Aug 27, 2012		<ul style="list-style-type: none"><li>• Data containing RNO and disability information is now anonymous throughout PMRS.</li><li>• Age replaces birth date throughout.</li><li>• Age has replaced Date of Birth throughout PMRS.</li></ul> I dropped version numbers in favor of just using the dates. FPPS replaces CHRIS. I cleaned up the page numbers.	S. Beste
Sep 12, 2013		<ul style="list-style-type: none"><li>• Employee database in Access dropped, replaced by the Employee Log in the web app.</li></ul>	S. Beste



# Privacy Impact Assessment

**Name of the Project.** Performance Measurement and Reporting System

**Project ID.** PMRS

**Legal Authority.** Government Performance and Results Act, 1993, "GPRA"

**Purpose of this System.** GPRA provides that agencies will have strategic plans with numeric performance targets. It further provides that agencies shall report their progress against those goals with auditable figures. PMRS is the system that collects and reports those auditable performance results at NARA.

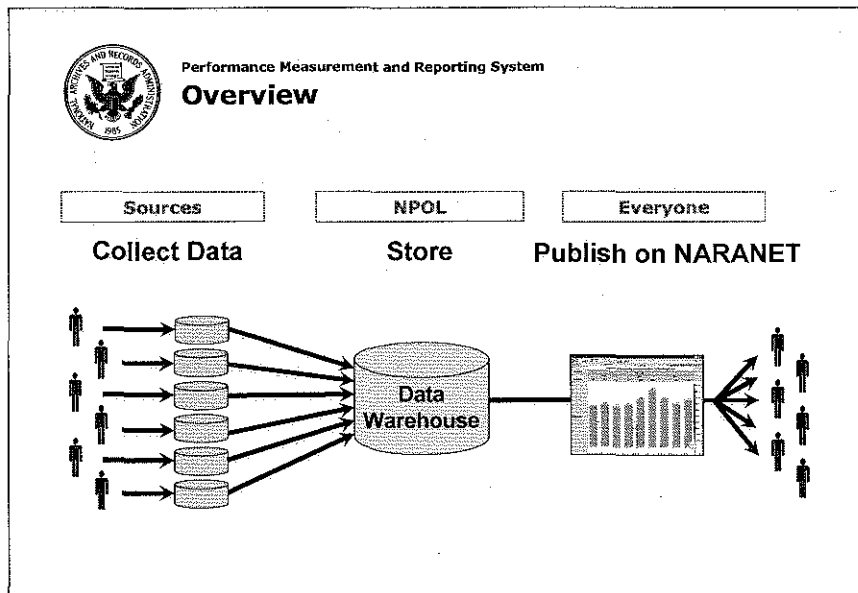
---

## 1. Overview of PMRS

---

### 1.1 A Data Warehouse

PMRS is a data warehouse application. As such, it has no data of its own. Rather, it gathers data from 71 NARA sources for the purpose of combining and publishing them through a common user interface. This is the big picture:



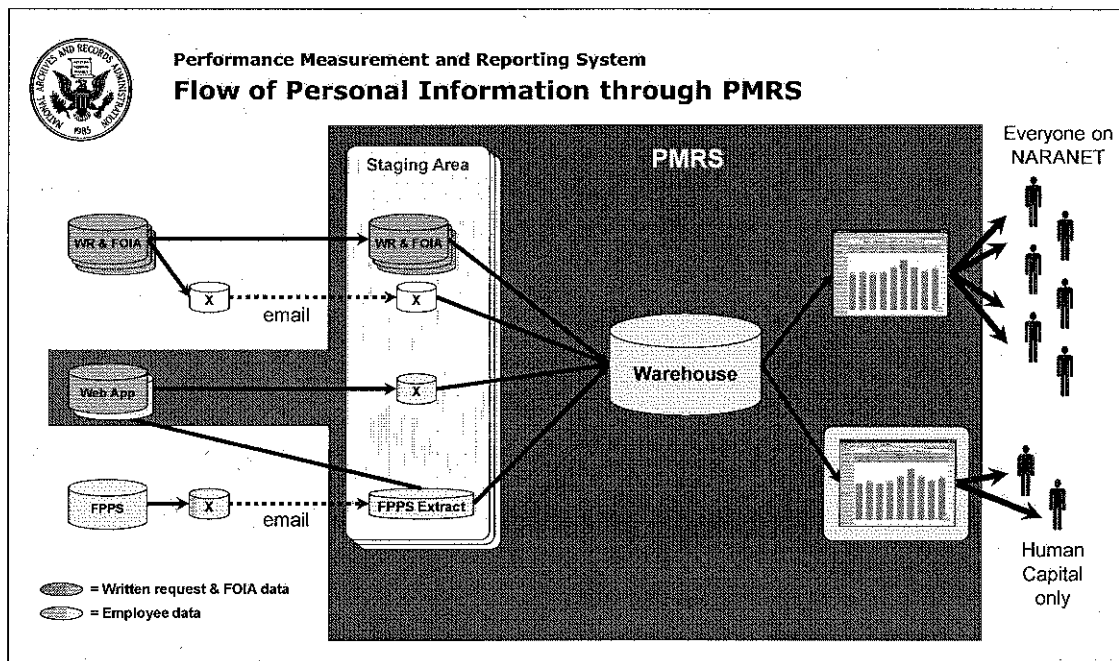
PMRS pulls hundreds of data elements from these databases each month, covering every aspect of NARA operations. Most of this has nothing to do with individuals or their privacy.

## 1.2 Parts of PMRS Relevant to Privacy

The diagram below shows where personally-sensitive information resides in PMRS. The dark background defines the boundary of PMRS. The colors pink and green show the two categories of data at issue:

- Pink: FOIA requests and written requests – data on requests for information from the public by FOIA or otherwise.
- Green: Employee data.

The rest of this assessment treats these two categories separately. But understand how all the data flows into and out of PMRS.



1. **People enter data into source databases** at left. Normally, source databases are the responsibility of their owners (CMRS, SOFA, FPPS...). The privacy impacts of those systems are not covered here. We have one exception: the PMRS web application is inside the PMRS boundary. It is a source database that is also part of PMRS.
2. **Some databases are sent whole to PMRS each month.** For example, NGC sends its entire FOIA-tracking database to the PMRS staging area every month.
3. **Other systems send only extracts.** With the exception of the extract from FPPS, these extract databases do not contain data on individuals.
4. **The Performance and Accountability Staff (CP) stages everything.** All incoming data takes the form of a file in the PMRS staging folder.
5. **CP keeps a copy of every submission.** For data quality and audit purposes, CP keeps a copy of every database it receives. It does this by saving a copy of the staging area each month.
6. **CP loads the warehouse.** Except for employee data, the warehouse contains no personally-identifiable information.

7. **CP publishes to everyone on NARANET.** This is the publication side of PMRS. It contains summary data only and no privacy data.
8. **CP publishes employee data to the Office of Human Capital (H).** A small amount of personally-identifiable employee data goes to selected people in H for use in workforce planning.

### 1.3 Borderline Cases Not Discussed Further

In the interest of complete disclosure, PMRS touches on two other categories of personal information.

#### 1.3.1 Data Regarding Online Reproduction Orders

PMRS collects data on every reproduction order placed through SOFA. However, it collects only the fields below. None of these identifies the requester or the subject of the request. *Therefore, this data has no bearing on privacy and will not be discussed further.*

ORDER EXTRACT Table		
Field Name	Data Type	Description
order id	Text	A unique identifier from the OFAS system for a reproduction order.
product type cd	Text	The OFAS code for what PMRS calls an order type. Expressed as a form #: 85, 72a, etc.
nara org cd	Text	The NARA org code of the archival business unit that processed the request.
order payment type cd	Text	The method by which a reproduction order is to be paid.
order result cd	Text	Indicates whether the records ordered for reproduction have been sought and found.
receipt dt	Date/Tim	The date the order was first entered into OFAS.
completion dt	Date/Tim	The date NARA completed all work on the order.
ready for shipment dt	Date/Tim	The date the order was ready to ship. Where [order payment type cd] = 'Billed', PMRS sets [completion dt] to this value.
servicing age	Number	The number of NARA working days that the order remained in the servicing part of the work flow.
production age	Number	The number of NARA working days that the order remained in the production part of the work flow.
ready age	Number	The number of NARA working days that the order remained in the ready-for-shipment part of the work flow.

#### 1.3.2 Employee Log-In Data

The PMRS web application is used by about 250 NARA employees. Regarding these users, the application stores:

- Their name.
- Their organization code(s).
- Their NARANET login ID.
- The date and time of their last login.
- The user ID and a timestamp of the last change made to every row of data. This information is visible to any colleague who can see that row of data.

This data is used to:

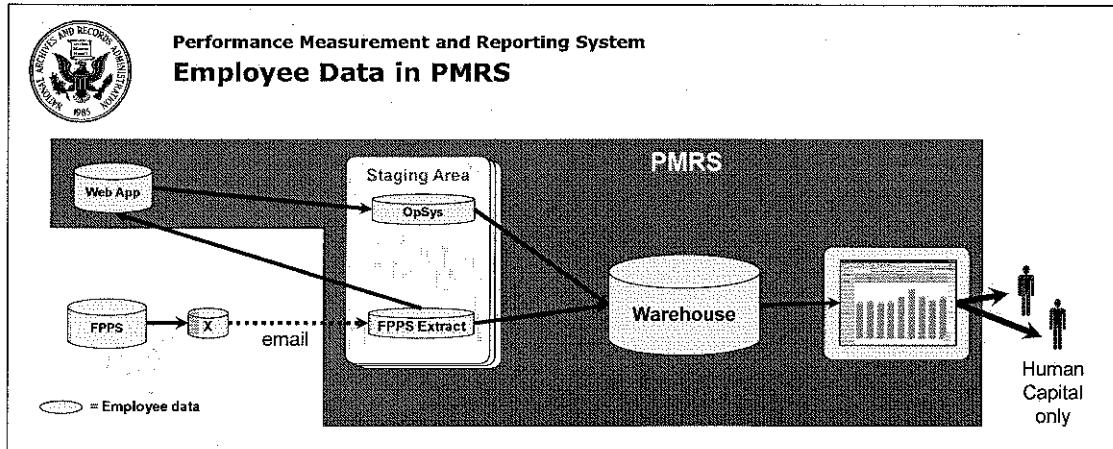
- Restrict system access to registered users
- Restrict user access to just the logs and organizations they need.
- Spot users who are inactive in the system (and who may therefore need to be dropped).
- Maintain accountability for the data by revealing who last changed it.

This information is necessary for the reasonable functioning of the system. No use is made of the data outside of the application. It is not particularly sensitive. *Therefore, this data will not be discussed further.*



## 2. Employee Data

This diagram is an extract of the one on page 2. It shows just the data about employees.



### 2.1 Employee Information Being Collected

Employee data enters PMRS from two sources:

- FPPS, the personnel system. This is the major source. Every month, HTS emails CP an extract from FPPS. This is shown at left in the diagram above.
- PMRS Web App (Employee Log). This web log holds a list of employees and a checkmark from their manager as to whether they are eligible to telework or not.

#### 2.1.1 FPPS Extract.accdb

This is PMRS's receiving database for the extract coming from FPPS. It is essentially an envelope for moving the data. It has no queries for analyzing the data. It has two tables for employees – one with identifying information but no RNO<sup>1</sup> data, and one with the reverse. See the displays below.

#### Employee Data with IDs – EMPLOYEE ID table

See the list of fields on the next page. This is a table of all current employees plus those who departed within the last year. The most sensitive fields are:

- NARA employee number
- Employee name

<sup>1</sup> RNO = Race and national origin.

Employee ID table

Field Name	Data Type	Description
employee num	Number	NARA's unique employee identifier. Switch from SSAN when CHRIS can give us separations by employ
employee name	Text	Last name and first name of the employee
pay plan cd	Text	A code designating schedule of pay grades typically meaning "GS" = General Schedule
grade num	Number	Level of the position, such as the "13" in "GS-13"
occupational series cd	Text	A code describing the kind of duties to which the employee has been assigned
supervisory level cd	Text	A code indicating the employee's supervisory role
nara org cd	Text	Org Code from PIRS
facility cd	Text	The duty city code from CHRIS, the personnel system
position title txt	Text	Title of the employee's position
hire dt	Date/Time	The date the employee's tenure at NARA officially began: Dt EOD NARA
separation dt	Date/Time	The date the employee's tenure at NARA officially ended: Dt Separated
separation reason cd	Text	From the personnel system, a code for the reason an employee left NARA.
appt type cd	Text	A code indicating the rule under which the employee holds his position
gender cd	Text	A code indicating the employee's sex
patcob cd	Text	A code indicating whether the person's position is professional, clerical, blue collar, etc.
appt auth cd	Text	3 digit code that identifies an appointment authority
work schedule cd	Text	A code that distinguishes between full-time, part-time, intermittent, and seasonal employment.
retirement eligibility dt	Date/Time	The earliest data that this employee will be eligible to retire.
federal service start dt	Date/Time	SCD (leave) in CHRIS. This is the date to use for calculating years of Federal service. It's a virtual date s
last promotion dt	Date/Time	The date of the employee's last promotion. If none, then [hire dt].
retirement plan cd	Text	The code that indicates which retirement plan applies to this employee.
target grade num	Number	The top grade level of the employee's current career track.
record status txt	Text	Status of the record as a result of the last update from the personnel system
idp flg	Yes/No	Yes=This employee has a Individual Development Plan approved as being linked to strategic goals
idp dt	Date/Time	The date on which the employee's Individual Development Plan was approved as being linked to strat
end of month idp dt	Date/Time	As of end of last quarter...The date on which the employee's Individual Development Plan was approv
performance plan flg	Yes/No	Yes=This employee has a current performance appraisal plan approved as being linked to strategic goa
performance plan dt	Date/Time	The date on which the employee's performance appraisal plan was approved as being linked to strateg
end of month performance plan dt	Date/Time	As of end of last quarter...The date on which the employee's performance appraisal plan was approv
new nara org cd	Text	Manually entered by the PMRS Administrator during times of reorganization when people have both o
cancel idp flg	Yes/No	Temp data. Yes = Cancel the person's IDP in Employee.mdb. Incoming data shows a change in org. pos
cancel performance plan flg	Yes/No	Temp data. Yes = Cancel the person's performance plan in Employee.mdb. Incoming data shows a cha
standard name	Text	Used for linking to data coming from ETAMS to data from CHRIS. See the ETAMS import code.

### Employee Data with IDs – EMPLOYEE RNO table

This covers only current employees. It is anonymized, meaning that employee names and IDs are not in the table. What remains is statistical information only, particularly:

- Disability code.
- Self-declared race code

### Employee RNO table

Field Name	Data Type	Description
nara org cd	Text	Org Code from PIRS
facility cd	Text	The duty city code from CHRIS, the personnel system
pay plan cd	Text	A code designating schedule of pay grades typically meaning "GS" = General Schedule
grade num	Number	Level of the position, such as the "13" in "GS-13"
occupational series cd	Text	A code describing the kind of duties to which the employee has been assigned
supervisory level cd	Text	A code indicating the employee's supervisory role
appt type cd	Text	A code indicating the rule under which the employee holds his position
appt auth cd	Text	3 digit code that identifies an appointment authority
disability cd	Text	A code indicating the most severe disability claimed by the employee
gender cd	Text	A code indicating the employee's sex
race combo cd	Text	A code of 1s and zeroes in which each of 6 digits indicates membership in a particular race.
patcob cd	Text	A code indicating whether the person's position is professional, clerical, blue collar, etc.
work schedule cd	Text	A code that distinguishes between full-time, part-time, intermittent, and seasonal employment.
target grade num	Number	The top grade level of the employee's current career track.
federal service start dt	Date/Time	SCD (leave) in CHRIS. This is the date to use for calculating years of Federal service. It's a virtual date since if her
last promotion dt	Date/Time	The date of the employee's last promotion. If none, then [hire dt].
retirement plan cd	Text	The code that indicates which retirement plan applies to this employee.
retirement eligibility dt	Date/Time	The earliest data that this employee will be eligible to retire.
age	Number	The employee's age at the time of extract.





### 2.1.2 PMRS Web App (Employee Log)

This is where managers check off people as being eligible to telework or not. It contains the minimum number of fields to support that function. The list of employees gets updated by FPPS Extract.accdb every time it imports new data from FPPS.

*Beyond the confluence of employee name and number, this database has no sensitive data.*

Field Name	Data Type	Description
month_end dt	Date/Time	The month and year for which eligibility applies.
employee num	Number	The number of the employee as assigned by the personnel system.
telework eligible qty	Number	From the OpSys.EMPLOYEE table.

### 2.1.3 PMRS Warehouse

This is the heart of PMRS. It stores data on all employees, present and past, with monthly snapshots of various properties, such as their current grade and position title. The database resides in SQL Server running on the PMRSprod Windows server. Access is restricted to the PMRS Administrator.

As with the feed files and FPPS Extract.accdb, the warehouse segregates the employee data into two areas

- Data with identifying information but no RNO or disability information.
- The reverse. Anonymized data with RNO and disability information.

#### Tables with Identifiers

This is EMPLOYEE, the parent table, with one row for every employee past and present. Sensitive fields are:

- NARA employee number
- Employee name

Field Name	Data Type
employee num	Number
employee name	Text
hire dt	Date/Time
separation dt	Date/Time
retirement eligibility dt	Date/Time
separation reason cd	Text
federal service start dt	Date/Time
retirement plan cd	Text
last active duty month end dt	Date/Time

This is EMPLOYEE MONTH ID, with one record for each employee each month. It is child to EMPLOYEE, with the link back being through [employee num]. This contains no RNO data.



Field Name	Data Type
month end dt	Date/Time
employee num	Number
hara org cd	Text
facility cd	Text
position title txt	Text
pay plan cd	Text
grade num	Number
occupational series cd	Text
supervisory level cd	Text
appointment type cd	Text
appointing authority cd	Text
gender cd	Text
patcob cd	Text
work schedule cd	Text
target grade num	Number
last promotion dt	Date/Time
employee qty	Number
performance plan qty	Number
individual development plan qty	Number
telework eligible qty	Number



This is **EMPLOYEE MONTH**, with one record for each employee each month. However, the data is anonymous.

Field Name	Data Type
month end dt	Date/Time
nara org cd	Text
facility cd	Text
pay plan cd	Text
grade num	Number
occupational series cd	Text
supervisory level cd	Text
appointment type cd	Text
appointing authority cd	Text
disability cd	Text
gender cd	Text
race combo cd	Text
patcob cd	Text
work schedule cd	Text
target grade num	Number
federal service start dt	Date/Time
last promotion dt	Date/Time
retirement plan cd	Text
retirement eligibility dt	Date/Time
employee qty	Number
employee age	Number



### 2.1.4 The Databeacon Web Site

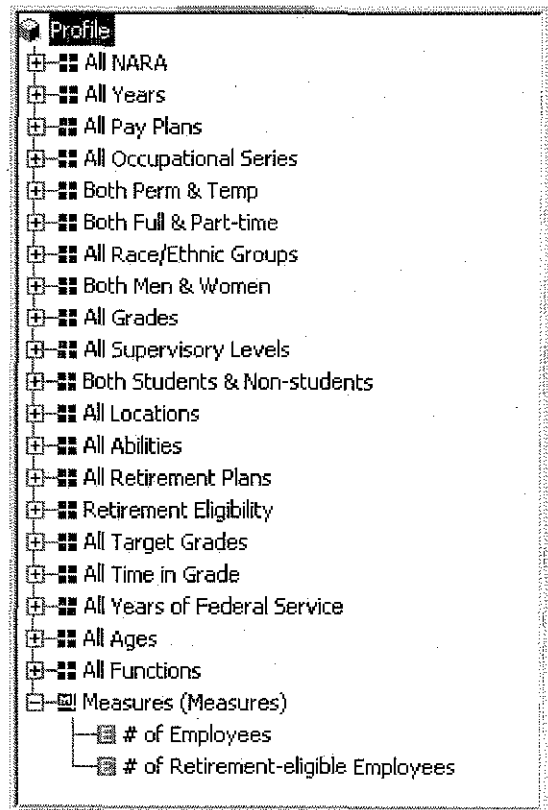
PMRS publishes its data on NARANET using Databeacon. Databeacon is an easy-to-learn tool for slicing and dicing numerical data using a web browser. Our standard Employee “cube” lets users slice the data on 17 dimensions, such as pay plan, grade, supervisory level, org code, gender, race, or any combination of these. The system does not let users ask about individuals. Indeed, neither employee names nor numbers are on the web site. However, by slicing the data fine enough, users can sometimes tell who the data is describing, especially in small units where there may be only one female GS-9 Archives Technician. Therefore, when H asked for more dimensions – in particular, a breakout by peoples’ ages – we knew that we had a privacy issue.

Our solution was to give H the additional dimensions they want, but to put that data at a hidden location on the PMRS web site. The data is accessible by anyone on NARANET, but only if they know the URL. Databeacon has no security facilities of its own.

The sensitive data here is peoples’ ages and the possibility that users could connect an age with a specific employee by qualifying all the other dimensions enough as described above.

#### hr\_employee

The main cube, hr\_employee, has two measures that can be broken out in 20 dimensions (right). The data covers monthly snapshots of active employees.



---

## 2.2 Why the Employee Information is Being Collected

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

The list of data elements is driven by the needs of H to do workforce planning. In particular:

- Retention analysis requires that PMRS keep data on individuals. We need to see if the specific people who were here last year are still here.
- The analysis by age requires peoples' birth dates. Knowing peoples' ages is a reasonable part of workforce planning and analysis.

In addition, CP has its own requirements for metrics.

- Our Annual Performance Plan says that we will measure how many of our employees are eligible to telework, and of those, how many do.
- A breakout of data by race, gender, and disabilities is required for our reporting to OMB.

### 2.2.2 Is there another source for the data? Explain how that source is or is not used?

FPPS is the only source of this data.

---

## 2.3 Intended Use of this Information

### 2.3.1 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. PMRS offers no more data about individuals than is already in FPPS – except for the fact of whether they are eligible to telework or not.

### 2.3.2 Will the new data be placed in the individual's record?

No. There is no new data.

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

No. There is no new data.

### 2.3.4 How will the new data be verified for relevance and accuracy?

There is no new data.

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

See the descriptions in section 2.1 above regarding the access restrictions on the various data stores.



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

See descriptions in section 2.1 above regarding the access restrictions on the various data stores. In addition, PMRS has extensive data quality checks to ensure the integrity of the data as it moves into the warehouse. If HTS adds a new code, if CP changes an org code, even if HTS assigns a new number to someone – these conditions are all caught by the import code.

**2.3.7 Generally, how will the data be retrieved by the user?**

Essentially, PMRS is a reporting tool offering summary data. Except for the administrator, the data is *not* retrievable by the user. Instead, PMRS delivers summary data through its web site.

**2.3.8 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.**

Except for the administrator writing ad hoc queries, the data is not retrievable by a personal identifier.

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

None.

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

No. PMRS will not allow NARA to treat individuals differently. Hopefully, it will help us be smarter about treating classes of individuals differently through the mechanism of workforce planning.

**2.3.11 Will this system be used to identify, locate, and monitor individuals?**

Not at all.

**2.3.12 What kinds of information are collected as a function of the monitoring of individuals?**

None.

**2.3.13 What controls will be used to prevent unauthorized monitoring?**

N/A.

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

Yes. As noted above, the web application requires its users to log in. It then tracks the changes they make. On the publication side, Databeacon creates cookies based on the IP address of the user's machine. It uses these to connect returning users with views of the data that they have saved. It has no capability to track usage. In any event, the only web users are government employees and contractors doing government work.



---

## 2.4 Sharing of Collected Information

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

See the descriptions of the various data stores in section 2.1 on page 4 above.

### 2.4.2 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.).

The access rules are simple and herewith documented.:

- The PMRS administrator (and presumably ITSS support staff) has access to everything in PMRS.
- Everyone on NARANET has access to the published data.
- H and the people they share the URL with have access to the web site that publishes summary employee data by age.
- Access to the web logs is open to anyone on NARANET whose supervisor sends an email making the request to the PMRS Administrator.

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

See the descriptions in section 2.1 on page 4 above regarding restrictions applied to the various data stores.

### 2.4.4 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 PMRS Administrator is the only person with access to sensitive details. His training in privacy requirements consists of the standard NARA online course plus the preparation of this PIA.

### 2.4.5 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?

Contractors are very much involved in the creation and operation of PMRS. However, PMRS is not a Privacy Act system of record, so there is no requirement for contract clauses.

### 2.4.6 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.

PMRS is all about sharing data. The source of employee data is FPPS.

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

FPPS is an approved Privacy Act system.



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

CP is responsible for controlling access to information in PMRS.

H is responsible for limiting the contents of the extract sent to PMRS from FPPS.

**2.4.9 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. PMRS is an internal NARA system.

---

**2.5 Opportunities for Individuals to Decline Providing Information**

**2.5.1 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 have no right to decline the uses documented here.

**2.5.2 Does the system ensure “due process” by allowing affected parties to respond to any negative determination, prior to final action?**

N/A. PMRS is a reporting system. It reports statistics after the fact. It is not involved in any determinations, certainly none regarding individuals.

---

**2.6 Security of Collected Information**

**2.6.1 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.).**

The data is refreshed every pay period with new data from FPPS. Thus, the current data is always as authoritative as it can be.

The program that imports the data from FPPS makes sure that all employees previously reported are accounted for in the new extract, either as current employees or as separated employees. It also spots people who have had their NARA employee number changed.

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

N/A. The system is used at only one site.

**2.6.3 What are the retention periods of data in this system?**

- **Data warehouse:** Ten years, per the PMRS records schedule, N1-064-03-1.
- **Employee.accdb:** N/A. This database does not retain historical data. It stores only a current snapshot of active employees from FPPS. Separated employees are removed as part of the update from FPPS.





- **CHIS Extract.accdb:** This likewise contains only the contents of the latest update from FPPS.
- **PMRS web site:** The data on this site is replaced each month with new data.
- **Historical copies** of the staging area: Kept for 3 years, per the PMRS records schedule, N1-064-03-1.

**2.6.4 What are the procedures for disposition of the data at the end of the retention period?**

- **Data warehouse:** Destruction is done automatically by a SQL Server scheduled job that runs every October.
- **Historical copies** of the staging area: Destruction is done manually by the PMRS Administrator every October.

**2.6.5 Is the system using technologies in ways that the Agency has not previously?**

No.

**2.6.6 How does the use of this technology affect public/employee privacy?**

N/A. No such technology is used.

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

Yes. PMRS has NARA C&A approval.

**2.6.8 Has a risk assessment been performed for this system?**

Yes.

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

- The units regularly view their performance on the PMRS web site. They complain if they find something amiss in the data.
- PMRS has extensive validation checks to ensure that data being imported is clean and complete.
- ITSS keeps backup copies for 90 days of all data in PMRS.

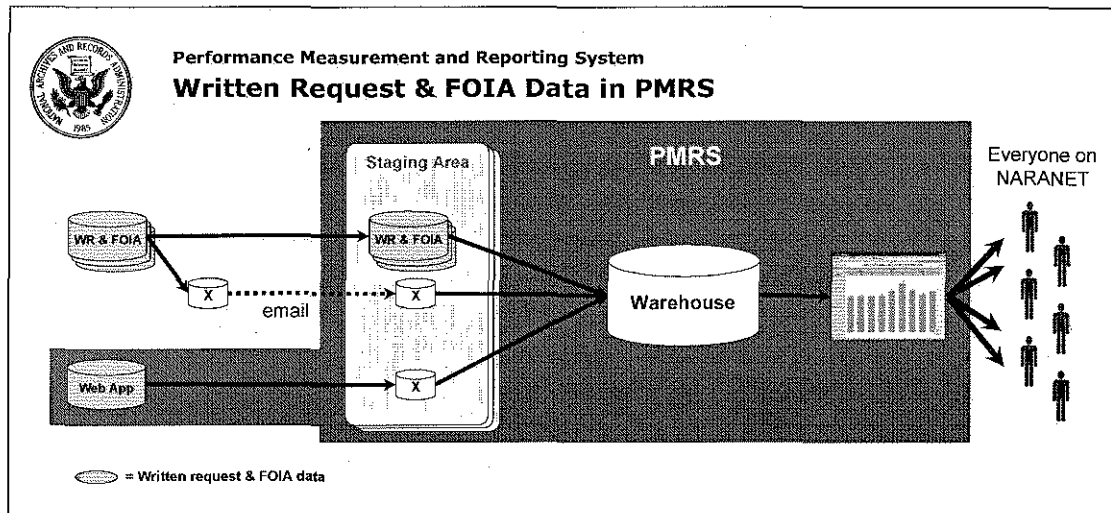
**2.6.10 Identify a point of contact for any additional questions from users regarding the security of the system.**

Steve Beste, CP. 301-837-0918.



### 3. Written Requests & FOIAs in the Unit Logs

This diagram is an extract of the one on page 2. It shows just the data about written requests and FOIAs. Data flows from the source systems on the left to the website users on the right.



NARA's customer service standards say that if you write to us requesting information, we will reply within ten working days. Likewise, if you send us a request and cite the Freedom of Information Act (FOIA), we will reply within 20 working days. PMRS measures and publishes this performance.

To do so, PMRS collects data on every FOIA request and every "written request". However, PMRS does not need to know anything about the requesters or the specifics of the requests. Therefore, the warehouse itself does not contain any such fields. *The warehouse is not discussed further.*

The units who reply to the requests obviously do need to know the requester and the specifics of their requests. Almost every unit in NARA therefore has a correspondence log of some kind and also a FOIA log. Sometimes, the two logs are combined in one database, sometimes not. In FY2004, PMRS replaced many of these local logs with the PMRS web application. This includes both a FOIA log and a written request log. Units were free to switch to the web app logs or to continue on as they were. This produced the two kinds of sources shown at the left in the diagram above: Local databases and the PMRS web app.

For those units that kept their own logs, two reporting mechanisms emerged. Some, such as NGC, simply email a copy of the entire log to the PMRS Administrator each month. This is simple, and 17 units take this approach. Other units (18) create an extract database and send only that. This is a little more work for the unit each month, but it's appropriate where the source database is large. The Bush and Clinton libraries, for instance, both have large, complicated logs that cover FOIAs, written requests, and many other management functions. They send extracts.

These extracts contain no personally-identifiable data. *The extracts are not discussed further.*

The topics of interest are thus:

- The copies of the unit logs that arrive at PMRS in full, and
- The web application. That is covered in section 4 on page 18 below.

---

### 3.1 Written Request and FOIA Information Being Collected in the Unit Logs

Every month, PMRS receives 14 databases containing written request details, 2 containing FOIA details, and one containing both for a total of 17 databases of interest here. The sensitive fields are typically:

- The name of the person making the request (a member of the public)
- The person's address and telephone number
- A description of the records being sought.
- The date of the request and the dates of our actions in reply.

Of the 17 databases:

- 2 go to the PMRS Administrator in CP.
- 6 go to the PMRS point of contact in L, the central office of the Legislative Archives, Presidential Libraries, and Museum Services office.
- 9 go to the PMRS point of contact in R, the central office of the Research Services office.

All of these people save the databases to the PMRS staging area on the PMRSprod server. Access to the staging area is limited to the PMRS Administrator and the PMRS points of contact in the L and R central offices. As a practical matter, none of these people actually looks at the data unless there's a problem. The act of saving the file in the staging area launches the PMRS warehouse loader. It extracts the fields relevant to timeliness and leaves the sensitive fields behind.

On the first of every month, the contents of the staging area are zipped and saved to a folder on the PMRSweb server accessible only by the PMRS Administrator. The staging area is then emptied, ready for the next month. This is an automatic process.

---

### 3.2 Why the Written Request and FOIA Information is Being Collected

The sensitive information arrives as a byproduct of collecting other data in these logs. PMRS makes no use of it and does not import it into the PMRS warehouse.

The alternative would be to have the units send in only extracts of their logs. Some units do this already. The question is whether it makes business sense to expand that design to all units. The tradeoffs are these:

- The cost of building, deploying, teaching, and maintaining 17 extract databases. These are small units with limited technical ability. CP would have to do the work.
- The additional complexity of the monthly submission step at each unit.
- The limited sensitivity of the data.
- The very limited additional exposure that the present system incurs.
- The value to the public in having NARA track the timeliness of our replies to these requests at reasonable cost.

Given the tradeoffs, CP concludes that the present design is appropriate.

---

### 3.3 Intended Use of this Information

None.



---

### **3.4 Sharing of Collected Information**

The data is not shared. It goes nowhere, as describe in the introduction to this section 3 on page 15 above.

---

### **3.5 Opportunities for Individuals to Decline Providing Information**

None.

---

### **3.6 Security of Collected Information**

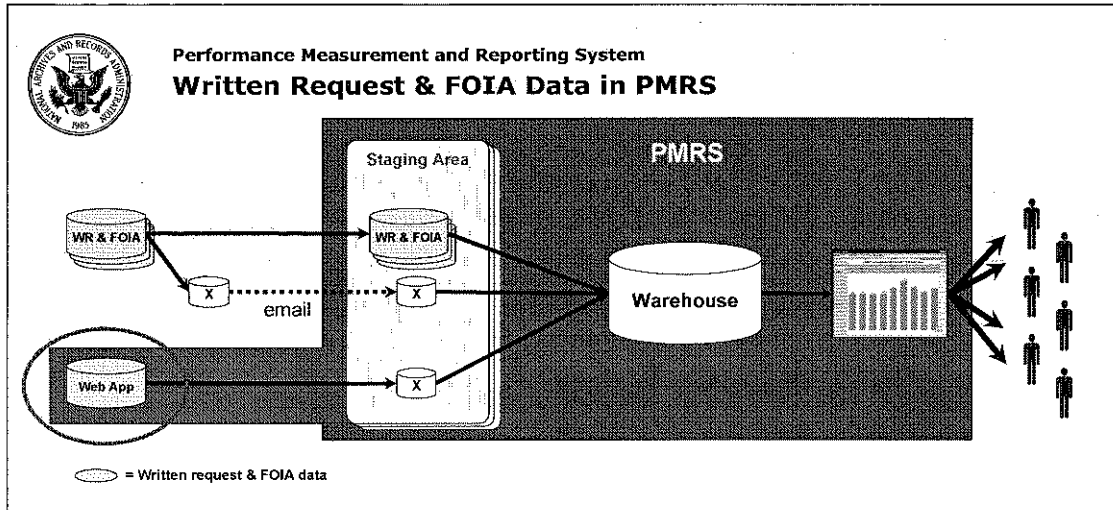
The files in question reside, in sequence:

- As email attachments in GroupWise, protected by the recipient's password.
- In the PMRS staging area. Access to that requires first a NARANET login and then an account on the PMRSprod server. Very few people have this. See section 3.1 on page 16 above.
- In the PMRS staging area archive. Access to this requires first a NARANET login and then an account on the PMRSweb server. Only the PMRS Administrator has this.



## 4. Written Requests & FOIAs in the PMRS Web Application

This diagram is an extract of the one on page 2. It shows just the data about written requests and FOIAs. Data flows from the source systems on the left to the website users on the right.



Please read the introduction to major section 3 on page 15 for an overview of written request and FOIA data in PMRS. This section concerns the PMRS web application, its FOIA Log, and its Written Request Log.

### *About the PMRS Web Application*

CP deployed the web app in FY 2004 as a replacement for several dozen Access databases that were then being sent in every month. The old databases were cumbersome, inflexible, and depended on people in the field to push the data to CP. By contrast, the web app allows central maintenance, and CP can pull the data from the database at any time. As the scope of PMRS expanded, the web app allowed CP to collect additional data at relatively low cost.

The downside of the web app is that it puts CP in the business of owning a source system. Normally, source databases are the responsibility of their owners (CMRS, SOFA, FPPS, and all the little Access databases that still come into PMRS). With the web app, CP is obliged to support the field units' requirements for day-to-day management data, at least within certain subject areas. Two of those subject areas are FOIAs and written requests.

In practice, many units chose to keep using their own databases in lieu of the web versions. This is the current situation:

- **FOIAs.** The big FOIA shops run their own databases. The National Personnel Records Center in St. Louis uses CMRS, Our Washington-area operation uses ADRES, the PRA libraries and NGC use home-grown Access databases. Only the small shops use the FOIA web log. Of the 12,186 FOIAs received in FY2007, only 3% (360) came into PMRS through the FOIA web log. But these covered 20 NARA units. That is 20 Access databases that we no longer have to chase each month.
- **Written requests.** Units are very attached to their correspondence logs. Only 5 units out of 41 chose to replace them with the one in the web app. The web app recorded 2,954 written requests in FY2007, 3% of the total excluding National Personnel Records Center.

The web application currently has 281 registered users. Many of these are supervisors and backup users. 154 users are active, having logged into the system in the past three months.

#### 4.1 Written Request and FOIA Information Being Collected in the Web Application

The sensitive fields are typically:

- The name of the person making the request (a member of the public)
- The person's address and telephone number
- A description of the records being sought.
- The date of the request and the dates of our actions in reply.

Specifically, in respect to FOIAs, the web app collects the fields at right.

In respect to written requests, the web app collects the fields below:

Web - WRITTEN REQUEST : Table		
Field Name	Data Type	
request num	AutoNumber	
nara org cd	Text	
request id	Text	
medium name	Text	
request receipt dt	Date/Time	
request due dt	Date/Time	
request completion dt	Date/Time	
action name	Text	
assigned staff name	Text	
request item name	Text	
customer name	Text	
organization name	Text	
comment txt	Text	
check num	Text	
received amt	Text	
last changed supplier id	Text	
last changed dtm	Date/Time	
rowversion num	Binary	

Web - FOIA DATA ENTRY : Table		
Field Name	Data Type	
request num	AutoNumber	
nara org cd	Text	
request id	Text	
foia complexity cd	Text	
requested records cat cd	Text	
foia determination cd	Text	
request dt	Date/Time	
request receipt dt	Date/Time	
referral start dt	Date/Time	
referral completion dt	Date/Time	
request completion dt	Date/Time	
nondis b1 flg	Yes/No	
nondis b2 flg	Yes/No	
nondis b3 flg	Yes/No	
nondis b4 flg	Yes/No	
nondis b5 flg	Yes/No	
nondis b6 flg	Yes/No	
nondis b7a flg	Yes/No	
nondis b7b flg	Yes/No	
nondis b7c flg	Yes/No	
nondis b7d flg	Yes/No	
nondis b7e flg	Yes/No	
nondis b7f flg	Yes/No	
nondis b8 flg	Yes/No	
nondis b9 flg	Yes/No	
nondis a flg	Yes/No	
nondis b flg	Yes/No	
nondis c flg	Yes/No	
nondis d flg	Yes/No	
nondis e flg	Yes/No	
nondis f flg	Yes/No	
nondis g flg	Yes/No	
nondis h flg	Yes/No	
nondis i flg	Yes/No	
nondis j flg	Yes/No	
requester last name	Text	
requester first name	Text	
requester middle initial name	Text	
requester org name	Text	
requester street name	Text	
requester city name	Text	
requester state cd	Text	
requester postal cd	Text	
requester country name	Text	
requester telephone num	Text	
requester email addr	Text	
request subject txt	Text	
assigned to name	Text	
comment txt	Text	
nondis b3 statute name	Text	
last changed supplier id	Text	
last changed dtm	Date/Time	
rowversion num	Binary	
old source name	Text	
old foia num	Number	



---

## 4.2 Why the Written Request and FOIA Information is Being Collected

The information is collected so that units can reply to requests from the public and manage the process of doing so.

---

## 4.3 Intended Use of this Information

The information is used by the respective NARA units to process the requests. PMRS extracts non-sensitive fields in order to measure performance. The web logs have no analytical or data mining or reporting ability

---

## 4.4 Sharing of Collected Information

Units can see only their own data, not each others'. The web log enforces this based on individual logins. The web application does not share this data at all.

---

## 4.5 Opportunities for Individuals to Decline Providing Information

None. If individuals want NARA records, they must tell us what they want and give us a way to contact them.

---

## 4.6 Security of Collected Information

### 4.6.1 How will the data be verified for accuracy, timeliness, and completeness?

- a) The people entering the data check it.
- b) The units check the figures that get published through PMRS, as these reflect on their performance.
- c) Central offices spot check the data in the logs during regular inspections, referring to the hard copies of the requests and replies.

### 4.6.2 How will consistent use of the system and data be maintained in all sites?

Uniform instructions have been created for all fields. These are available through the online help as well as in companion User Guides.

Extensive field and cross-field validations are built into the logs themselves. These prevent mistakes such as dates from last year or completion dates earlier than receipt dates.

Central offices spot check the data in the logs during regular inspections.

### 4.6.3 What are the retention periods of data in this system?

Three years. This is set by the PMRS records schedule, N1-064-03-1.

### 4.6.4 What is the procedure for disposition of the data at the end of the retention period?

Per the schedule, the data is destroyed. This is accomplished by a SQL Server scheduled job that runs every October.



**4.6.5 Is the system using technologies in ways that the Agency has not previously employed?**

No.

**4.6.6 How does the use of this technology affect public/employee privacy?**

N/A. No such technology is being used.

**4.6.7 Does the system meet IT security requirements?**

Yes. PMRS has NARA C&A approval.

**4.6.8 Has a risk assessment been performed for this system?**

Yes.

**4.6.9 Describe any monitoring, testing, or evaluation done on this system to ensure continued security of information**

The units regularly view their performance on the PMRS web site. They complain if they find something amiss in the data.

At the detail level, the system stamps every changed record with the date, time, and the ID of the person making the change.

**4.6.10 Identify a point of contact for any additional questions regarding the security of the system**

Steve Beste, CP. 301-837-0918.

---

## **5. Is this a System of Record Covered by the Privacy Act?**

PMRS is not a Privacy Act system of record. Nor is it required to be.

---

## **6. Conclusions and Analysis**

**6.1 Did any pertinent issues arise during the drafting of this Assessment?**

No.

**6.2 If so, what changes were made to the system/application to compensate?**

N/A.

---

## **7. Approvals**

The Following Officials Have Approved this PIA





**System Manager**

*Susan Ashtianie*

09/13/13

Susan Ashtianie  
Director, Performance and Accountability Staff  
301-837-1490

**Senior Agency Official for Privacy**

*Gary M. Stern*

*9/27/13*

Gary M. Stern  
General Counsel & Senior Agency Official for Privacy  
301-837-3026

**Chief Information Officer**

*Michael Wash*

*9.27.13*

Michael Wash  
Assistant Archivist for Information Services & Chief Information Officer  
301-837-1992

