

Privacy Impact Assessment

Name of Project: Order Fulfillment & Accounting System

Project's Unique ID: OFAS

Legal Authority(ies): 44 U.S.C. 2116(c) and 2307

Purpose of this System/Application:

Originally developed in 1998, NARA's Order Fulfillment and Accounting System (OFAS) provides NARA staff nation-wide with a means to receive orders, track the fulfillment status of customer requests for copies of records, and record and report the revenue generated. OFAS also provides an integrated Point of Sale (POS) solution with inventory management functionality. The system is only operated by NARA employees who will take information from the public requesting reproduction orders.

Reproduction order requests are received by mail, phone, fax, in person and via the Internet. Orders fall into three groups: Fixed Fee Reproductions (Form 80 orders), Quoted Reproductions (Form 72), and Merchandise. Orders received by mail, phone, fax and in person are keyed into the OFAS system by a NARA employee. Internet orders for Form 80's are handled by an interface with the Order Online! system. Order Online! provides a customer with the ability to order Form 80's on the Internet via the archives.gov website. A PIA has been conducted for the Order Online! system. Paper records of orders are subject to the retention rules outlined in NARA 1807.

The Order fulfillment piece of OFAS was migrated to a new system initiated by NARA. The new system, the Siebel Order Fulfillment Application (SOFA), now handles all order fulfillment and tracking, previously handled by OFAS. OFAS receives all financial information from the fulfillment of orders from SOFA.

Section 1: Information to be Collected

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

- a. **Employees:** Employees accessing the system will have their User ID and password stored in the system along with their first and last name. The department symbols in which they work will also be stored in the system.
- b. **External Users:** Several types of required and voluntarily provided information related to the public are used in the system.

User Profile Information - includes the following user-provided information: first name, last name, e-mail address [optional], shipping address, billing address, and credit card information may be stored as part of the user's profile to automatically insert the information in subsequent orders.

All user-provided information is securely stored in the OFAS system

- i. **Transaction Information** – includes information related to a specific order that is submitted to NARA such as item being ordered, shipping recipient and address, credit card number and expiration date, and billing address.
 - ii. **Order History Information** – includes information related to submitted orders.
- c. **Audit trail information (including employee log-in information):**

Audit Logs:

- i. **Application Logs** – Individual access to the **Great Plains** system is logged within the supporting security tables. The majority of **Great Plains** transactions and modifications applied within **OFAS** are logged with the individual's username and time stamp associated with the modification. Non critical events are not logged in order to reduce volume but can be turned on if deemed necessary to investigate fraudulent activity.
- ii. **Operating System Logs** – Event logs are set to 81,920 KB and archived on the 15th of every month. The security logs are actively monitored and security failure events are sent immediately to the Sys Admin. Notifications of other events (system and application) are actively monitored with exceptions to reduce false alarms. Exceptions include false positives and extraneous events that do not directly affect the security or stability of the system.

d. **Other (describe):** OFAS does not collect or maintain any other types of data.

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

All data that encompasses the OFAS solution is stored on a highly secure Windows 2003 server miming Microsoft SQL Server 2005. The database server is continually monitored utilizing both manual and automated intrusion detection software (IDS). The latest NIST standards have been implemented to ensure a secure environment and separate security audits performed by independent third party contractors.

a. **NARA operational records**

The majority of transactional records are handled electronically, however there are a few processes that are still manual. These processes include the manual entry of paper order forms from the public. These paper order requests are sent to the Archives and subsequently manually keyed into the OFAS and SOFA systems for processing. Once the data from the forms are entered into the system, the transaction is then handled electronically and the remaining paper forms are managed in accordance with NARA 1807.

b. **External users:** Several types of required and voluntarily provided information related to the public are used in the system.

User Profile Information - includes the following user-provided information: first name, last name, e-mail address [optional], shipping address, billing address, and credit card information may be stored as part of the user's profile to automatically insert the information in subsequent orders.

All user-provided information is securely stored in the OFAS system

- i. **Transaction Information** – includes information related to a specific order that is submitted to NARA such as item being ordered, shipping recipient and address, credit card number and expiration date, and billing address.
- ii. **Order History Information** – includes information related to submitted orders.

c. **Employees:** Employees accessing the system will have their User ID and password stored in the system along with their first and last name. The department symbols in which they work will also be stored in the system.

d. **Other Federal agencies (list agency):** Currently, no Federal Agency provides data that is used in the system.

e. **State and local agencies (list agency):** None

f. **Other third party source:** A secure credit card processing server, located at the National Archives, is used to facilitate the authorization of purchases made by credit card. All data retained on these credit card processing servers is encrypted and purged (deleted per retention rules outlined in NARA 1807) as part of the end of day reconciliation process. The credit card processing servers are administered by onsite staff within Archives II.

Section 2: Why the Information is Being Collected

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

The data elements are required for the business purpose of the system. OFAS provides NARA staff nation-wide with a means to receive orders, track the fulfillment status of customer requests for copies of records, and record and report the revenue generated.

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

The Siebel Order Fulfillment Application (SOFA) sends over quotes and completed orders to OFAS.

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?

The system will not derive new data or create previously unavailable data about an individual through aggregation of other collected data.

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

This is not applicable, as the system will not create or store information about an individual beyond optional profile information (such as user name, billing address and shipping address) that is used to pre-populate information in the order request. Information on users will only be maintained as a mechanism to fulfill orders and stored in a variety of tables within OFAS. Information will not be available as a separate file.

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

The system does not make determinations about the public or NARA employees.

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

The only new data into the system are new orders received from the customer. The information will be verified by the customer when taking the order.

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

There is no consolidation of system data.

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

Not applicable.

7. Generally, how will the data be retrieved by the user?

Individual data elements based on specific customer identification can only be retrieved by users with the appropriate level of access. Individual names or personal identification will only be used as a means to fulfill orders or facilitate customer service requests about that individual.

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.

A user can retrieve a customer's account by searching a customer ID, which is a generated number assigned to each new user in the system. A user can also search for a customer by first or last name. Individual names or personal identification will only be used as a means to fulfill orders or facilitate customer service requests about that individual.

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

The system will not create or store information about an individual beyond optional profile information (such as user name, billing address and shipping address) that is used to pre-populate information in the order request. Information on users will only be maintained as a mechanism to fulfill orders and stored in a variety of tables within OFAS. Information will not be available as a separate file.

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

The system does not make determinations about the public or NARA employees

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, the system is not used to identify, locate or monitor individuals.

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

Not applicable.

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

Not applicable.

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

This system does not use persistent cookies or other tracking devices.

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)?
 - a. **Users:** The users of the system are the employees of NARA. The public does not use this system. The users are assigned a level of access according to their job description. Profile information on the users is limited to login, password and security level.
 - b. **Managers:** Regional and Museum store Managers have limited access to the system associated with their location. The limited access includes running reports and accessing the Point of Sale application.
 - c. **System Administrator:** The OFAS system administrator has access to OFAS production data; however, encrypted data (e.g., user passwords) cannot be deciphered. Credit Card and financial data can be accessed by System Administrators with the appropriate level of access.
 - d. **Developers:** Developers have access to production data. Access is gained through login ID and password authentication. This access is required for initial data migration and trouble report investigation. Again, encrypted data cannot be deciphered.

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 OFAS project team is responsible for ensuring that access to OFAS data is properly controlled throughout the system lifecycle. This oversight ensures that only authorized individuals have access to the system data. The project staff follows NARA's Strategic Sequencing Process to identify and validate data ownership, establish and maintain administrative controls, and define and control access rights.

NARA's information technology projects follow a multi-step process, called the Strategic Sequencing Process, to ensure the proper implementation of new technology capabilities. This process guides NARA's transition from its current state of automation environment (or Baseline Architecture) to its planned state of automation (or Target Architecture), and ensures that each information technology project is properly coordinated with other enterprise initiatives.

Six key steps comprise the process: (1) conduct Business Process Reengineering (BPR) efforts, (2) analyze architectural differences and assess technology maturity, (3) select transition opportunities, (4) define/update architectural implementation plan and projects, (5) define/update Information Resource Management (IRM) project portfolio, and (6) implement projects in accordance with NARA's system development lifecycle

The highly controlled nature of the Strategic Sequencing Process ensures that team members thoroughly understand the business and technology environment, and that responsible NARA stakeholders are aware of and sign-off on major project milestones. These controls ensure that privacy concerns regarding sensitive data are identified and factored into the system design, user access administration, and ongoing system operations.

An employee's manager will determine their level of access required to fulfill their job responsibilities and the OFAS system manager (NARA employee), who has oversight over this process, will review the level of access requested and provide final approval.

All OFAS Managers have been given written instructions on proper procedures to request access to the OFAS solution for end users. This process includes the standard NARA background security check and a subsequent approval process by the OFAS application owner. Various levels of security access from within OFAS have been documented and are maintained by Tmst Fund support staff. End user access to OFAS is validated quarterly as part of the standard financial system audit procedures.

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

Users' access will be restricted to the data they need to complete their job responsibilities. There are several levels of access rights incorporated into the OFAS system with varying degrees of access. An employee's manager will determine their level of access required to fulfill their job responsibilities and the OFAS system manager (NARA employee), who has oversight over this process, will review the level of access requested and provide final approval.

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)?

There are two primary controls that prevent the misuse of data (e.g., unauthorized browsing) by those who have data access: (1) Data Encryption and (2) NARA Information Technology (IT) Policy. NARA's IT Policy is described in Section 5.b below.

- a. **Data Encryption:** The most sensitive data in the OFAS system are user passwords and financial information associated with the various OFAS

transactions. A variety of different layers of encryption and access controls are implemented to ensure this data is secured from unauthorized access. The various layers of security include Network, Operating System, Database and the Financial Application.

- b. **NARA IT Policy:** NARA IT Policy is formal guidance that establishes the rules of procedure for the development, implementation, and maintenance of IT systems. This policy includes several components, such as:
- i. **NARA Directives, Supplements, and Interim Guidance** - includes policy guidance such as the Information Technology (IT) Systems Security directive (NARA 804) and its related IT security handbooks that stipulate Management Controls, Operations Controls, Technical Controls, and IT Security Web Page Controls related to NARA systems, support staff, and contractors.

For example, the policy guidance requires that all system users receive appropriate training, including rules of behavior and consequences for violating the rules. It ensures that NARA maintains an effective incident handling capability (including intrusion detection monitoring and audit log reviews) and that each project adheres to the prescribed incident handling procedures. In addition, OFAS provides a small training session to users annually at the AO Conference held in College Park, MD. Additionally, background investigations are conducted on all NARA IT staff and contractors.

- ii. **Certification and Accreditation** – this process, which is conducted annually, or as major changes are implemented, to verify compliance with NARA’s IT policies and controls.
- iii. **Inspector General (IG) Audits** – periodically, the IG will conduct an independent audit to review compliance with NARA internal guidelines, external guidelines (e.g., NIST), and program-level procedures and controls.

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?

Yes, contractors were involved with the design and development of this system and are also employed to handle the ongoing maintenance of the system. The contractors were subject to a background check when they were brought onboard. In addition, all NARA employees and contractors are required to take an annual PII training course to ensure they are aware of PII data and the methods needed to protect this 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.

OFAS receives orders submitted by Order Online!. The data is transmitted via an automated Extensible Markup Language (XML) interface that operates within NARA's secure internal network. Order status updates are sent back to Order Online! by OFAS to communicate order history and status information to the submitting user. In addition, OFAS receives order information and payment data from the SOFA system. Please refer to the PIA for Order Online! for more information.

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

Yes, the OFAS system has received an approved certification and Privacy Impact Assessment.

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

The OFAS System Owner is responsible for protecting the privacy rights of the public and employees affected by the interface. NARA's Senior Agency Official for Privacy is responsible for ensuring compliance with the privacy rights of the public and NARA 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.

Limited financial information is transmitted to the Bureau of Public Debt (BPD) who provides extended accounting functionality to the agency.

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?

The system does not request any information beyond that to fulfill the customer's order request. The request submitted by the customer is a voluntary order request. The information is not used for any other means other than fulfilling the customer's order.

3. 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.).

The data in the system is submitted by the customer, therefore already making the data validated by the customers themselves.

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?

OFAS is operated at one site, and its data is centrally stored at that secure site, which is located in NARA's College Park, MD facility.

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

Official OFAS retention periods are documented in NARA 1807. Retention periods are further detailed in the OFAS Archiving and Purging system procedures document (need copy).

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 unclassified that cannot be destroyed or purged until the schedule is approved.

Data in the system is archived and purged according to the criteria outlined in the NARA 1807.

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, this system does not use any technologies in ways that the Agency has not previously employed.

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

Not applicable.

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?

No risks regarding dating safeguarding were identified in the risk assessment.

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

The primary method to ensure continued security of the information is to view server logs to identify any authorized access. The database server is also continually monitored utilizing both manual and automated intrusion detection software (IDS). In addition, granular level logging is capable but is only activated based on need to evaluate suspicious behavior.

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

National Archives Trust Fund
301-837-3550

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.

OFAS operated under NARA 25 Order Fulfillment and Accounting System. This notice was last published in the Federal Register on October 23, 2003.

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

Not applicable This system is not being modified.

Conclusions and Analysis

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

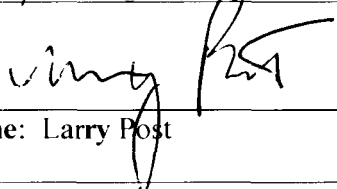
No.

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

Not applicable.

The Following Officials Have Approved this PIA

System Manager (Project Manager)



(Signature)

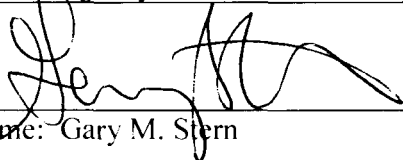
8/16/2011 (Date)

Name: Larry Post

Title: Secretary of the National Archives Trust Fund

Contact information: 301-837-3165

Senior Agency Official for Privacy (or designee)



(Signature)

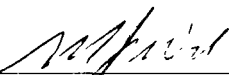
8/31/11 (Date)

Name: Gary M. Stern

Title: SAOP and General Counsel

Contact information: 301-837-3026

Chief Information Officer (or designee)



(Signature)

8.15.11 (Date)

Name: Michael Wash

Title: CIO

Contact information: 301-837-1992