

Privacy Impact Assessment

System Description

1. **System Name:** Order Fulfillment & Accounting System (OFAS)
2. **System Location:** National Archives and Records Administration (NARA), Archives II facility located in College Park, Maryland.
3. **System Description:**

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 outline 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.

Data in the System

1. **Categories of Information Used in the System:**
 - a. **Public:** 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.
- b. **Employee:** 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.
- c. **Other: OFAS does not collect or maintain any other types of data.**

2. Sources of Information in the System:

- a. **NARA Files and Databases:** All data that encompasses the OFAS solution is stored on a highly secure Windows 2003 server running Microsoft SQL Server 2000. 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.
- b. **Federal Agency-Provided Data:** Currently, no Federal Agency provides data that is used in the system.
- c. **State and Local Agency-Provided Data:** None.
- d. **Other Third Party Data:** 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.
- e. **Public or NARA Employee Data:**

Public: 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

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.

Order History Information – includes information related to submitted orders.

Employee: 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.

3. General Controls for Data Integrity to Ensure Integrity (e.g., accuracy, completeness, and validity) of System Data:

Data Retention Schedule:

Official OFAS retention periods are documented in NARA 1807.

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 (Dan Rick). 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 effect the security or stability of the system.

Documentation of Data Elements: All data elements associated with the Great Plains product are documented within the supporting Microsoft Software Development Kit and associated data model. This information was subsequently imported into the NARA PVCS (a configuration management tool that includes features such as version control and system

change tracking for projects. The software is configured so that it implements the agency's configuration management requirements and processes) application.

Configuration Management: The OFAS production baseline and all subsequent changes (e.g., application, data, infrastructure) are maintained using NARA's configuration management (CM) guidelines, as stated in NARA's Systems Development Lifecycle directive (NARA 805) and supplements to this directive: NARA Information Technology Systems Development Guidelines and Information Technology Systems Development Lifecycle Handbook.

Service Continuity: Contingency procedures for OFAS will be enacted if there is an outage for more than 48 hours (two (2) business days). The NAT Director will make the decision as to whether to attempt to restore operations at Archives II, continue operations at Archives II at a degraded level, attempt to move and restart operations offsite, or move to another plan entirely. The contingency plan for OFAS is documented in the OFAS Contingency Plan.

All of the OFAS servers are backed up daily via an automated tape backup. Incremental backups are conducted daily; full back ups are conducted weekly.

Once backups are completed, the tapes are secured in a locked room near the main computer room at Archives II. The tapes are then moved weekly offsite, to Archives I in Washington, DC. Individual Monthly backups are retained for a year and managed by the OFAS System Administrator.

Backup is performed on Compaq ProLiant 3000 Servers running Windows 2003 Server software or latest Server Operating System using the ARCserve 2000 Backup software. Both OFAS data and the OFAS application are fully backed up every Wednesday at 11:59 PM. Incremental backups are automatically scheduled for 11:59 PM all other days.

Certification and Accreditation:

Xacta recorded a C&A completion date of 5/19/2005.

Program Self-Audit:

Both independent 3rd party auditors and onsite support staff perform periodic audits of application and system software solutions that incorporate OFAS.

Access to the Data

1. Who will Have Access to the Data in the System (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 Data Access Determined?

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

3. Are Criteria, Procedures, Controls, and Responsibilities Regarding Access Documented?

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 Trust Fund support staff. End user access to OFAS is validated every 12 months as part of the standard financial system audit procedures.

4. Will users have access to all data on the system or will the users' access be restricted?

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.

5. What Controls are in Place to Prevent the Misuse of Data by Those Having Access?

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.

6. Other Systems that Share Data or Have Access to System Data

a. What systems share data or have access to system data?

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.

b. 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.

7. Other Agency Access to System Data

a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?

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

b. How will the data be used by the agency?

BPD utilizes this information to provide for larger accounting capabilities and requirements necessary to meet Federal fiduciary guidelines.

c. Who is responsible for assuring proper use of the data?

There are multiple individuals who are responsible for ensuring the proper use of data: Senior Agency Official for Privacy, Privacy Act Officer, Chief Information Officer, Information Security Officer, OFAS Program Manager, and OFAS System Administrator.

- d. **How will the system ensure that agencies only get the information they are entitled to obtain?** Only specific data elements required by the BPD to perform contract requirements are being exported from OFAS. These data elements are validated through automated scripting processes prior to secure transmission.

Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

NARA's Strategic Sequencing Process (see Access to the Data, Section 2) ensures that requirements are properly formulated and tested against the production system. This results in an information architecture that reflects only data that is needed to satisfy the functionality of the system.

2. New Data

- a. **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?** The system will not derive new data or create previously unavailable data about an individual through aggregation of other collected data.
- b. **Will the new data be placed in the individual's record (public or employee)?** 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.**
- c. **Can the systems make determinations about the public or employees that would not be possible without the new data?** The system does not make determinations about the public or NARA employees.
- d. **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.

3. Data Consolidation

- a. **If 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.
- b. **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?** Not applicable.

4. Data Retrieval

- a. **How will the data be retrieved? Can it be retrieved by personal identification?**
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.
- b. **What are the potential effects on the due process rights of the public and employees regarding:**
 - i. **Consolidation and Linkage of Files and Systems:** There are no perceived effects on the due process rights of the public and NARA employees.
 - ii. **Derivation of Data:** Not applicable.
 - iii. **Accelerated Information Processing and Decision Making:** Not applicable.
 - iv. **Use of New Technologies:** Not applicable.
 - v. **Mitigation of Effects:** Not applicable.

Maintenance of Administrative Controls

1. General Controls

- a. **Explain how the system and its use will ensure equitable treatment of the public and employees.** There are no impacts regarding the equitable treatment of the public and NARA employees
- b. **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.
- c. **Explain any possibility of disparate treatment of individuals or groups.** There is no possibility of disparate treatment of individuals or groups.

2. Data Retention

- a. **What are the retention periods of data in this system?**

OFAS recommended retention periods are outlined in section 3 of this document and further detailed in the OFAS Archiving and Purging system procedures document.

- b. **What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?**

Data within OFAS is purged using a variety of different utilities within the Great Plains application. The process for performing the purge is documented within the Great Plains and Compass Technologies system administrator materials. Further detail specific to the NARA purging schedule and requirements is outlined in the OFAS Archiving and Purging system procedures document stored on the NAT shared drive..

- c. **While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?**

Limited user access is provided to make modifications to data elements after initial submission. The limited access level prevents the likelihood of modification to orders after initial submission. Modifications to most order related information is tracked through detailed logging capabilities.

3. Use of New Technology

- a. **Is the system using technologies in ways that NARA has not previously employed (e.g., Caller-ID)?**

The OFAS solution is primarily an enterprise accounting system that tracks and reports on revenue received through various departments within NARA. The solution provides a central source for managing this financial information and exporting to the Bureau of Public Debt.

- b. **How does the use of this technology affect public/employee privacy?**

The OFAS system provides the mechanism by which the public can pay for NARA products and services and the Trust Fund can account for the subsequent revenue received. Any data collected, stored, and administered within the system is performed in a manner that fully protects the public's and employees' privacy.

4. Use of Data for Monitoring

- a. **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.** The system only captures customer orders for NARA products and services, therefore, it does not provide the capability to identify, locate, or monitor individuals. Employee transaction monitoring is possible as a means to identify fraudulent activity.

- b. **Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.** The system does not provide the capability to identify, locate, or monitor groups of people including users and employees.

- c. **What controls will be used to prevent unauthorized monitoring?** This is not applicable, as the system does not support or enable monitoring of individuals.

5. System of Record (SOR) Notice

- a. **Under which SOR notice does the system operate?** OFAS operated under NARA 25 Order Fulfillment and Accounting System. This notice was last published in the Federal Register on October 23, 2003.
- b. **If the system is being modified, will the SOR require amendment or revision?** The current SOR does not need to be modified at this time.

Glossary of Terms

Term	Description
<p>Order Fulfillment and Accounting System (OFAS)</p>	<p>NARA’s system that supports the financial element of the customer ordering process.</p> <p>Sales and Order Entry: OFAS is used in many of NARA’s organizational units to process “point of sale” transactions. This includes:</p> <ul style="list-style-type: none"> • Office of Records Services - Washington, DC; • Office of Presidential Libraries; • Office of the Federal Register; • Office of Regional Records Services; and • National Archives Trust Fund Division. <p>Payment Processing: OFAS bills customers for orders; maintains payment records for orders; processes order payments; and processes refunds. Additionally, OFAS routes customer refunds to the Bureau of Public Debt (BPD), which provides NARA's financial and accounting system under a cross-servicing agreement.</p> <p>OFAS records may include: catalogue order forms; other ordering forms; correspondence; copies of checks, money orders, credit card citations, and other remittances; invoices; and order and accounting information in the electronic system. These records may contain some or all of the following information about an individual: name, address, telephone number, record(s) or item(s) ordered, and credit card or purchase order information. OFAS records also include user profile data, reproduction order form data, transaction data, and credit card payment data transmitted from OFAS (See description, below) via an automated XML (Extensible Markup Language) interface that operates within NARA’s secure internal network.</p> <p>Automated Monitoring: Several tools are used within OFAS to monitor system security and stability. These monitoring capabilities are used to alert System Administrators when various problems are encountered.</p> <p>Credit Card Processing: OFAS utilizes a secure Credit Card processing server located in the Archives II Network Operations Center as a means to process payments with a Credit Card.</p>