Privacy Impact Assessment (PIA)

Name of Project: The Expanding NARA Online Services (ENOS) /Holdings Management System (HMS)

Project's Unique ID: 393-00-01-04-01-005-00

Legal Authority(ies):	**NARA's ENOS and e-Government Program stems from a 1998 OMB mandate: The Government Paperwork Elimination Act (GPEA, Pub. L. 105-277) requires that, when practicable, Federal agencies use electronic forms, electronic filing, and electronic signatures to conduct official business with the public.**

Purpose of this System/Application:
Supports online ordering and fulfillment of non-electronic record reproductions and enables NARA services to be requested electronically by external customers using the internet.
HMS automates, centralizes and standardizes the NARA business processes necessary to manage the physical aspects of permanent, non-electronic archival holdings agency-wide.

Section 1: Information to be Collected

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

Employees		As described below, information is passed directly from ENOS into Order Fulfillment and Accounting System (OFAS), as such, limited information related to NARA employees or its agents is used in the system.
External Users		**External Users.** Several types of voluntarily provided information related to the public are used in the system. **i. Customer Profile Information** – includes the following customer-provided information: login ID, password, first name, last name, e-mail address, challenge question, and challenge answer. The latter two types of information are used to validate a customer's identity for password reset, if needed. All customer-provided information is stored in the system until deleted by the customer. **ii. Transaction Information** – includes information related to a specific order or request that is submitted to NARA via the NARA Online Ordering System, such as item being ordered, shipping recipient and address, credit card number and expiration date, and billing address. This information is passed from the NARA Online Ordering System into OFAS via an automated Extensible Markup Language (XML) interface within NARA's secure internal network for order fulfillment.

		iii. Order History Information – includes information related to submitted orders and unfinished orders that may be retained by the customer for short-term reference. Customers can access this information with their login ID and password. This information is accessible for up to one year and is in accordance with NARA's Files Maintenance and Records Disposition Data Retention Schedule. "Session" cookies, which support the web-to-database transactions, are used. No "persistent" cookies are downloaded onto the user's computer. All customer-provided information is retained until deleted by the customer. **iv. Transaction Information** – includes information related to a specific order or request that is submitted to NARA via the NARA Online Ordering System, such as item being ordered, shipping recipient and address, credit card number and expiration date, and billing address. This information is passed from the NARA Online Ordering System into OFAS via an automated Extensible Markup Language (XML) interface within NARA's secure internal network for order fulfillment. **v. Order History Information** – includes information related to submitted orders and unfinished orders that may be retained by the customer for short-term reference. Customers can access this information with their login ID and password. This information is accessible for up to one year and is in accordance with NARA's Files Maintenance and Records Disposition Data Retention Schedule. "Session" cookies, which support the web-to-database transactions, are used. No "persistent" cookies are downloaded onto the user's computer.
Audit trail information (including employee log-in information)		ENOS maintains audit logs that track user access to the system and records database modifications. Detailed system logs are maintained for all system processes that run on the NARA Online Ordering System servers. This includes: **i. Integration logs** that provide details on the orders that are currently sent to OFAS. One log maintains details on the orders that are transferred to OFAS and a second log maintains details on order status updates that are received from OFAS. These are evaluated daily. **ii. System logs** also report multiple failed login attempts and system administrator updates to the NARA Online Ordering System environment. System logs are evaluated on a monthly basis and are securely backed-up and stored for possible "after-the-fact" reconstruction of performance or security threats. The NARA Online Ordering System also maintains audit logs that track the status of database or record updates using key system fields: created date, created by, last modified date, last modified by, conflict ID quote number, order number, and order line item number. **i. Created Date** – the date and time on which a record was created in the database. For

		example, each order in the system stores the date and time the order was created. **ii. Created By** – the ID of the individual who created a record in the database. For example, the User ID of the person who created an order. **iii. Last Modified Date** – the date on which the record was last modified. For example, the date when the system updates the order status from "Received" to "Processing". **iv. Last Modified By** – the User ID of the individual who last modified the record. **v. Conflict ID** – controls maintained to ensure data integrity in cases where more than one user attempts to access and potentially update the same record in the system. **vi. Quote Number** – the number associated with a quote record in the database. For example, each quote in the system stores the quote number. **vii. Order Number** – the number associated with an order record in the database. For example, each order in the system stores the order number. **viii. Order Line Item Number** – the number associated with a request line item within a order record in the database. For example, each individual request line item within an order in the system stores the order line item number and the business unit assigned to that request line item.
Other (describe)		Non-personal information, such as sample images of products and services available for sale, Frequently Asked Questions (FAQs), and the Privacy and Use statement are stored in the system.
Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?		
NARA operational records		NARA indexes and other related information are used to describe the products (e.g., microfilm publications) and services (e.g., archival material available for reproduction) that can be requested using the ENOS.
External users		Information cited in par. 1b above, the following customer profile information is collected from the public for use in the system: login ID, password, first name, last name, e-mail address [optional], challenge question, and challenge answer. The latter two types of information are used to validate a customer's identity for password reset, if needed. Optionally, the customer can submit the shipping address, billing address, and credit card information which is retained until the order is completed then is purged from the system.
Employees		As cited in par.1a above, limited information related to NARA employees or its agents is collected for use in the system (Par. 1c above, outlines the instances that the NARA User ID is used).

Other Federal agencies (list agency)		Currently, no Federal Agency provides data that is used in the system. In the future, NARA may attempt to acquire usage rights for certain indexes to NARA records that have been created by and are in the custody of other Federal Agencies. These third-party indexes may be used to assist customers in identifying NARA holdings.
State and local agencies (list agency)		None
Other third party source		Payment information is passed from the ENOS to Siebel Order Fulfillment Application (SOFA) via an automated XML interface within NARA's secure internal network for credit card validation from a third-party credit card validation service to approve individual credit card transactions before the order is approved and accepted by NARA for fulfillment. Upon approval, the ENOS receives an order status update from SOFA.

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.
Yes, each data element is necessary for completing the transaction.

2. Is there another source for the data? Explain how that source is or is not used?
There is no other source for collecting NARA Online Ordering system data.

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?
For NARA employees, the system will maintain information about system login, system logout, and record status changes. For the customer, 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 online order request.

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?
Users who choose to store information in their user profile are prompted to review the information prior to it being saved in the system. Additionally, the user may edit or delete the profile information at any time.

5. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
Although statistical reports are used to manage the ENOS system, 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?
NARA staff and contractors (acting as authorized agents) access information that is necessary to fulfill, troubleshoot, and ship orders.

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.
The information is retrieved by order number or customer name. Only those individuals with approved access rights have this authority and data accessibility.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?
This is not applicable, as the system only captures customer orders for NARA products and services.

10. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain.
No.

11. Will this system be used to identify, locate, and monitor individuals? If yes, describe the business purpose for the capability and the controls established explain.
The system only captures customer orders for NARA products and services, therefore, it does not provide the capability to identify, locate, or monitor individuals.

12. What kinds of information are collected as a function of the monitoring of individuals?
This is not applicable, as the system does not support or enable monitoring of individuals.

13. What controls will be used to prevent unauthorized monitoring?
Only authorized personnel have access to ENOS data. Physical and technical security controls are in place to prohibit unauthorized access and production oversight is provided by the system owner; currently, the SO and only a limited number of system administrators maintain the system.

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
The system does not use persistent cookies or other tracking devices to identify web visitors.

Section 4: Sharing of Collected Information

1. Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?
Users (NARA), Managers(NARA), System Administrators (Contractor) and Developers(Contractor)

2. How is access to the data by a user determined and by whom? Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where are they documented (e.g., concept of operations document, etc.). Are safeguards in place to terminate access to the data by the user?
A NARA Supervisor must submit a new user request form to create an account or change the user's responsibilities.

The NARA supervisor sends the exit clearance form (na-3009b) to disable the account. Additionally, on a yearly basis NARA system owners review users and disable accounts as applicable.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.
The ENOS is a Siebel software application that incorporates numerous access controls that manage the relationship between internal NARA user roles and responsibilities (or access rights), and application data views and database records. These access controls, referred to as Siebel "visibility" controls, determine different sets of views and different sets of records that NARA users can see when they log onto the ENOS. For customers, these controls ensure that they are able to see only their own Customer Profile Information, Transaction Information and Order History, in addition to other non-personal information that is stored for customer reference. The System Administrator oversees the different levels of access.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those who have been granted access (please list processes and training materials)? How will these controls be monitored and verified?
Restrictive physical security controls protect against unauthorized access to the ENOS workstations. Technical controls protect against unauthorized access to or misuse of ENOS and facilitate detection of security violations by generating audit logs to record users' activities and warn of anomalous conditions on the ENOS system. Audit tools create, maintain, and protect a trail of actions of users and administrators that trace security-relevant events to an individual, ensuring accountability. Also, in an effort to prevent data/record loss or unauthorized modification, the delete function has been disabled on the Preservation folder in ENOS.

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 involved with the design and development of the system are involved with the maintenance of the system. Appropriate Privacy Act contract clauses were inserted in their contracts, and other regulatory measures were addressed.

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.
The NARA Online Ordering System passes payment information to the Order Fulfillment and Accounting System (OFAS) for payment processing. 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 the ENOS by SOFA to communicate order history and status information to the submitting user.

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

A security evaluation study of SOFA was updated in FY 2017 and the OFAS privacy impact assessment has

been updated.

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

The System Administrator/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.

No other agency will share data or have access to data in the ENOS.

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?

Online forms used by the ENOS to collect information for processing an order alert the individual of the information that is required and the statutory authority for collecting the information.

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

Not applicable.

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.).

Customers enter their information directly into the system, and without valid billing information, the orders are not fulfilled. Additionally,

Security controls ensure the integrity of the NARA Online Ordering System data. These controls are evaluated annually as a part of NARA's Certification and Accreditation and Program Self-Audit. The NARA

Online Ordering System Program Manager is responsible for the overall integrity of the system's data. Certification and Accreditation (C&A) evaluations are conducted on an annual basis, or as major changes are implemented, to reevaluate the ENOS system and operational environment as major changes are implemented. A security evaluation study of the ENOS system was completed for FY 2017, in accordance with NIST 800-37, "Guidelines for Computer Security Certification and Accreditation."

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

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

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

The following is in accordance with NARA Files Maintenance and Records Disposition Manual (FILES 203, Appendix 18, File Number 1807), establishes the data retention schedule for the ENOS system.

The FILES 203 guidance has been implemented according to the following technical specification. Every twelve months, a scheduled business service purges the completed order data from the system and permanently destroys it. For customers who voluntarily choose to store their profile information (e.g., shipping address, billing address, credit card data) in the ENOS system for later retrieval, the profile information will remain active in the system until the customer deletes the information using the ENOS system or contacts NARA with a request that corresponding data should be deleted. Therefore, the ENOS system will not expire or inactivate any customer accounts or account profile information unless the customer initiates the deletion action.

4. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented? Cite the disposition instructions for records that have an approved records disposition in accordance with FILES 203. If the records are unscheduled, they cannot be destroyed or purged until the schedule is approved.

1807	**NARA Online Ordering System (Order Online! / SOFA) and Related Records**	
	Records documenting web-based customer orders for products and services. Orders are for reproductions of popular documents (e.g. Census), and researching and copying records. Includes records enabling	

	customers to track and smart-fill online orders, initiate financial transactions, and for staff to track and fulfill orders. May include orders paid by other than credit card originating with the Order Fulfillment and Accounting System (OFAS) (mail, fax, phone, or Point of Sale).	
1807-1	Customer profile data	Delete when no longer needed for administrative or financial purposes. (N1-64-072, item 1)
1807-2	Order transaction files (NATF Form 72, Order for Reproduction Services)	
	a. Form 72 Quotes.	Cut off at end of fiscal year. Delete or destroy when 2 years old. (N1-64-07-2, item 2a)
	b. Form 72 Orders.	Cut off at end of fiscal year. Destroy when 1 year old. (N164-07-2, item 2b)
	c. Canceled orders.	Cut off at end of fiscal year. Delete or destroy when 1 year old. (N1-64-07-2, item 2c)
1807-3	Fulfillment-related records created and received by custodial/reference units and the authorized contractor:	
	a. Originals of requests (e.g. Form 80's) scanned into the order fulfillment system.	File after verifying readability of scan and attachment to correct order number. Cut off at end of FY. Destroy 3 years after cutoff. (N1-64-07-2, item 3a)
	b. Pull slips, NA form 14001's (Reference Service Slips) and copies of packing slips. (NOTE: Because these NA form 14001's are used internally, they are marked to distinguish them from public research room 14001's.)	Cut off at end of FY. Destroy when 3 years old. (N1-64-072, item 3b)
	c. Other hardcopy records.	Cut of at end of FY. Destroy when 3 years old. (N1-64-072, item 3c)
1807-4	System documentation. Data, file, and output specifications and user guides.	Cut off at end of year in which system documentation is superseded or obsolete. Destroy/delete 2 years after cutoff. (N1-64-07-2, item 4)

5. Is the system using technologies in ways that the Agency has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, describe.
No.

6. How does the use of this technology affect public/employee privacy?
The user of e-commerce technology automates the customer's ability to submit and pay for NARA products and services. The same data is collected, stored, and administered in a
manner that fully protects the user's privacy.

7. Does the system meet both NARA's IT security requirements as well as the procedures required by federal law and policy?
A security evaluation study of the ENOS system is planned to be completed in FY 2017 in accordance with NIST 800-37, "Guidelines for Computer Security Certification and Accreditation."

8. Has a risk assessment been performed for this system? If so, and risks were identified, what controls or procedures were enacted to safeguard the information?
As outlined in Section 1 above, the Chief Information Security Officer initiates a self-assessment to ensure compliance with relevant external policy and requirements, internal NARA policy and requirements, and ENOS. The FIPS 199 rating relating to confidentiality, integrity, and availability for the ENOS system is MODERATE. The last Risk Assessment Report (RAR) was completed on July 25, 2017.

9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.
Continuity testing of the ENOS system is preformed via scripts every 30 minutes; Certification and Accreditation (C&A) evaluations are conducted on an annual basis, or as major changes are implemented, to reevaluate the ENOS system and operational environment as major changes are implemented; and the Chief Information Security Officer initiates a self-audit annually.

10. Identify a point of contact for any additional questions from users regarding the security of the system.
Edward Graham
PM ISE/NISP
Phone: 301-837-3732
Email: edward.graham@nara.gov

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.
NARA 37 is the SORN for ENOS.

2. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.
In addition to the Privacy Impact Assessment, the SORN will be updated as the ENOS system is modified or upgraded.

Conclusions and Analysis

1. Did any pertinent issues arise during the drafting of this Assessment?
No.

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

See Attached Approval Page

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

IT Security Manager
Privacy Act Officer

The Following Officials Have Approved this PIA	
System Manager (Project Manager)	
Edward V. Graham Digitally signed by Edward V. Graham DN: cn=Edward V. Graham, o=Project Management Division, ou=IJ, email=edward.graham@nara.gov, c=US Date: 2020.04.09 11:01:11 -04'00' (Signature)	(Date)
Name: Edward Graham	
Title: ISE/NISP Program Manager	
Contact information: Phone: 301-837-3537 Email: edward.graham@nara.gov	
Senior Agency Official for Privacy (or designee)	
GARY STERN Digitally signed by GARY STERN Date: 2020.03.26 15:59:05 -04'00' (Signature)	(Date)
Name: Gary M. Stern	
Title: General Counsel and Senior Agency Official for Privacy	
Contact information: Phone : 301-837-3026Email: garym.stern@nara.gov	
Chief Information Officer (or designee)	
SWARNALI HALDAR Digitally signed by SWARNALI HALDAR Date: 2020.04.13 11:36:45 -04'00' (Signature)	(Date)
Name: Swarnali Haldar	
Title: Chief Information Officer	
Phone : 301-837-1583 Email: swarnali.haldar@nara.gov	