

Privacy Impact Assessment (PIA)

Name of Project: Edocs Upgrade

Project's Unique ID: CPIC# 3020P

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

Purpose of this System/Application: This system is a technical refresh of OFR's existing eDOCS application for processing documents for publishing in the Federal Register and associated document workflows, such as the production of Slip Laws and the annual Statutes at Large.

Section 1: Information to be Collected

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

Employees	Userid, name, and associated email address.
External Users	Userid, name, associated email address, and phone number
Audit trail information (including employee log-in information)	The system will have a log of various user actions to include logins and actions taken on documents processed by the system.
Other (describe)	

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

NARA operational records	None
External users	Only information provided by external users when registering for an account.
Employees	Only information provided by employees when creating an account.
Other Federal agencies (list agency)	Submitted Federal Register documents (Notices, Rules, Proposed Rules, Presidential documents, and supporting materials).
State and local agencies (list agency)	None

Other third party source	None
--------------------------	------

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.
 The userid is necessary in order to authenticate the user.
 The email address is necessary for sending system notifications.
 Name and telephone are necessary to contact submitters for clarifying information.

2. Is there another source for the data? Explain how that source is or is not used?
 No.

Section 3: Intended Use of this Information

1. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?
 No.

2. Will the new data be placed in the individual's record?
 Not applicable - no new data.

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 user.

4. How will the new data be verified for relevance and accuracy?
 Not applicable - no new data.

5. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
 There is no data consolidation. The system contains strong safeguards to protect user information and to limit the access to that information to the user and certain approved administrators. These security

controls are described in depth in the various system security plans.

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

No existing processes are being consolidated.

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

Data will be retrieved by the end user via the user interface of the application only after user identification and authentication.

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.

No.

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

Managers can retrieve productivity reports on individual OFR users for the purpose of managing employees and workloads.

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

Yes. The public can only access publicly posted documents (e.g., Public Inspection version of documents posted to the Public Inspection website). Non-OFR users can only submit documents for processing and retrieve status information. OFR users can access most information about documents being processed, as defined by the security controls associated with the role within the system.

11. Will this system be used to identify, locate, and monitor individuals? If yes, describe the business purpose for the capability and the controls established explain.

No.

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

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?

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)?

Authorized users and contractors as designated by NARA will be able to use the system, but only designated system administrators would have admin access.

2. How is access to the data by a user determined and by whom? Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where are they documented (e.g., concept of operations document, etc.). Are safeguards in place to terminate access to the data by the user?

The system employs role-based security. Roles and access are determined by OFR leadership.

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

Explain.

OFR users can access information about documents being processes, as defined by the security controls associated with the role within the system.

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?

System security controls are documented in the SSP. Audit trails can be used to determine actions by users.

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, and yes.

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.

No.

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

Not applicable.

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

The system does not maintain any information about the public. No non-public information is maintained on 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.

Non-OFR users can only retrieve status information regarding documents they have submitted for

processing.

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?

N/A

2. 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.).

N/A

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

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

Retention periods for the archival and disposition of documents and metadata are defined by Chapter 15 of the NARA Records Schedule .

4. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented? Cite the

disposition instructions for records that have an approved records disposition in accordance with, FILES 203. If the records are unscheduled that cannot be destroyed or purged until the schedule is approved.

Disposition instruction for documents and metadata are defined by Chapter 15 of the NARA Records Schedule.

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?

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?

Yes.

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

Security scans are completed by NARA IT Security. Monitoring will be provided by the AWS cloud provider.

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

The points of contact are Aaron Woo, Krishna Kumar, and Keith Day.

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.

Not applicable.

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

Not applicable.

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.

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:

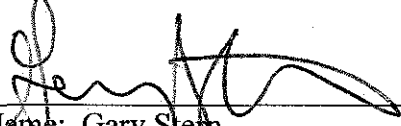
IT Security Manager
Privacy Act Officer

The Following Officials Have Approved this PIA

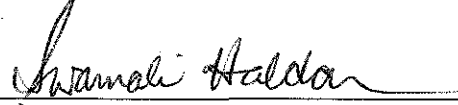
System Manager (Project Manager)

(Signature)	(Date)
Name: Sambandham Krishnakumar	
Title: Project Manager	
Contact information: Sambandham.Krishnakumar@nara.gov	

Senior Agency Official for Privacy (or designee)

 (Signature)	8/15/14 (Date)
Name: Gary Stern	
Title: NARA General Counsel	
Contact information: garym.stern@nara.gov	

Chief Information Officer (or designee)

 (Signature)	8/25/14 (Date)
Name: Swarnali Haldar	
Title: CIO	
Contact information: swarnali.haldar@nara.gov	