

## Privacy Impact Assessment (PIA)

**Name of Project: Electronic Records Archives (ERA) 2.0**

**Project's Unique ID: ERA 2.0**

**Legal Authority(ies):**

44 U.S.C. 2203. and 44 U.S.C. 2107

**Purpose of this System/Application:** ERA 2.0 is intended to preserve and provide access to the content of born-digital records and digital surrogates in NARA's holdings that are determined by the Archivist to have sufficient historical or other value to warrant continued preservation by the United States Government.

### Section 1: Information to be Collected

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

**Employees**

NARA users of ERA 2.0 will provide agency specific information rather than personal information in order to be granted a user account to the system. The Service Desk collects the employee's Name (First and Last Name), NARANet User ID, Job Title, Job Status (Federal / Contractor), NARA Business Unit / Preservation Group, ERA 2.0 Role, Work Email and Work Phone Number for account management purposes.

The specific information utilized to create an application user account in ERA 2.0 is the employee's NARANet User ID and NARA Business Unit / Preservation Group. Employee application user accounts are represented as entries in the ERA 2.0 PostgreSQL Database.

The specific information utilized to create a System Administrator user account in ERA 2.0 is the employee's Name and a User ID (assigned by O&M staff using a combination of the employee's Name). Employee System Administrator user accounts are represented as entries in the ERA 2.0 ApacheDS.

The specific information utilized to create an AWS IAM account for ERA 2.0 is the employee's User ID (assigned by O&M staff using a combination of the employee's Name). Employee AWS IAM user accounts are represented as entries in the AWS Management Console.

**External**

Employees of other federal agencies will provide agency specific information

<b>Users</b>	<p>rather than personal information in order to be granted a user account to the system. The Service Desk collects the external user's Full Name (First, Middle, Last), User ID (assigned at time of account creation), Agency Account Manager, Agency Account Manager Email, Job Title, Job Status (Federal / Contractor), ERA 2.0 Role, Work Address, Work Email and Work Phone Number for account management purposes.</p> <p>The specific information required to create an account in ERA 2.0 is the employee's Full Name, a User ID (assigned by O&amp;M staff using a combination of the employee's Full Name), and their agency IP address to add to an access whitelist.</p>
<b>Audit trail information (including employee log-in information)</b>	All login attempts, whether they succeed or fail, are logged and recorded in the data warehouse. The User ID (Username) and IP address is recorded in the application and system logs; no other personal related information regarding the user is recorded.
<b>Other (describe)</b>	
<b>Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?</b>	
<b>NARA operational records</b>	N/A
<b>External users</b>	Information is obtained directly from external Federal employees who need ERA 2.0 accounts
<b>Employees</b>	Information is obtained directly from NARA employees who need ERA 2.0 accounts
<b>Other Federal agencies (list agency)</b>	<p>Information on individuals contained in Federal records stored in ERA 2.0 as accessions in the legal custody of the National Archives. This information, subject to FOIA, may not be releasable under exemptions (b)(6) and (b)(7)(C) of the FOIA. Note: Accessioned records are specifically exempt from most provisions of the Privacy Act.</p> <p>Information on individuals contained in Presidential records stored in ERA 2.0 in the legal custody of the National Archives is controlled by the PRA (44 U.S.C. Chapter 22), Executive Order 13489, and the privacy exemptions - (b)(6) and (b)(7)(C) - of the FOIA.</p> <p>Information on individuals contained in records of the Congress, legislative branch agencies, and judicial branch records are controlled by directions of the originating governmental body and NARA's general restrictions (36 C.F.R. 1256, Subpart D).</p>
<b>State and local agencies (list agency)</b>	No state or local governmental agencies will provide data directly to NARA for use in ERA 2.0. However, there may be personal data previously received by Federal agencies from state and local government sources that is present in the Federal records stored in ERA 2.0.
<b>Other third</b>	Information on individuals contained in donated archival materials is controlled

party source | | by directions of the donor's deed of gift.

## Section 2: Why the Information is Being Collected

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

ERA 2.0 requires the minimum information needed to uniquely identify users as well as provide contact information used to determine or verify access to data stored in ERA 2.0. Data identifying these users and their access rights, and describing their use of ERA 2.0, is necessary for system management and security and as a control against fraud, waste and abuse.

For information on individuals contained in records stored in ERA 2.0, preserving and providing appropriate access to this data is the purpose of ERA 2.0 in fulfillment of the agency's mission.

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

The information is not available from a different source.

## 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?

ERA 2.0 will neither derive new data nor create previously unavailable data about an individual through information aggregation.

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

N/A

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

N/A

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

N/A

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

NARA staff and government contractors responsible for managing and operating ERA 2.0 will have access to the PII data about ERA 2.0 system users. Service Desk staff responsible for responding to user requests for assistance will have access to data necessary to provide assistance. ERA 2.0 users performing system management can retrieve user account information by a search on a unique user identifier or user name.

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

Management, operational, and technical controls to prevent misuse of data by those with privileged access have been selected in accordance with NIST SP 800-53/FIPS PUB 200. ERA 2.0 system components implementing these controls detect unauthorized access and unauthorized monitoring. Continuous monitoring is in place to ensure effective security controls.

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

For NARA operational PII data (in support of system user accounts), the NARA Delegated Account

Representatives (DAR) will have user account information for those users whom they recommend for ERA 2.0 accounts. The DAR will not have access to any other ERA 2.0 user information. Service Desk staff responsible for responding to user requests for assistance will have access to data necessary to provide assistance. ERA 2.0 users performing system management can retrieve user account information by a search on a unique user identifier or user name.

For archival holdings stored in ERA 2.0, users will be able to query the contents and metadata of records available to them according to the Business Unit and Preservation Groups to which the users have been assigned.

**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.**

Data about registered ERA 2.0 system users will be retrievable by personal identifiers by the privileged users who maintain the system. Service Desk and support staff with access to the authentication system can retrieve user account data by searching on username, first name, last name, or email address.

Where personal identifiers may appear in digital files maintained as archival holdings in ERA 2.0 those records may be queried by NARA archival users.

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

Reports in ERA 2.0 are not produced specifically on individuals. Regular reports can be generated on system accounts that have passed thresholds for inactivity. These reports are generated for maintenance of the system and to ensure user accounts no longer requiring access to data in the system can be deactivated in a timely manner.

**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.**

No

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

Audit logs of users who access the system to perform authorized actions on the system in accordance with their job responsibilities will be captured within the system at the application level for user's with and the infrastructure level for privileged users.

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

Audit logs will only be accessible to authorized individuals.

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

ERA 2.0 uses browser cookies to maintain user authentication information. Additional user context is contained within the URL.

#### **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)?**

NARA staff and government contractors responsible for managing and operating ERA 2.0 will have access to the PII data about ERA 2.0 system users. Service Desk staff responsible for responding to user requests for assistance will have access to data necessary to provide assistance. ERA 2.0 users performing system management can retrieve user account information by a search on a unique user identifier or user name. ERA 2.0 reports containing PII data, such as user id, of ERA 2.0 system users may be utilized by NARA staff for account usage monitoring and reauthorization activities as directed by the NARA IT Security Requirements.

**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 following restrictions are in place in ERA 2.0 for user access to information.

For NARA operational PII data (in support of system user accounts), the NARA Delegated Account Representatives (DAR) will have user account information for those users whom they recommend for ERA 2.0 accounts. The DAR will not have access to any other ERA 2.0 user information. Appropriate ERA 2.0 system maintenance staff will have access to all user account information.

For archival holdings stored in ERA 2.0, access to data will be based on the user's NARA organization, confirmed during the account request process, and will be enforced by system rules.

ERA 2.0 user accounts will be reviewed on a defined recurring basis as directed in the NARA IT Security Requirements.

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

User access is determined by role, and the aspects of logical control called Business Unit and Preservation Group. Within the Process system component users will only be able to see and process materials belonging to their Business Unit. Digital materials are assigned to only one Business Unit, and users can only belong to one Business Unit as well. Within the Discover component digital materials are stored in one Preservation Group, and users are granted access to these materials based which Preservation Groups they have been assigned.

System maintenance staff have technical access to all data, but they are not given permission to access the data unless it is required to perform a specific task to maintain 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?**

Management, operational, and technical controls to prevent misuse of data by those with privileged access have been selected in accordance with NIST SP 800-53/FIPS PUB 200. ERA 2.0 system components implementing these controls detect unauthorized access and unauthorized monitoring. Continuous monitoring is in place to ensure effective security controls.

Annual assessments of the selected security and privacy controls will be conducted by NARA's independent assessors at the direction of the NARA IT Security Management Division (IS).

All NARA users receive mandatory annual holding protection training to prevent the misuse of the data contained in the system.

**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.**

ERA 2.0 will share data with NARA's Description and Authority Service (DAS). DAS includes standardized descriptions of both non-electronic and born digital holdings, as well as links to other descriptive contents. In support of the creation of archival descriptions ERA 2.0 will share with DAS elements of non-private descriptive metadata intended for public access via NARA's Catalog.

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

DAS has an approved Security Certification, but did not require a Privacy Impact Assessment.

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

General responsibility for protecting personal privacy information in materials in NARA's custody rests with the Archivist of the United States in accordance with the FOIA, 5 U.S.C. 552, as amended; the Privacy Act, 5 U.S.C. 552a, as amended; the Federal Records Act, 44 U.S.C. 2108; and the Presidential Records Act, 44 U.S.C. 2204 and 2207.

The ERA 2.0 Designated Approving Authority will have the responsibility for protecting the privacy of personal information that is required submit an account on the NAC system. The Designated Approving Authority also has the responsibility for ensuring the controls implemented within ERA 2.0 are protecting the privacy of personal information that is specifically stored within the ERA 2.0 system.

The NARA Senior Agency Official for Privacy is the NARA General Counsel (NGC). The General Counsel will provide legal guidance and has overall responsibility and accountability for ensuring NARA's implementation of information privacy protections, including NARA's full compliance with federal laws, regulations, and policies relating to information privacy.

**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.**

Other agencies will log in to ERA 2.0 to transfer records. They will not have access to any information other than that pertaining to their agency.

Any governmental entity requesting access to unopened archival records, other than records they

created, held in ERA 2.0 will coordinate their request for access with the respective NARA archival custodial units who manage access to their records. The archival custodial units will provide access to requested records in compliance with the requirements of FOIA, the PRA (for Presidential records), the directions of the originating governmental body (for records of the Congress, legislative branch agencies, and judicial branch records), or the donor's deed of gift (for donated archival materials).

Opened archival records are made available to the public through the National Archives Catalog, and by other means.

### **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 ERA 2.0 account management form lists the data required for an account on the system. The required fields are designated and users can decline to provide any optional information requested on the form. There is no opportunity to decline to provide the required information if an individual requires access to the system in order to perform his/her official duties.

There are no additional uses of the information so there is no need to seek consent for other uses.

**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.).**

User account information collected by ERA 2.0 will be verified, to the extent practicable, for accuracy and that the information is current and complete. This information will be used to verify the identity of ERA 2.0 users to ensure the protection of privacy records within the system. The electronic account information stored in ERA 2.0 is verified for accuracy, relevance, timeliness, and completeness on an annual basis.

The creators of the archival holdings stored in ERA 2.0 are responsible for the quality of the data transferred into the legal custody of NARA.

**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?**

Consistency of operation and data between availability zones is a function that is intrinsic to AWS.

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

The born-digital records and digital surrogates held in the system that have been determined by the Archivist to have sufficient historical or other value to warrant continued preservation by the United

States Government will be retained in ERA 2.0 for the life of the system.

**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.**

System generated records, such as audit logs, are retained in accordance with the General Records Schedule.

Archival records held in the system that have been determined by the Archivist to have sufficient historical or other value to warrant continued preservation by the United States Government will be retained in ERA 2.0 for the life of the system.

**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.**

ERA 2.0 is the first natively built cloud-based application for NARA. It utilizes many of the services provided by the cloud vendor to ensure high availability, elasticity, and security.

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

By utilizing built-in cloud security features, and specifically by hosting ERA 2.0 in the AWS GovCloud region, many of the security controls necessary to keep data within the application are automatically inherited by ERA 2.0. ERA 2.0 system leverages the pre-existing FedRAMP Authorization for AWS GovCloud.

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

The system has been designed and built to meet NARA IT Security Requirements as well as requirements of the NIST SP 800-53 Moderate Baseline and FedRAMP requirements for cloud based systems.



**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?**

A risk assessment is scheduled to be performed as part of the initial security assessment performed by NARA's independent assessors. A Risk Assessment Report (RAR) will be prepared by the independent assessors and will be used by the NARA Designated Approval Authority (DAA) and the Senior Agency Official for Privacy (SAOP) in their determination to grant an Authorization to Operate (ATO) to the system. Mitigations for identified risks will be tracked in a Plan of Action and Milestones (POA&M) in order to ensure safeguards are in place to protect information processed by the system. Physical controls will be in place to restrict access to the system infrastructure and they are inherited from FedRAMP ATO for GovCloud. All data is encrypted at rest and in transit.

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

An initial security assessment is scheduled to be conducted by NARA's independent assessors. A Security Assessment Package will be prepared by the independent assessor that includes a Security Assessment Report (SAR), RAR, POA&M, and Certifier's Recommendation. Once an ATO has been granted for the system by the DAA, the annual assessment of select security and privacy controls will be conducted by NARA's independent assessors. The SAR, RAR, and POA&M will be updated accordingly based on the results of the annual assessment. In addition to the annual assessment of security and privacy controls implemented on the system, NARA will continuously monitor the system for vulnerabilities and configuration compliance.

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

Sam McClure - System Owner  
[sam.mcclure@nara.gov](mailto:sam.mcclure@nara.gov)  
301-837-1958

**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.**

ERA 2.0 is not a system of records covered by the Privacy Act.

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

N/A

### **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?**

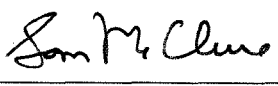
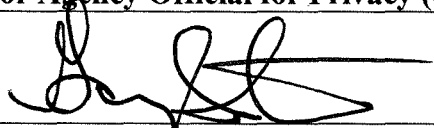
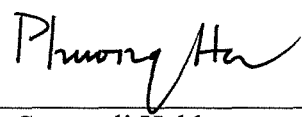
N/A

### **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**

<b>System Owner</b>	
 (Signature)	7/26/18 (Date)
Name: Sam McClure	
Title: Electronic Records Program Director	
Contact information: 8601 Adelphi Road, Room 4108, College Park, MD 20740-6001 (301) 837-1958, sam.mcclure@nara.gov	
<b>Senior Agency Official for Privacy (or designee)</b>	
 (Signature)	7/25/18 (Date)
Name: Gary M. Stern	
Title: General Counsel	
Contact information: 8601 Adelphi Road, Room 3110, College Park, MD 20740-6001 301-837-3026, Gary.stern@nara.gov	
<b>Chief Information Officer (or designee)</b>	
 (Signature)	8/2/18 (Date)
Name: Swarnali Halder      PHUONG HA - Acting CIO	
Title: Executive for Information Services/CIO (I)	
Contact information: 8601 Adelphi Road, Room 4415, College Park, MD 20740-6001 301-837-1583, swarnali.haldar@nara.gov	