

Privacy Impact Assessment (PIA)

Name of Project: History Hub

Project's Unique ID:

Legal Authority(ies): 44 USC. 2104

Purpose of this System/Application: History Hub is an online community managed by the National Archives for researchers, citizen historians, archival professionals, and open government advocates. It uses social media tools and discussions to allow the public access to NARA subject matter experts and to crowdsource information from other experts and users.

Section 1: Information to be Collected

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

Employees	For employees that sign up for a History Hub account, NARA requires: first and last name, email, and password. Employees can also identify themselves as working at NARA and provide their title as well as a biography.
External Users	For external users that sign up for a History Hub account, NARA requires: first and last name, email, and password. Employees of other agencies can be designated as “experts” with their agency logo.
Audit trail information (including employee login information)	
Other (describe)	
Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?	
NARA operational records	No information about users is obtained from other NARA systems or files
External users	External users provide information directly to the History Hub application
Employees	Employees provide their information directly to the History Hub application
Other Federal agencies (list)	When employees of other agencies use History Hub, they provide their information in the same way as external users or NARA users

agency)		
State and local agencies (list agency)		n/a
Other third party source		n/a

Section 2: Why the Information is Being Collected

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

Yes, for the system to work as a collaboration tool, users need to be identifiable. Employer and job title can be helpful information to judge the quality or trustworthiness of an answer provided in the forum.

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?

Information about a person's expertise or research area may be revealed by that person in the conversations that take place on the platform. Most information is maintained on the platform and is accessible to everyone, with the exception of a few private groups used for management of the platform. Users may provide an email address and sign up for notifications when they receive direct messages on the platform. These messages are managed with the History Hub platform.

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

The information will remain in the History Hub platform. It is not exported in the regular course of business.

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

No.

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

Information is provided by individuals voluntarily. Where information is inaccurate, it is the expectation that members of the crowd will identify the inaccuracy and provide accurate information, through crowdsourcing.

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

Data is not being consolidated.

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

n/a

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

Data on History Hub can be retrieved by searching and browsing. It is possible to click on an individual user's profile and see all of their public activity.

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 is retrievable by username on the site. SSNs are not collected.

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

History Hub allows users and system administrators to sort information by the creator of the content to see what information the user has shared in the system.

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

The information members of the public and employees share on History Hub may enable each to make more informed decisions, including focusing on what the researchers' needs are and where the information they need may be located.

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, though the system will make it possible to view an individual's contributions to the platform.

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

No information is collected other than what the individual provides voluntarily.

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

The system contains audit logs which can be reviewed.

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

Yes, the application uses several cookies to provide a better user experience, including cookies used for collecting web analytics. Information on how to opt out of cookies is included in the archives.gov privacy policy. Individuals can also choose not to check "remember me" when logging in, which will ensure a cookie is not set for their History Hub profile.

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)?

System administrators, including contractors that are part of development efforts, are able to have access to the administrative data. Most of the content in the system is public facing.

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?

Yes, users can delete any of their own data themselves. Administrators can also delete any information.

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

Users will have all access to public data on the system. Users can set information in their profiles to be restricted only to contacts, however.

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?

Access to admin panels is restricted to admin logins only.

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.

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.

Not at this time, but NARA plans to integrate employee accounts for the Internal Collaboration Network with History Hub, which run on the same platform. Employees would then be able to post in either forum without separately logging in.

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

Yes

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

The system administrators and the privacy office.

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.

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?

History Hub is entirely voluntary. If individuals do not want to sign up and provide information, they do not have to. Much of the information is available to browse without logging in.

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

If a system user was removed from the system because they had abused the platform, they would be allowed to contact NARA about the decision. Depending on the severity of their actions, they may or may not be given a chance to respond prior to being removed.

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 information is provided by individuals directly.

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 site is cloud hosted and thus remains in sync across all physical sites it is used in.

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

These records have not yet been scheduled.

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.

n/a

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 technology provides a platform for members of the public and employees to communicate, giving them the choice as to what to share.

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.

The system is hosted in a FedRamp compliant data center in the United States and receives regular

security scans.

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

Kelly Osborn, 301-837-0870, Kelly.osborn@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.

n/a

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

Conclusions and Analysis

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

n/a

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

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)

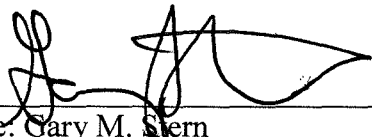
 (Signature) 6/22/18 (Date)

Name: Dana Allen-Greil

Title: Web and Social Media Branch Chief

Contact information: dana.allen-greil@nara.gov

Senior Agency Official for Privacy (or designee)

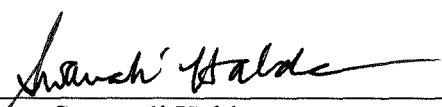
 (Signature) 6/19/18 (Date)

Name: Gary M. Stern

Title: General Counsel

Contact information: garym.stern@nara.gov

Chief Information Officer (or designee)

 (Signature) 7/13/18 (Date)

Name: Swarnali Halder

Title: CIO

Contact information: swarnali.haldar@nara.gov