Privacy Impact Assessment (PIA)

Name of Project: Internal Collboration Network

Project's Unique ID:

Legal Authority(ies):	44 USC 2104

Purpose of this System/Application:
The Internal Collaboration Network (ICN) is a place to collaborate on ideas and projects, to share information, and to build relationships across departments.

Section 1: Information to be Collected

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

Employees		Contact information for all employees is pulled from the NARA LDAP, including name (first and last), work email, and work telephone number. Employees are also asked to provide their employment category. Employees may provide information related to their job, including title, department, address, date of hire, organization code, location, professional affiliations, interagency committees, and certificates. Other information, such as personal contact information (including home address and telephone number, email address, blogs, social media accounts), biography, expertise, and hobbies may be provided at the user's discretion. Users can set privacy settings to limit or restrict access to the voluntary information they provided.
External Users		To the extent that contractors have accounts on the ICN, the information available about them is the same as the information available discussed above for employees.
Audit trail information (including employee log-in information)		The username for ICN users will be the unique username provided by NARA. The password is the same password used for accessing NARANet systems.
Other (describe)		

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

NARA operational records		Name, office phone number, email address.
External users		None
Employees		Employees are asked to provide their employment category. Employees may provide information related to their job, including title, department, address, date of hire, organization code, location, professional affiliations, interagency committees, and certificates. Other information, such as personal contact information (including home address and telephone number, email address, blogs, social media accounts), biography, expertise, and hobbies may be provided at the user's discretion.
Other Federal agencies (list agency)		none
State and local agencies (list agency)		none
Other third party source		non

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.
Yes, required data elements (including first and last name, work email, and employment category) are necessary to identify users. Other data elements may be provided at the discretion of the users.

2. Is there another source for the data? Explain how that source is or is not used?
The sources for the data are NARA's LDAP system, used to sign on to all NARA work stations, and information provided at the discretion of the user.

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?
New information may be created in the form of blogs, conversations, groups, and projects, all of which may contain information about individuals. The information will be maintained on the ICN.

2. Will the new data be placed in the individual's record?
The information will not, as a matter of course, be placed in an employee's official personnel record or unofficial record. If an employee misuses the system, information about that misuse may become part of their record.

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

No, the system cannot make determinations about employees.

4. How will the new data be verified for relevance and accuracy?
Not applicable.

5. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
The ICN is available only to those with NARANet accounts. The ICN is hosted in a FISMA-moderate secure environment.

6. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.
Yes, controls on access to the system are part of the FISMA security controls in place.

7. Generally, how will the data be retrieved by the user?
Through an account on the ICN accessed by NARANet username and password.

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.
Yes. Data can be retrieved by name. Social Security numbers are not collected by the system.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?
The system keeps track of activity on the ICN. This can be accessed by anyone through viewing a person's activity feed. This information shows level of engagement and content generated by each individual. Individual users are able to set privacy controls on portions of their profile field and have private discussions and groups on the platform if they choose.

10. Can the use of the system allow NARA to treat the public, employees or other persons

differently? If yes, explain.
No, only NARA employees and contractors will be allowed access to the system. Members of the public will not be allowed access.

Individual users of the system may choose how they treat other system users, but the platform's terms of use specify what is acceptable behavior.

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?
Each user is allowed to establish privacy settings on their profile. They do not need to provide any personal info, if they do not want to do so.

In addition, the security setup of the network, including is integration with NARANet's sign on directory ensures that only authorized users are allowed access.

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

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, system administrators, and network administrators will have access to the data. Users include NARA employees, contractors, interns and volunteers.

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?
Access to the network and content on the network is given to NARA employees, contractors, interns, volunteers, and network administrators. When an employee leaves NARA, their access is revoked. Login is controlled by NARANet access.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.
Access will be based on the user type with varying levels of access granted. Users can set privacy settings to restrict access of PII on their profiles. Additionally, users can set groups to private or secret and control access to those groups.

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?

FISMA moderate controls are in place, so that the system can only be accessed by authorized NARANet account users.

All content on the ICN is contributed voluntarily, and each user is responsible for their own privacy settings. Group owners are responsible for ensuring a group is not accessible to a category of users who should not have access.

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 will perform system maintenance. All regulatory and legal requirements were included in the contract, including Privacy Act clauses.

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.
Yes. Login and password are pulled from data on the LDAP. No data is provided to another system, though.

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?

Members of the public are not able to access the ICN. Employees have the capability to set their own privacy settings, and thus ensure only information they want shared will be shared with other ICN users.

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?
Users are responsible for updating their profile from the default setting, which shows only the user's name and work email address, and maintaining any optional information shared by the user.

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

No final action is taken in the ICN, and all information can be updated and changed as needed.

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.).

PII in the system is provided by the user. We assume the individual is providing accurate, timely and complete information regarding themselves and their content.

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?
All content is contained in an Oracle database.

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

The information is not being disposed of as it is not yet scheduled.

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.

Yes. We're using Jive Social Business Software to communicate and collaborate across geographic locations and business areas.

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

Employees have increased individual control over how much information they share about themselves and with whom they share their information.

7. Does the system meet both NARA's IT security requirements as well as the procedures required by federal law and policy?
Yes, the system has been reviewed by the NARA IT security staff and is certified in a FISMA moderate level.

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?

No additional risks were identified.

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

The system is maintained and monitored by NTIS, part of the Department of Commerce in a FISMA certified environment.

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

Kelly Osborn
Information Technology Specialist
Kelly.osborn@nara.gov
301-837-0870

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 42

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

The system of records notice is being published in conjunction with the PIA

Conclusions and Analysis

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

No, privacy considerations were incorporated into the initial design of the system.

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 (P~~roject Manager)~~	
Pamela Wright (Signature)	9/10/12 (Date)
Name: PAMELA WRIGHT	
Title: Chief Digital Access Strategist	
Contact information:	
Senior Agency Official for Privacy (or designee)	
(Signature)	9/10/12 (Date)
Name: Gary M. Stern	
Title: General Counsel & SAOP	
Contact information:	
Chief Information Officer (or designee)	
Michael Wash (Signature)	9/12.12 (Date)
Name:	
Title: CIO	
Contact information:	