

Privacy Impact Assessment (PIA)

Name of Project: NARAnet

Project's Unique ID: NARAnet

Legal Authority(ies): 44 USC 2102, 2103, 2104

Purpose of this System/Application: NARAnet is a general support system (GSS) utilized as NARA's information technology infrastructure on which agency administrative and mission activities are accomplished electronically. NARAnet connects the entire agency internally and the agency to its public and government customers via the Internet. NARAnet fosters the agency's ability to create, maintain, retrieve, and analyze vital agency resources and information for sharing essential evidence. NARAnet also provides the network backbone needed to support distributed access to all NARA electronic access systems. NARAnet provides files, print and e-mail services for the agency.

NARAnet provides a transmission medium for NARA's IT systems. It does not in and of itself control other system's PII data. The system does not have any mechanisms which are designed to recognize, or extract PII data, and does not have any mechanisms designed to protect PII data other than access controls that limit user access to the data they are authorized to see.

During FY2013, as part of NARA's migration of email to a cloud service provider, it became necessary to collect small amounts of PII in order to facilitate its two-factor authentication to the cloud email provider and the telework environment. Integrated into the email system is ZL Tech's Cloud-based Unified Archiving solution, EMM's Cloud-based Blackberry service, and a SecureAuth appliance installed within NARAnet. Each system will have similar read-only access to NARA's eDirectory for authentication. This information is stored in the Identity Vault application which is integrated with eDirectory.

NARAnet end users may store other data on NARAnet servers that may contain PII, but that data is the responsibility of the data owner to manage and control.

Section 1: Information to be Collected

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

Employees	Personal telephone number (mobile or home number) and/or email address are the only currently-used fields in the Identity Vault that contain Personally Identifiable Information.
External Users	For contractors, volunteers, or other persons doing business on NARA's behalf, the user's private email address or phone number will be collected if they use the telework or email system from outside NARAnet (e.g. from home or a non-NARA issued device such as a cell phone).
Audit trail information	The system will have a log of user logins.

(including employee log-in information)		
Other (describe)		N/A
Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?		
NARA operational records		The Google directory will contain e-mail addresses synchronized from the NARA eDirectory
External users		The email address of an external addressee and their name will be captured by the system.
Employees		Employees e-mail address, name, and work contact information will be captured from the employee directory. Employees will be able to update this information in the employee directory.
Other Federal agencies (list agency)		The email address of an external addressee and their name will be captured by the system.
State and local agencies (list agency)		The email address of an external addressee and their name will be captured by the system.
Other third party source		The email address of an external addressee and their name will be captured by the system.

Section 2: Why the Information is Being Collected

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

Yes. In order to authenticate to the telework or email environments, the user must enter a PIN number. In order to meet the requirement for a second factor of authentication from outside the NARAnet boundary, the authentication system sends the PIN to the users' phone or a personal email address.

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

Yes. The user enters the data into the Employee Locator application (not within the system boundary of NARAnet). The data is pulled from the Employee Locator and placed in NARAnet's Identity Vault. This allows end users to easily update their information, so that it is accurate at all times, without compromising the security of Identity Vault by allowing end user access.

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. The information is provided by the user.

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

No.

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

No, the Identity Vault performs no determinations. The data contained in the Identity Vault is contact

information for those employees, contractors, volunteers and others working on behalf of NARA who use NARA's telework solution, or who wish to access NARA's email system from outside NARA's domain.

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

The user provides the data on a voluntary basis. The user has the ability to correct and update their information as necessary. It is the user's responsibility to update the information if it changes.

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 within the system. The controls are discussed more fully below in Section 4.

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

No processes are being consolidated.

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

The user accesses their information through the Employee Locator. Once the basic information regarding the user's work information is entered, the user receives a confirmation email at their nara.gov address. The user clicks on the link to confirm the work information and is given access to the page where they input their personal information. Once they complete entering their personal information, they confirm the changes. The data is then synchronized with the Identity Vault.

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.

From the Identity Vault or eDirectory, it is possible to retrieve the data by user name and/or email address.

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

From the Identity Vault, it is possible to produce a report of the user's name, personal phone number, login activity, and personal email address. Pulling these reports is not done as a matter of course. Only the IT system administrators contracted to manage this system can access this information.

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

Limited calendar data will be visible to the public (busy v. free time) whereas full details can be shared with internal employees. Non-NARA users cannot see a NARA employee's chat status. Before sharing a document with an external user, the NARA user will receive a pop-up warning that the recipient is outside of NARA's domain.

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?

N/A, see question 11.

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

N/A, see question 11.

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

No.

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 employees, interns, volunteers, and contractors who have been provided a NARA email address will be able to use the system. Only contractors, system administrators, and developers will have access to the data as it resides in the Identity Vault.

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 data in the Identity Vault is not accessible by non-privileged end-users. It is only accessible to contractors, system administrators, and developers who are contracted to use and maintain the system.

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

Explain.

End users do not have access to the Identity Vault data. Privileged users have only the access needed to carry out their job duties. End-users generally only have access to data they are authorized to see, such as their office shared drive or office files.

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?

NARANET components (firewalls, switches, and routers) do restrict access to non-public facing, internal systems/applications residing on NARANET. However, NARANET does not have any mechanisms which are designed to recognize, process or extract PII data, and does not have any mechanisms designed to protect PII data other than the access controls which limit user access to the data they are authorized to see. Individual data owners are responsible to manage and secure any PII data which resides in NARANET according to agency directive.

The system will keep a log of all administrator actions on the system. Administrative access is only provided to NARA-authorized individuals by granting the appropriate roles/permissions to the user. Monitoring of the log data is described in NARA's Cloud Email A&A documentation.

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?

Contractors are involved in the design and development of the system. IT Support contracts have the necessary Privacy Act contract clauses in place.

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 data is provided to the Identity Vault through synchronization with eDirectory which links with the Employee Locator, which is part of a collection of web servers owned by the Web and Social Media Branch of the Office of Innovation.

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

The collection of web servers is not a FISMA-reportable system. NARANet, which houses eDirectory and the Identity Vault, is a FISMA-reportable system, has received Security Certification and has a Privacy Impact Assessment on file.

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

Individual data owners are responsible for managing and securing any PII data which resides in NARANET according to agency directive. The system can be configured to search for plain-text SSN patterns in outgoing messages and prevent those types of messages from being sent, or alerting an administrator that such a message was sent. The public is not affected by the system.

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.

The data in the Identity Vault will not be shared with other agencies at this time.

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 information is provided by the users themselves. If they do not consent to the use of the information, they simply do not have to provide the information. They can access the systems remotely still by allowing a voicemail to be left on their office phone with their PIN number, and then calling in to retrieve that PIN.

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

The data in the Identity Vault is not made to make any determinations.

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.).

It is the responsibility of the user to ensure that the data is accurate. The Security Management Division uses the data as it resides in the Employee Locator for Continuity of Operations activities. From time-to-time, they ask for updates to the data, which is then synchronized with the Identity Vault.

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?

Currently the information in the Identity Vault is backed up to the enterprise storage area network

(SAN).

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

Email records of senior officials will be permanently maintained. Email records of non-senior officials will be maintained for seven years. The system log files and other similar records will be managed under NARA's records schedule or the General 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.

The process for deletion of data is documented in Google's SSP which has been reviewed by NARA's security team and is available for additional review at Google's location should it be needed. At a high level the process is summarized below.

Google Apps for Government is operating under an Authorization to Operate (ATO) issued by NARA on June 24, 2014 and is subject to continuous security assessment and authorization.

Agency policy and user discretion govern the actual deletion of data from user control. Once a user has deleted information, Google Apps removes the information from the Google File System as described below.

Deleted Data

After a Google Apps user or Google Apps administrator deletes a message, account, user, or domain, and confirms deletion of that item (e.g., empties the Trash), the data in question is removed and no longer accessible from that user's Google Apps interface.

The data is then deleted from Google's active servers and replication servers. Pointers to the data on Google's active and replication servers are removed. Dereferenced data will be overwritten with other customer data over time.

Media Disposal

When retired from Google's systems, disks containing customer information are subjected to a data destruction process before leaving Google's premises.

First, Google requires the disk to be logically wiped by authorized individuals. The erasure consists of a full write of the drive with all zeroes (0x00) followed by a full read of the drive to ensure that the drive is blank. Then, another authorized individual is required to perform a second inspection to confirm that the disk has been successfully wiped. These erase results are logged by the drive's serial number for tracking.

Finally, the erased drive is released to inventory for reuse and redeployment. If the drive cannot be erased due to hardware failure, it must be securely stored until it can be destroyed. Each facility is audited on a weekly basis to monitor compliance with the disk erase policy.

ZL Tech

Additionally, NARA's email records will be managed by ZL Tech's Unified Archiving solution that is integrated into the system. NARA's email records retention policies will be enabled within this portion of the system and will provide for email Archiving, Records Management, and e-Discovery capabilities. Data stored in the ZL Technologies Unified Archive is retained and disposed of in accordance with NARA records retention schedule.

ZL stores data in an encrypted form in Windows based Unified Archiving servers. Metadata and search indices are input to the SQL DBMS and discrete messages stored as individual files in the file system. Once the retention period has expired UA purges the message from the archives. The purge consists of deletion of metadata and search indices from the DBMS and files from the file system. The file deletion includes a series of 7 overwrites of the deleted file to prevent file physical reconstruction from commonly available file restoration utilities.

Users are responsible for completing records management on any non-email records that reside on NARAnet prior to their departure from NARA. In rare situations, such as the departure of a senior management official or a litigation matter, all of the end-user's data may be copied and retained to ensure compliance with applicable laws and regulations.

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.

The system will use an appliance from SecureAuth to provide for SAML single sign-on capability from within NARAnet. SecureAuth will also provide a new method of enforcing two-factor authentication when trying to access the system remotely.

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

As stated above, the system will use SecureAuth to provide a new method of enforcing two-factor authentication when trying to access the system remotely. A one-time PIN number will be sent to a registered email or phone (voice message or SMS message). Contact data is stored from within NARA's eDirectory and the user provides this data on a voluntary basis. If the user chooses not to provide personal contact data, the default mechanism for distributing their PIN is leaving a voice message on their work phone.

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

Yes, to a large degree NARAnet meets NARA's IT security requirements as well as those requirements set down by federal law and policy. NARAnet is the GSS that provides many of the security controls for the systems that reside on it. As such, NARAnet is itself responsible for handling and meeting many of the NARA IT security requirements for those systems. NARA's IT security requirements are based on Federal law, policy, and procedures.

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, a risk assessment has been performed. The NARANET GSS comprises many components. The risk assessment for the NARANET GSS is continually reviewed and updated as significant changes occur to this GSS. A POA&M has been established for NARANET, which is also continuously reviewed and updated to reflect planned actions to mitigate identified risks.

There are concerns about data loss prevention and the potential of leaking sensitive information as the system cannot provide a technical means to prevent end-users from saving data to their own (non-Government Furnished Equipment) devices. Part of this can be mitigated with policy, but without a technical means of enforcing policy, users will still be able to save information to their devices. The NARA project team is continuing to analyze this risk and perform research to identify viable third party products that may be able to integrate with the system to provide some coverage.

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

NARA conducts vulnerability scans on all network devices on a monthly basis according to a predefined schedule. A quarterly report of open vulnerabilities is compiled and analyzed. In addition, a subset of NIST 800-53 controls are tested for NARA systems on an annual basis.

NARANet traffic is monitored by an Intrusion Detection Service provided by their Trusted Internet Connection provider and the Department of Homeland Security's EINSTEIN program. Components of NARANET also feed log files into a Security Information Management (SIM) system.

Various components of the GSS have centrally-managed, and monitored anti-virus software and host-based intrusion detection software in place.

NARANet also uses McAfee Policy Auditor to monitor compliance with the CIS and USGBC benchmarks.

Google Apps for Government is operating under an Authorization to Operate (ATO) issued by NARA on June 24, 2014 and is subject to continuous security assessment and authorization.

Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems, and outside knowledge of vulnerabilities.

At many points across the Google global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as unexpected activity in former employees' accounts or attempted access of customer data.

Google Security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and web bulletin board systems. Automated network analysis helps determine when an unknown threat may exist and escalates to Google Security staff, and network analysis is supplemented by automated analysis of system logs.

The system is monitored by Google 7 x 24 and those procedures are documented in the Google SSP. The Google solution contains intrinsic mechanisms for providing data protection, data segmentation, and data access control.

Continuous Monitoring: Google conducts automated scans of systems for vulnerabilities in accordance with the Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE), and

National Vulnerability Database (NVD) standards and other organizations such as the United States Computer Emergency Readiness Team (US-CERT). Continuous monitoring is a key capability for rapid incident identification, notification, logging, tracking, and remediation. ATOs and periodic scheduled reviews ensure that Google systems mitigate vulnerabilities per NARA requirements and within specified timeframes. Scan results will be managed and mitigated in Plans of Action and Milestones (POA&Ms) and submitted together with the quarterly POA&M submission and per US-CERT Federal Incident Reporting Guidelines.

The security controls described in the SSP were assessed by an independent third-party assessor. As part of its continuous monitoring process, Google reviews and tests its security controls periodically to determine whether controls operate effectively to prevent the unauthorized disclosure of customer data. As part of these controls, Google maintains an entity-wide data breach notification process to identify, isolate, and address potential data breaches. This process is coordinated by Google's incident response capability.

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

Any additional questions regarding the security of the system can be directed to Bernarr Coletta or 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.

Information stored on NARAnet may be covered by any NARA SORN which applies to electronic records.

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

No. There are no planned changes to the system that would require a modification to the SORN at this time.

Conclusions and Analysis

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

None

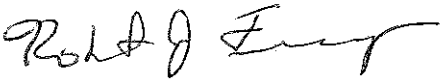
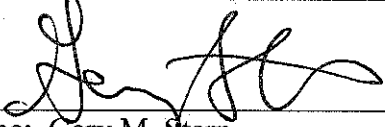
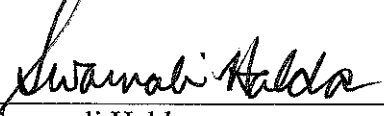
2. If so, what changes were made to the system/application to compensate?

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)	10/8/2014 (Date)
Name: Robert J. Finigan	
Title: NARAnet System Owner	
Contact information: 8601 Adelphi Road Suite 4500 College Park, MD 20740 301-837-3578	
Senior Agency Official for Privacy (or designee)	
 (Signature)	11/7/18 (Date)
Name: Gary M. Stern	
Title: Senior Agency Official for Privacy, General Counsel	
Contact information: 8601 Adelphi Road Suite 3200 College Park, MD 20740 301-837-3026	
Chief Information Officer (or designee)	
 (Signature)	10/15/14 (Date)
Name: Swarnali Halder	
Title: Chief Information Officer	
Contact information: 8601 Adelphi Road Suite 4400 College Park, MD 20740 301-837-1583	