Privacy Impact Assessment (PIA)

Name of Project: Cloud Email

Project's Unique ID: CPIC# 2090P

Legal Authority(ies):	**44 U.S.C. 2104**

Purpose of this System/Application: This system will replace NARA's existing email infrastructure (on-premise Novell Groupwise) with a Cloud-based email solution based on Google Apps for Government. Also integrated into the 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. For the remainder of the document, the "system" shall refer to all of the components listed above.

Section 1: Information to be Collected

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

Employees		The address book or contacts feature will contain employee name, phone number, work address and email address. End users may add additional information to each contact entry. To authenticate into the system, users will provide their user name and password.
External Users		The data elements will vary depending on what users choose to enter. The system will have the users e-mail addresses and can have contact information, if a user adds the information.
Audit trail information (including employee log-in information)		The system will have a log of user log-ins.
Other (describe)		

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)		N/A
Other third party source		The email address and name of an exteral 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.
The email address and user name of individuals is necessary to the system to operate and facilitate delivery of email content. Other user contact information may be needed to populate the Contacts Management features of the systems or in the case of SecureAuth, be used to provide an altemative (voluntary) method for two-factor authentication when accessing the system remotely.

2. Is there another source for the data? Explain how that source is or is not used?
The authoritative source of login data for users is the NARA cDirectory, the email system is synchronized to that source. This data is used for end-user authentication and to facilitate communications by email.

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?
The system will only maintain records related to documents, messages, calendar entries, etc. that the users themselves create and enter.

2. Will the new data be placed in the individual's record?
This data contained within the system will not be automatically tied to an employee's official record.

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?
The system will sync log in information with the NARA edirectory. Employees can update the edirectory if their information changes. The edirectory is updated when employees leave the agency's employment.

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.

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 to email and other applications (calendar, contacts, chat, tasks management)

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.
Directory data, which is synced from NARA's eDirectory, is linked to the user's 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?
Reports can be produced showing when users logged on and off. Only NARA-authorized administrators granted admin rights will have access to this type of data. Administrator actions are also tracked in log files.

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

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

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 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?

Only NARA-authorized system administrators have any access beyond normal user level access.

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

User's will only have access to their own data or data that is specifically shared by another user.

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?

The system will keep a log of all administrator actions on the system. Administrative access is only provided to NARA-authorized invididuals 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?

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.

Yes. The Google directory is sync'd from NARA eDirectory (one way from eDirectory)

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

Yes, NARA's eDirectory is covered under the umbrella NARAnet PIA and SSP documentation.

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.

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?
Individuals can decline to provide personal contact information (a cell phone, home phone, or personal e-mail address) to SecureAuth. If they do not provide this information, they will have more limited options for accessing the system remotely.

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?
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 Govemment is operating under a General Services Administration (GSA) Authorization To Operate (ATO) dated April 12, 2011 and remains in effect through July 22, 2013.

Agency policy and user discretion govem 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.

Data is stored 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.

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 SAME 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 PfN 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.

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?

There are concems 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-Govemment Fumished 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.

Google Apps for Govemment is operating under a General Services Administration (GSA) Authorization To Operate (ATO) dated April 12, 2011, and remains in effect through July 22, 2013.

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

At many points across the Google global network, intemal 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 infrastmcture. 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 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 vulnerabilifies 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.
The point of contact for additional questions regarding security of the system, is 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.
N/A

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?
While the physical data centers of the Cloud vendors are secure and meet security requirements, there are concems about data loss prevention and leaking of sensitive information as the system cannot provide a way to prevent end-users from saving data on to their own devices. While part of these concems will be mitigated with policy, without a technical means of enforcing policy, users will still be able to save information to their devices.

2. If so, what changes were made to the system/application to compensate?
The NARA project team is analyzing this risk and doing research to identify viable third party products

that may be able to integrate with the system to provide some coverage.

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)	2/8/13 (Date)
Name: Aaron Woo	
Title: Project Manager	
Contact information: aaron.woo@nara.gov	
Senior Agency Official for Privacy (or designee)	
(Signature)	2/6/13 (Date)
Name: Gary M. Stern	
Title: General Counsel	
Contact information: garym.stem@nara.gov	
Chief Information Officer (or designee)	
(Signature)	2/7/13 (Date)
Name: Michael Wash	
Title: Executive of Information Services/CIO	
Contact information: michael.wash@nara.gov	