



# **Infrastructure**

## **Privacy Impact Assessment**

**Version 1.4**

**February, 2013**

**Table of contents**

<b>Description</b>	<b>Page</b>
<b>1 System Name/Title .....</b>	<b>1</b>
<b>A. Contact Information .....</b>	<b>1</b>
<b>B. System Application /General Information.....</b>	<b>1</b>
<b>C. Data in the System.....</b>	<b>2</b>
<b>D. Attributes of the Data .....</b>	<b>5</b>
<b>E. Maintenance and Administrative Controls .....</b>	<b>7</b>
<b>F. Access to Data .....</b>	<b>8</b>

## **INFRA Privacy Impact Assessment (PIA)**

### **1 System Name/Title**

Infrastructure (INFRA) is an information system in the Department of the Interior (DOI)/U.S. Geological Survey (USGS).

#### **A. Contact Information**

**Name:** David J. Newman  
**Title:** Privacy Officer  
**Organization:** USGS/AEI/EI/OIIM  
**Address:** 12201 Sunrise Valley Drive, Mail Stop: 807  
**City:** Reston **State:** VA **Zip code:** 20192  
**Phone Number:** (703) 648-7196  
**Email Address:** [djnewman@usgs.gov](mailto:djnewman@usgs.gov)

#### **B. System Application /General Information**

##### **(1) Does this system contain any information on individuals?**

One of the core components of INFRA (Lotus Notes) is the Name and Address Book (NAB). However, no personal information is included within the NAB. The NAB only provides work related information on individuals who have a Lotus Notes account. This information is inclusive of email address, work address, mobile phone if applicable, name and division. As a service provided by Lotus Notes, individuals are able to send and receive information utilizing the INFRA system that may include personal information. System users are aware that information held in the system could be subject to monitoring or collection. INFRA also provides Quicker, SharePoint, and Sametime services both of which may also include personal information. Information within Federal systems is considered to belong to the organization and regardless of the nature is subject to court rulings requiring collection in litigation and FOIA inquiries.

##### **a. Is this information identifiable to the individual?**

Yes, however, the information maintained about employees is business related information and not PII. There is a potential that employees may transmit types of personally identifying information through the system. Employees are trained annually on FISSA+ and have been notified of the USGS policy on transmitting PII and Sensitive data through Lotus Notes.

##### **b. Is this information about individual members of the public?**

No, only employee business information is maintained.

**c. Is the information about employees?**

Yes. Although no personal information is included within the Lotus Notes NAB, there are a variety of Electronic Files processed over the INFRA system that may contain one or more personal data items, such as personal name, personal identifier, or some other category of personal information, about USGS employees which are accessible only by authorized DOI and USGS officials. Examples of the files potentially transmitted over the network are:

- (1) Employee Health Record
- (2) Employee Safety Record
- (3) Employee Training Record
- (4) Employee Worker Compensation Notice
- (5) Letter of Employee Medical Restriction
- (6) Letter of Employee Termination
- (7) Lotus Notes Employee Address and Contact Records
- (8) Office Continuity of Operations Plan (COOP)
- (9) Office Occupant Emergency Plan (OEP)
- (10) Office Information Technology Contingency Plan
- (11) Record of Employee Disciplinary Action
- (12) Emergency Response Plan

**(2) What is the purpose of the system/application?**

INFRA provides encrypted email and instant messaging services for the USGS and its employees. INFRA also provides collaborative tools to facilitate information sharing. The Lotus Enterprise (Domino) is the core component of INFRA and is used as the email and messaging platform for USGS. The application provides messaging and collaborative applications through an integrated platform for secure online interactions between users.

**(3) What legal authority authorizes the purchase or development of this system/application?**

5 U.S.C. 301, 3101, 5105-5115, 5501-5516, 5701-5709; 31 U.S.C. 66a, 240-243; 40 U.S.C. 483(b); 43 U.S.C. 1467; 44 U.S.C. 3101; Executive Order 11807.

**C. Data in the System****(1) What categories of individuals are covered in the system?**

INFRA is utilized by employees of USGS. For the purposes of this assessment, an employee is considered to be either government (e.g. students, interns, volunteers, and emeritus), or contractor personnel working for the USGS. There is a separate domain that is available for non-USGS employees, such as research associates from universities, that is used for communication of USGS information. The separate domain does not provide access to the USGS or DOI

address books. USGS employees using this system use it for email, internal messaging, and conferencing capabilities.

**(2) What are the sources of the information in the system?**

**a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?**

Information of a privacy nature is assumed to be obtained from the user or sources which have user supplied information such as personnel records. Emails can be received from various sources sent to users of the system. Likewise information shared over Quicker, SharePoint, or Sametime can be received from various sources with access to INFRA. These sources can contain one or more data items about USGS employees to include all or some of the following information, some of which is personal, depending on the specific electronic file being accessed: (name, social security number or employee identification number, home address, home phone number, date of birth, award category and recommendation, disciplinary action, and medical condition. This information is accessible only by DOI, USGS officials or contractors employed by the USGS. When you encrypt an email message, the Lotus Notes client scrambles the information so that only specified recipients can read the message. Only the body of a message is encrypted, not the header information. Encrypting a mail message will not delay the routing time for a message but it will increase the time required to send and open a message. SameTime uses SSL to encrypt the connection for Instant Messaging and File Transfers.

**b. What Federal agencies are providing data for use in the system? DOI/USGS**

**c. What Tribal, State and local agencies are providing data for use in the system? None**

**d. From what other third party sources will data be collected? None**

**e. What information will be collected from the employee and the public?**

Information collected is from employee or official DOI/USGS sources only. Electronic files that are sent through email or shared via Quicker, SharePoint, and Sametime may contain one or more of the personal data items shown below:

- (1) Employee Health Record. Employee Name, Social Security Number, Home address; Home phone number.
- (2) Employee Safety Record. Employee Name, Social Security Number, Home address; Home phone number.
- (3) Employee Training Record. Employee Name and Social Security Number.
- (4) Employee Worker Compensation Notice. Employee Name and Social Security Number.
- (5) Letter of Employee Medical Restriction. Employee Name, Social Security Number, Home address; Home phone number.
- (6) Letter of Employee Termination. Employee Name and Social Security Number.

- (7) Lotus Notes Employee Address and Contact Records. Employee Name, Home Address, and Home Phone Number.
- (8) Office Continuity of Operations Plan (COOP) Emergency Employee Phone Contact Tree. Employee Name, Home Address, and Home Phone Number.
- (9) Office Directory. Employee Name, Title, Office Number, Office location, Home Address, and Home Phone Number.
- (10) Office Occupant Emergency Plan (OEP) Emergency Employee Phone Contact Tree. Emergency Employee Phone Contact Tree. Employee Name, Home Address, and Home Phone Number.
- (11) Office Information Technology Contingency Plan. Emergency Employee Phone Contact Tree. Employee Name, Home Address, and Home Phone Number.
- (12) Record of Employee Disciplinary Action. Employee Name and Social Security Number.
- (13) Emergency Response Plan. Employee Name, Home Address, and Home Phone Number.

### **(3) Accuracy, Timeliness, and Reliability**

#### **a. How will data collected from sources other than DOI records be verified for accuracy?**

PII data is not collected by Lotus Notes, SharePoint, or Video Communications Initiative (VCI). Lotus is a tool to potentially transmit PII and not a system that creates or the official system that stores the PII that can be retrieved by a unique identifier. Verification of the accuracy of information that is passed through email or stored in a repository within the system boundary is not conducted. It is incumbent on the individual using the system to verify data for accuracy.

#### **b. How will data be checked for completeness?**

Information that is user generated within email or stored in Quicker/SharePoint is not checked for completeness and it is the responsibility of the individual to ensure completeness. There is no validation for completeness of email or files that transverse or are stored by the system. Audit trails are enabled for all databases associated with the system providing logging of the time, action, and ID that made modifications or deletions. The systems have file integrity monitors such as tripwire implemented at the Operating System level to ensure system integrity.

#### **c. Is the data current?**

Verification of the currency of information passed through email or via Quicker, SharePoint, and Sametime is not formally enforced. Some of the information may be reviewed for currency if that review is part of a larger process that uses INFRA (i.e. The COO is stored on Quicker and is reviewed periodically). The NAB is periodically updated but does not contain privacy data specifically. DOI provides updates and modifications as required and the NAB is maintained weekly based on agent scans to ensure employee listings are current.

#### **d. Are the data elements described in detail and documented? If yes, what is the name of the document?**

Yes, all data elements are described in detail in the Procedures and Guidelines database. Information collected is from employee or official DOI/USGS sources only. Electronic files that are sent through email may contain one or more of the personal data items shown below:

- (1) Employee Health Record. Employee Name, Social Security Number, Home address; Home phone number.
- (2) Employee Safety Record. Employee Name, Social Security Number, Home address; Home phone number.
- (3) Employee Training Record. Employee Name and Social Security Number.
- (4) Employee Worker Compensation Notice. Employee Name and Social Security Number.
- (5) Letter of Employee Medical Restriction. Employee Name, Social Security Number, Home address; Home phone number.
- (6) Letter of Employee Termination. Employee Name and Social Security Number.
- (7) Lotus Notes Employee Address and Contact Records. Employee Name, Home Address, and Home Phone Number.
- (8) Office Continuity of Operations Plan (COOP) Emergency Employee Phone Contact Tree. Employee Name, Home Address, and Home Phone Number.
- (9) Office Directory. Employee Name, Title, Office Number, Office location, Home Address, and Home Phone Number.
- (10) Office Occupant Emergency Plan (OEP) Emergency Employee Phone Contact Tree. Emergency Employee Phone Contact Tree. Employee Name, Home Address, and Home Phone Number.
- (11) Office Information Technology Contingency Plan. Emergency Employee Phone Contact Tree. Employee Name, Home Address, and Home Phone Number.
- (12) Record of Employee Disciplinary Action. Employee Name and Social Security Number.
- (13) Emergency Response Plan. Employee Name, Home Address, and Home Phone Number.

## **D. Attributes of the Data**

**(1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Yes, though these are supervisory or organizational electronic files generally.

**(2) 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 new privacy data is derived or created. All information in the NAB that is provided is standard data that is collected at the initial account setup. No analysis is performed on other information passed through email. Supervisory or organizational electronic files may be also be

stored, transmitted, or processed, but with no automated interfaces and no capability to create new data.

**(3) Will the new data be placed in the individual's record?**

Not applicable because no new privacy data is created.

**(4) Can the system make determinations about employees/public that would not be possible without the new data?**

No.

**(5) How will the new data be verified for relevance and accuracy?**

Not applicable because no new privacy data is created.

**(6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

INFRA uses encrypted access through the use of the Lotus client, encrypted POP, VPN access, or web access using SSL. Additionally, Quicker, SharePoint, and Sametime have restricted access based on discretionary access controls. All access is restricted to USGS employees or authorized contractors.

**(7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?**

No processes are being consolidated; however, access to the system requires identification through the use of user ID and password for web authentication, POP, and VPN, or a valid certificate for use of the Lotus client. Automated agents are restricted and will only perform information retrieval, all modifications to information is implemented by personnel. Audit logs will record the actions and the logs themselves are limited in who has access to them.

**(8) How will the data be retrieved?**

Lotus stores a copy of the email and the user can obtain copies of emails sent by using their employee business account ID.

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

There are no defined reports. There are no predefined uses for information printed. Users can print email, SharePoint, and Quicker files for which they have access and are responsible for their proper safeguarding.

**(10) 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 individuals can grant consent?**

None for the NAB, which doesn't contain privacy information. Individuals must provide information that is stored in the NAB to obtain an account. Privacy information contained in

Quickplace or Sametime is controlled by the individual user and does not have 'Official' use controls applied. It is the responsibility of the user to control this information.

## **E. Maintenance and Administrative Controls**

### **(1) 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 GS Lotus Admin team centrally manages INFRA. Local site administrators are restricted in capabilities on the systems. Auditing is enabled throughout the enterprise and logs any modifications implemented. System integrity software such as Tripwire is implemented to provide logging of modification made at the OS level. The GS Lotus Admin team maintains a Change Management database and a Server Management database to provide baseline records of the current approved system design. Information is synchronized across individual INFRA servers on a regular basis assuring any privacy data is consistent across the system. The process used is commonly referred to as replication.

### **(2) What are the retention periods of data in this system?**

Data maintained in various Quickr or SharePoint files is retained for an undefined period of time. Data maintained in email form is maintained indefinitely.

### **(3) What are the procedures for disposition of the data at the end of the retention period?**

Tapes are overwritten and reused. If tape does not function the Backup Administrator is notified and the tape is sent to the degaussing unit who destroys the tape. Disposition procedures for this data will be in accordance with USGS, GRDS 432-1-S1, Chapter 400, Item # 418-01b.

### **(4) Is the system using technologies in ways that the DOI has not previously employed (e.g., Monitoring software, SmartCards, Caller-ID)?**

No, only current or previously employed technologies are used.

### **(5) How does the use of this technology affect public/employee privacy?**

Not applicable because technology is not being used in new ways.

### **(6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

No. The system does not provide the capability to identify, locate or monitor individuals. The only location information provided is the individual's work location and phone number located in the NAB and is considered public information.

### **(7) What kinds of information is collected as a function of the monitoring of individuals?**

Information is not collected, as a function, to allow monitoring of individuals. Email tracking is enabled to provide for verification if required for the routing within INFRA. This can provide proof of sending but will not retain email contents; this logging consists of recording who email was sent from, to, and the subject, no message content is recorded. In the case of providing

access to a user's mail file, a written request is presented from the user's supervisor with documentation that they have followed the proper procedures through personnel for this access and the access granted will be logged with the appropriate documentation.

**(8) What controls will be used to prevent unauthorized monitoring?**

Only administrators have access to system logs through ACLs with access being restricted within the administrator group. The access to the logs is monitored and logged.

**(9) Under which Privacy Act Systems of Record notice (SOR) does the system operate?**

Not applicable no records can be retrieved using a unique identifier.

**(10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision?**

Modification will not have an effect on the privacy information as the system was not established as a privacy system. Modifications are related to data transmitted or stored by a specific user or user's and needs to be addressed by the systems providing the information. INFRA acts as a conduit or as disk storage for some information and the system does not interact with or modify the data.

## **F. Access to Data**

**(1) Who will have access to the data in the system?**

Only authorized personnel have access to the system that is restricted through the use of Access Control Levels (ACLs). Authorized users include government workers and contractors that have been identified as employees of USGS. Authorization occurs when a user account is established. Users are only able by default to view their email directory, they are able to allocate permissions to other users to access their director at their discretion.

**(2) How is access to the data by a user determined?**

Access to the system is granted only to personnel of USGS who have an active user ID. Access to databases must be added by the owner of the database, and is limited through the use of discretionary ACLs. USGS personnel have the ability to give other personnel access to their mailbox.

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

Access is restricted by user ID. By default the general access is None.

**(4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?**

All users are given annual security training. The training includes mis-use, access, and disposition of data. Users are able to assign access permissions to other system users at their own risk through the use of delegation. Collected data is protected by a combination of user id

and user password. Files in transit are encrypted if emailed between supervisors. These files are encrypted via Lotus Notes email.

**(5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system?**

Yes, contractors were involved with the design, development and maintenance. Security clauses and non-disclosure agreements are included in the contract and pre-employment clearance is required. All design, development, or modifications by a contractor is further reviewed by at least one federal employee. Any major change in the system requires approval from a federal employee. These policies and procedures are documented in the procedures and guidelines.

**(6) Do other systems share data or have access to the data in the system?**

INFRA exchanges address books with DOI agencies. The information in the NAB is read-only, and allows for modification of contents only by the owner. Users are not able to input modifications to the NAB. No other formal system data sharing occurs.

**(7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The GS Lotus Admin team is responsible for protecting the privacy rights of the employees.

**(8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

No. Only NAB directory information is formally shared with other agencies. Sharing of email data is the responsibility of the user.

**(9) How will the data be used by the other agency?**

The user's cooperative agreement controls this access if the cooperator is going to be part of the USGS NAB. If the agency is not directly in the NAB then their access is only through the copy of the NAB that is replicated to their DOI servers. The information contained within the NAB is limited to providing work related contact information that would be used to contact the individuals.

**(10) Who is responsible for assuring proper use of the data?**

All data managers that have provided the data as well as provided access to the data according to DOI policy. Individual users of email, Quicker, SharePoint, and Sametime share the burden of responsibility for proper use of the data.