Privacy Impact Assessment for the

Directory Services and Email System (DSES)

Contact Point
James Kief
Functional Area Manager
Department of Homeland Security/US Coast Guard
(304) 264-2573

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The U.S Coast Guard manages and operates the Directory Services Electronic Mail System (DSES) used by all DHS e-mail users. DSES handles e-mail traffic in, out, and between DHS, its Components, and the Internet, and provides a directory of users' official contact information. This PIA is being conducted to assess the risk associated with the personally identifiable information that is processed, stored, and transmitted within the DSES system, which is currently operational.

Overview

DSES is owned by the Department of Homeland Security and operated by the U.S. Coast Guard. The system is made up of two portions: Directory Services and the E-mail System. DSES provides a single search point for DHS employees to locate other DHS employees' contact information electronically, accessible by a web-based directory on the DHS intranet, or with e-mail client software. DSES unifies DHS e-mail addresses from all DHS Components into a single directory and provides a single route for incoming and outgoing e-mail. Each DHS Component maintains control of its internal e-mail system and updates between their mail system directory and the DSES DHS-wide directory.

Directory Services, the GAL

The Directory Services portion of DSES provides an enterprise-wide Global Address List (GAL). The GAL is an electronic directory of the official contact information for DHS employees and contractors with active DHS e-mail accounts. Each DHS Component provides a listing of their users who should be assigned a DHS e-mail account via a directory synchronization process. The DSES system then assigns the user an email address from the information provided by the Component and includes the user in the Departmental GAL. This GAL directory is available to other DHS employees and contractors with active DHS e-mail accounts. The GAL is a centralized searchable directory of all DHS employees and contractors with active e-mail accounts issued by DHS. GAL information can also be retrieved by viewing the DHS White Pages on the DHS intranet. The information available in both searches include any contact information provided by the Component, which at a minimum includes the Component for which the person works, the person's name and email address. Additional optional data includes office location (such as room or floor number), desk, mobile and pager telephone number, fax number and physical mailing address. These directory searches are typically used by DHS employees and contractors to look up contact information for their colleagues at DHS.

The directory synchronization process captures log information on when a user is added to the system, when changes are made to the user object, and when the object is removed from the central directory. Logs are also maintained of the GAL objects which are exported to the DHS Component Active Directory systems so that users can locally access the GAL in their email clients.

The DHS GAL is shared with internal DHS Components as requested and approved by the DHS Program Manager. Each Component is updated with changes to the GAL nightly. A limited portion of the DHS GAL is exported to the US Department of Justice (DOJ). This export is limited to DHS Headquarters staff user information contained in the DHS GAL and is provided to DOJ for correspondence purposes as part of the agencies' collaborative working relationship. Similarly, DHS has some contact information on DOJ colleagues in the DHS GAL, supplied by the DOJ.

E-mail System

The E-mail System portion of DSES serves as a mail relay or routing facility and is not a mail repository. An e-mail message sent from any DHS-issued e-mail account is sent from the user's e-mail client software (such as Microsoft Outlook), to the DHS Component e-mail server. The DHS e-mail server relays the message to the DSES gateway, where it is scanned for viruses. If no viruses are found, the message is passed to servers that match the message with the user's assigned "@dhs.gov" address, and then forward it to its intended destination, either within DHS or to the Internet. The personally identifiable information collected by the E-mail System portion of DSES is the e-mail sender or recipient's e-mail address, which usually includes that person's first name, last name, and middle initial. Because e-mails that contain viruses or spam are quarantined and stored by DSES, any personally identifiable information contained within those messages will also be stored by DSES, although it will not be used for any other purpose.

An e-mail message sent to a DHS e-mail address from the Internet enters the DSES E-mail System, where it is first scanned for viruses. If no viruses are found, it is scanned for spam content. If spam content exists, the e-mail message is not delivered to the user and the e-mail is stored in a protected quarantine database. If no spam content exists, the e-mail is matched by DSES to the user's internal Component e-mail address, and then forwarded to the DHS Component where the user's mailbox resides.

In both e-mail scenarios, logs of the messages processed are retained on the servers that handle the email message. This log contains the Internet Protocol (IP) addresses and Domain Name (if available) of the e-mail sender's and recipient's servers. Included in this information are the e-mail addresses of the sender and all recipients, and the subject line of the message. Additionally, any information relating to virus content and spam scoring is retained in the logs as well.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

- *Information in the GAL:*

  The information available within DSES includes any contact information provided by the Component which can include the Component in which the person works, the person's name, display name, title, both their DHS and internal e-mail addresses, office location, telephone numbers, and physical mailing address.

- *Information in the E-mail System*

  The information used to record received and processed e-mails are the sender's e-mail address, IP address and server name and the recipient's e-mail address and e-mail domain server name. E-mails are not retained unless they are identified as SPAM, then the entire message is quarantined for 14 days and then is expunged from our system.

1.2 What are the sources of the information in the system?

- *Information in the GAL:*

  Each DHS Component provides a listing of their users who should be assigned a DHS e-mail account via a directory synchronization process. The DSES system then assigns the user an e-mail address from the information provided by the Component and includes the user in the Departmental GAL.

- *Information in the E-mail System*

  Header information is collected from each e-mail that is send to any DHS e-mail address.

1.3 Why is the information being collected, used, disseminated, or maintained?

- *Information in the GAL:*

  The Directory Services portion of DSES provides an enterprise-wide Global Address List (GAL). The GAL is an electronic directory of the official contact information for DHS employees and contractors with active e-mail accounts issued by DHS. This information will be represented to the end-user as contacts within the GAL, which can be accessed using Microsoft Outlook (Exchange 2003 or 5.5) or Lotus Notes.

- *Information in the E-mail System*

  DSES unifies DHS e-mail addresses from all DHS Components into a single directory and provides a single route for incoming and outgoing e-mail.

1.4 How is the information collected?

- *Information in the GAL:*

  Each DHS Component provides a listing of their users via a directory synchronization process to DSES. The individual fills in the contact information.

- *Information in the E-mail System*

  Header information for all emails, and the content of emails that contain viruses or spam content are automatically collected in electronic format by the DSES server.

1.5 How will the information be checked for accuracy?

- *Information in the GAL:*

  Information that DSES receives from each Component is presumed to be accurate; however, when a user is assigned a DHS e-mail address, an e-mail notification is sent to the user's new DHS e-mail address. The user may then review their information at http://directory.dhs.gov or via the GAL and submit any necessary change requests to their own helpdesk.

- *Information in the E-mail System:*

  Information collected in the email system is done automatically with no additional check for accuracy.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

DHS has collects the information in DSES according to *Departmental Regulations* (5 U.S.C. 301) and *Records management by agency heads; general duties* (44 U.S.C. 3101).

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Risk: GAL content release to unauthorized users.

Mitigation: The DHS whitepages and GAL are on the DHS Core Network and only DHS personnel have access to this network. Select portions of the DHS GAL are shared with the DOJ, which keeps it on the DOJ network and similarly restricts access.

Risk: GAL content may be modified by unauthorized personnel.

Mitigation: The GAL information is collected from each of the Components. Only local administrators can modify this information. Also, GAL information published to a Component is refreshed nightly from the master export, therefore; any changes not initiated by the Component will be overwritten.

Risk: E-mail transaction logs may be viewable and modifiable by unauthorized personnel.

Mitigation: The logs are stored on a secure server with limited validated access for system administrators.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

- *Information in the GAL:*

  DSES provides a single search point for DHS employees to locate other DHS employee's contact information electronically, accessible by a web-based directory on the DHS intranet (http://directory.dhs.gov), or with e-mail client software.

- *Information in the E-mail System:*

  The E-mail System portion of DSES serves as a mail relay or routing facility and is not a mail repository.

2.2 What types of tools are used to analyze data and what type of data may be produced?

- *Information in the GAL:*

  Each Component is responsible for analyzing their data for accuracy prior to providing it to DSES for Global Address List (GAL) population. The GAL is an electronic directory of the official contact information for DHS employees and contractors with active e-mail accounts issued by DHS through each Component.

- *Information in the E-mail System:*

  DHS uses tools to identify and quarantine potentially harmful email messages, which results in quarantining some messages and may produce data that helps DHS recognize future harmful messages.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

DSES does not use commercial or publicly available data in the GAL or in the E-mail System.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

If data in the GAL is out of date or incorrect, the onus is on each user to submit a ticket to their HelpDesk to have the information corrected. The negative impact of inaccurate data is minimal because the information is only used as an internal contact directory. Information in the E-mail system is primarily a historical transactional log and has minimal controls commensurate with its minimal use.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

- *Information in the GAL:*

  Each DHS Component manages their list of contacts. User information is kept in the database for as long as his or her account is active and valid. Once a user is no longer employed, their information is expunged from the GAL.

- *Information in the E-mail System*

  DSES currently has 4 years of email transaction log files and will keep this information for 7 years.

3.2 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

- *Information in the GAL:*

  Information in the GAL is not subject to a NARA General Records Schedule because it is used for reference and is updated as needed.

- *Information in the E-mail System:*

  Information in the E-mail system is subject to the NARA General Records Schedule 20, item 4, *Data Files Consisting of Summarized Information*, which only requires that the records be deleted when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes. DHS has determined that the records are needed for 7 years for audit purposes. E-mails that are quarantined (malicious and junk emails) are not subject to a NARA General Records schedule because they are not considered federal records.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Risk: Retaining period longer than necessary

Mitigation: Information is needed to perform audits on the e-mail traffic.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

The GAL is a centralized searchable directory of all DHS employees and contractors with active email accounts issued by DHS. The information available includes any contact information provided by the Component which at a minimum includes the Component in which the person works, the person's name and email address and can include office location, telephone numbers, and physical mailing address

- *Information in the GAL:*

  The DHS GAL and whitepages are shared with all DHS Components.

- *Information in the E-mail System:*

  The header information is shared with DHS Components that perform auditing functions.

4.2 How is the information transmitted or disclosed?

DSES exports user information via a secure network transfer to each Component's Directory Server.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Risk: Information may be accessible outside of user community.

Mitigation: The DHS GAL is located on the DHS LAN is only accessible by DHS employees and contractors with security clearances.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

- *Information in the GAL:*

  A limited portion of the DHS GAL is exported to the US Department of Justice. This export is limited to DHS Headquarters staff and includes all available user information contained in the DHS GAL to enable DOJ to contact DHS colleagues. Additionally, individual employees may provide information out of the GAL to those outside DHS to conduct official business.

- *Information in the E-mail System:*

  The e-mail information is not shared externally.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

A limited portion of the DHS GAL is exported to the US Department of Justice. This export is limited to DHS Headquarters staff and includes all available user information contained in the DHS GAL to enable DOJ to contact DHS colleagues.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

DSES maintains a server that allows DOJ direct, read-only access in order for them to retrieve their daily GAL sync.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Risk: Non-authorized personnel obtaining access to the information.

Mitigation: The DSES server is Internet Protocol and account restricted for limited DOJ admin users.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

- *Information in the GAL:*

  DHS gives notice of user information for DHS employees and contractors prior to its collection in DSES in the form of Privacy Act Statements on the forms individuals fill during the on boarding process (OF-306, *Declaration for Federal Employment*, or 3130, *DHS Non-Staff Assignment Form*, as applicable.) Notification is also given in the DHS General Information Technology Access Account Records System (GITAARS) system of records notice (DHS/ALL-004) 73 FR 28139, and the Office of Personnel Management General Personnel Records SORN (OPM/GOVT-1), 71 FR 35342-01. Additionally, DSES notifies each user via e-mail after their e-mail account is established.

- *Information in the E-mail System:*

  The user is notified by the standard DHS notice when accessing the DHS LAN that information will be collected. It is standard for e-mail servers to log header information. Therefore the external sender should reasonably expect this information to be collected by DSES.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

- *Information in the GAL:*

  No, each Component controls their user's information that is required in order to participate as a DHS employee.

- *Information in the E-mail System:*

  Users may decline to provide information by not e-mailing to a DHS e-mail address.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

- *Information in the GAL:*

  No, but use of the information in the GAL and whitepages is limited to DHS employees for contact information.

- *Information in the E-mail System*

  User's may decline to provide information by not e-mailing to a DHS e-mail address.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Risk: Individuals are not aware information is being collected about them.

Mitigation: The user is notified by the standard DHS notice when accessing the DHS LAN that information will be collected. It is standard for e-mail servers to log header information. Therefore the external sender should reasonably expect this information to be collected by DSES.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

- *Information in the GAL:*

  Information will be represented to the end-user as Contacts within the GAL, which can be accessed using and e-mail client. Information is also accessible by a web-based whitepages directory on the DHS intranet (http://directory.dhs.gov).

- *Information in the E-mail System:*

  Individuals can request access to any DSES information by submitting a request to the DHS Freedom of Information Act (FOIA) Office at:

  Director of Departmental Disclosure
  U.S. Department of Homeland Security
  Washington DC 20528

7.2 What are the procedures for correcting inaccurate or erroneous information?

Users may correct inaccurate or erroneous information by contacting their component IT Help Desk.

7.3 How are individuals notified of the procedures for correcting their information?

Each user is sent an e-mail notification when their DHS email address is created and their information is added to the GAL. The email informs them that their information is available and to contact their Help Desk for any discrepancies.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is provided to users. Users may correct inaccurate or erroneous information contacting their Help Desk.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Risk: Inaccurate or erroneous information

Mitigation: Inaccurate or erroneous information can be corrected by contacting the Component Help Desk.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

This directory is only available to other DHS and DOJ employees and contractors with active e-mail accounts issued by DHS.

The firewall software is configured to allow only limited access to authorized IP addresses. These settings are not documented due to security risks.

8.2 Will Department contractors have access to the system?

- *Information in the GAL:*

  Yes, the GAL and whitepages are available to all employees and contractors with active DHS e-mail accounts for read-only access.

- *Information in the E-mail System:*

  System administrator and managers have role-based access accounts for header information.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

DHS mandates Annual Computer Security Awareness Training.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The office of the Chief Information's Officer at DHS granted DSES the Authority to Operate on July 31, 2008. This ATO will be valid for a period of three years.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

DSES has deployed auditing software and the logs are used to track unauthorized access attempts on the system.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Risk: Non-authorized personnel obtaining access to the information.

Mitigation: The DSES server is Internet Protocol and account restricted for limited DOJ admin users.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

The Directory Services portion of DSES provides an enterprise-wide Global Address List (GAL). The E-mail System portion of DSES serves as a mail relay or routing facility and is not a mail repository.

9.2 What stage of development is the system in and what project development lifecycle was used?

DSES is currently in the operations and maintenance phase of the system development life cycle (SDLC).

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No.

Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security