



Privacy Impact Assessment  
for the  
E-Mail Secure Gateway  
(EMSG)

**DHS/MGMT/PIA-006**

**March 22, 2012**

**Contact Point**

**David Jones  
MGMT/OCIO/ITSO/ESDO  
DHS HQ  
(202) 447-0167**

**Reviewing Official**

**Mary Ellen Callahan  
Chief Privacy Officer  
Department of Homeland Security  
(703) 235-0780**



## Abstract

The Department of Homeland Security (DHS) manages and operates the E-Mail Secure Gateway (EMSG) used by all DHS e-mail users. This service was previously managed under the Department of Homeland Security Directory Services Electronic Mail System (DSES). EMSG 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 (PII) that is received and processed within the EMSG system. This PIA does not cover the PII that may be contained within the body of an email or attachment.

## Overview

E-Mail Secure Gateway (EMSG) is owned by the Department of Homeland Security and operated by DHS Headquarters (HQ). This service was previously managed under the Department of Homeland Security Directory Services Electronic Mail System (DSES). EMSG 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. EMSG 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 EMSG DHS-wide directory. The system is made up of two portions: Directory Services and the E-mail System.

### *Directory Services and the Global Address List (GAL)*

The Directory Services portion of EMSG 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 EMSG 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 includes 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 may include:

- 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, such as 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 Delivery System*

The E-mail System portion of EMSG serves as a mail relay or routing facility, and is not a packages 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 EMSG 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 email address, and then forward it to its intended destination, either within DHS or to the Internet. The PII collected by the E-mail System portion of EMSG is the e-mail sender or recipient's e-mail address, which usually includes that person's first name, last name, and middle initial. E-mails that contain viruses or spam are quarantined for 15 days and then expunged from the EMSG system, and any personally identifiable information contained within those messages will also be quarantined and expunged by EMSG. If no spam content exists, the e-mail is matched by EMSG 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.

This PIA does not cover the PII that may be contained within the body of an email or attachment.

## **Section 1.0 Authorities and Other Requirements**

### **1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?**

DHS has legal authority to collect the information in EMSG under *Departmental Regulations* (5 U.S.C. § 301) and *Records management by agency heads; general duties* (44 U.S.C. § 3101).



## **1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?**

The PII contained by the EMSG system is addressed under these existing SORN(s):

- DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS), September 29, 2009, 74 FR 49882

## **1.3 Has a system security plan been completed for the information system(s) supporting the project?**

A System Security Plan (SSP) has been completed and submitted for the EMSG system. An ATO was issued for EMSG on July 30, 2011.

## **1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?**

*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 Created by the E-mail Delivery 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.

## **1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.**

The EMSG system is not covered by the PRA. It does not generate any sort of paperwork or forms.

## **Section 2.0 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.

### **2.1 Identify the information the project collects, uses, disseminates, or maintains.**

*Information in the GAL:*

The information available within EMSG includes any contact information provided by the component, which can include:



- the component in which the person works;
- the person's first, middle and last name;
- the display name;
- title;
- both DHS and internal e-mail addresses;
- office location;
- office telephone numbers; and
- physical office mailing address.

#### *Information Created by the E-mail Delivery System:*

The information used to record received and processed e-mails are:

- the sender's e-mail address;
- IP address;
- server name;
- the recipient's e-mail address; and
- e-mail domain server name.

E-mails are not retained unless they are identified as "spam," in which case the entire message is quarantined for 15 days and then is expunged from the EMSG system.

The EMSG system does not create new information.

The EMSG system does not receive information from another system. In certain instances, EMSG may have filters in place that capture when PII in the body of the email or an attachment is sent unencrypted.

## **2.2 What are the sources of the information and how is the information collected for the project?**

#### *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 EMSG system then assigns the user an e-mail address from the information provided by the component and includes the user in the Departmental GAL.

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

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 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.

#### *Information Created by the E-mail Delivery System*

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



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

### **2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.**

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

### **2.4 Discuss how accuracy of the data is ensured.**

*Information in the GAL:*

Information that EMSG 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 Created by the E-mail Delivery System:*

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

### **2.5 Privacy Impact Analysis: Related to Characterization of the Information**

#### **Privacy Risk:**

Inaccurate, erroneous or out of date information is entered or stored in the GAL.

#### **Mitigation:**

If data in the GAL is out of date or incorrect, each user will 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.

#### **Privacy Risk:**

The possibility of the GAL being populated with more information than is needed, including home phone number.

#### **Mitigation:**

The DHS white pages 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.



## Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

### 3.1 Describe how and why the project uses the information.

*Information in the GAL:*

EMSG 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 Created by the E-mail Delivery System:*

The E-mail System portion of EMSG simply 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 to the DHS component e-mail server. The DHS e-mail server relays the message to the EMSG 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 email address, and then forward it to its intended destination, either within DHS or to the Internet. Only users who have a valid dhs.gov email account will have a match. This PIA does not cover the contents or attachments associated with the e-mails themselves.

### 3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

The EMSG System does not use technology to conduct electronic searches, queries or analyses in an electronic database to discover or locate predictive pattern or anomaly.

### 3.3 Are there other components with assigned roles and responsibilities within the system?

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 white pages are shared with all DHS components.

*Information Created by the E-mail Delivery System:*

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

### 3.4 **Privacy Impact Analysis: Related to the Uses of Information**

#### **Privacy 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 synchronization, therefore; any changes not initiated by the component will be overwritten.

## **Privacy Risk:**

E-mail transaction logs may be viewable and modifiable by unauthorized personnel. Additionally, there is a risk of the appearance of accessing and monitoring the content of emails.

## **Mitigation:**

The logs are stored on secure servers with limited validated access for system administrators. Only the virus scans, headers, and the transaction logs are retained by the system. The content of the emails are not searched or retained by the EMSG system. Further, this PIA does not cover the PII that may be contained within the body of an email or attachment.

## **Section 4.0 Notice**

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

### **4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.**

*Information in the GAL:*

DHS gives notice of user information for DHS employees and contractors prior to its collection in EMSG, 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, EMSG notifies each user via e-mail after their e-mail account is established.

*Information Created by the E-mail Delivery System:*

The user is notified by the standard DHS notice when accessing the DHS LAN that information will be collected. The standard DHS notice is loaded on each server and workstation and is placed before the user logs into the server or workstation. Its states that the user is on a government system and any information input or gained through is system is governed by the federal government. Additionally, it is standard for e-mail servers to log header information. Therefore, the external sender should reasonably expect this information to be collected by EMSG, the mail delivery system for DHS.

### **4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?**

*Information in the GAL:*



Although, user information is automatically included in the GAL at the time that their account information is populated into their network account, the use of the information in the GAL and white pages is limited to DHS employees for contact information. Users may opt out of providing consent to the use of their information in the GAL. However, that will result in the user not being able to obtain a DHS account.

#### *Information Created by the E-mail Delivery System*

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

### **4.3 Privacy Impact Analysis: Related to Notice**

#### **Privacy 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 EMSG.

## **Section 5.0 Data Retention by the project**

The following questions are intended to outline how long the project retains the information after the initial collection.

### **5.1 Explain how long and for what reason the information is 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. An update is done nightly on the EMSG system. Once a delete occurs on EMSG, the information is completely removed from the system.

#### *Information Created by the E-mail Delivery System:*

EMSG currently has four years of email transaction log files and will keep this information for seven years under its NARA approved retention schedule.

### **5.2 Privacy Impact Analysis: Related to Retention**

#### **Privacy Risk:**

There is a privacy risk related to having a retaining period that is longer than necessary for the information.

#### **Mitigation:**

EMSG retains email information, and user information to synchronize and provision contacts and disabled user accounts back to components and AppAuth, respectively. User information is retained until a given user is deleted from a component, which may be for a longer period than the Privacy Act and the Federal Records Act require. However, the data is retained for no longer than the time needed to remove a user account from the domain.



## Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government and private sector entities.

### **6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.**

*Information in the GAL:*

A limited portion of the DHS GAL is exported to the U.S. Department of Justice (DOJ). 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.

*Information Created by the E-mail Delivery System:*

The e-mail information collected by the delivery system is not shared externally.

### **6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.**

Routine use F permits contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS to access the GAL, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

Routine use H allows access to the GAL by sponsors, employers, contractors, facility operators, grantees, experts, and consultants in connection with establishing an access account for an individual or maintaining appropriate points of contact and when necessary to accomplish a DHS mission function or objective related to this system of records.

Routine use I permits the dissemination of EMSG data to other individuals in the same operational program supported by an information technology system, where appropriate notice to the individual has been made that his or her contact information will be shared with other members of the same operational program in order to facilitate collaboration.

### **6.3 Does the project place limitations on re-dissemination?**

EMSG maintains a server that allows DOJ direct, read-only access in order for them to retrieve their daily GAL sync, allowing for DOJ to pull information to update their GAL for their email exchange.

### **6.4 Describe how the project maintains a record of any disclosures outside of the Department.**

The only data the EMSG System discloses to entities outside DHS is GAL information to the



DOJ. Records of this disclosure are provided via synchronization logs.<sup>1</sup>

## **6.5 Privacy Impact Analysis: Related to Information Sharing**

### **Privacy Risk:**

There is a possibility of unauthorized users within DOJ accessing GAL content, as well as inappropriate sharing by individual employees.

### **Mitigation:**

The possibility of unauthorized users obtaining access to the GAL content is limited by restrictions placed by the EMSG system by IP addresses, as well as account restrictions, in addition to limiting access solely to approved DOJ admin users.

## **Section 7.0 Redress**

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

#### *Information in the GAL:*

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

#### *Information Created by the E-mail Delivery System:*

Individuals can request access to any EMSG 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

---

<sup>1</sup> EMSG will provide logs for:

- Anti-virus / Anti-spam logging and mail routing logs on the individual servers and they are deleted every thirty days; and
- SQL will log all GAL events (adds, deletes, modify, etc.), which are purged after every full or differential backup.



## **7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?**

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

## **7.3 How does the project notify individuals about 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. Additionally, users may correct inaccurate or erroneous information by contacting their component IT Help Desk.

## **7.4 Privacy Impact Analysis: Related to Redress**

### **Privacy Risk:**

Inaccurate or erroneous information is entered in the GAL.

### **Mitigation:**

Inaccurate or erroneous information in the GAL can be corrected by contacting the component Help Desk.

## **Section 8.0 Auditing and Accountability**

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

### **8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?**

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

### **8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.**

DHS mandates annual Computer Security Awareness Training, as well as annual Privacy training to all DHS employees and contractors.

### **8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?**

This directory is only available to other DHS and DOJ employees and contractors with active e-mail accounts issued by DHS.<sup>2</sup>

---

<sup>2</sup> When email accounts are made and associated with user accounts, the user account has the right to have remote access. Outlook Web access is a tool that allows users to access their email through the web, by being able to authenticate to the exchange server with their user account. Only users with valid accounts can access the



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

## **8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?**

While no MOUs are anticipated for the EMSG system, if any are required, they will be reviewed by the program manager, component Privacy Officer, and counsel and then sent to DHS for formal review.

### **Responsible Officials**

David Jones  
Email Product Manager  
Department of Homeland Security

### **Approval Signature**

[Original signed copy on file with the DHS Privacy Office]

Mary Ellen Callahan  
Chief Privacy Officer  
Department of Homeland Security