Privacy Impact Assessment Update
for the

E-Mail Secure Gateway (EMSG)

DHS/ALL/PIA-012(b)

February 25, 2013

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

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) manages and operates the E-Mail Secure Gateway (EMSG) used by all DHS e-mail users. This PIA Update for EMSG clarifies that the directory of user contact information and all e-mail traffic in, out, and between DHS, its components, and the Internet is also available to users on mobile devices. This PIA Update also clarifies the records retention schedule and security of mobile devices. This PIA Update 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.

This PIA Update for EMSG clarifies that the directory of user contact information and all e-mail traffic in, out, and between DHS, its components, and the Internet is also available to users on mobile devices. This PIA Update also clarifies the records retention schedule. This PIA Update does not cover the PII that may be contained within the body of an email or attachment.

Reason for the PIA Update

This PIA Update is being conducted to: 1) describe the information within EMSG that may be viewed and stored on a user's mobile device; 2) update the appropriate General Records Schedule for the retention period of the information stored within EMSG; and 3) describe the security measures within DHS if a mobile device is lost, stolen, or improperly accessed.

Information Shared with Mobile Devices from EMSG

The system is made up of two portions: Directory Services and the E-mail System. 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. 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. 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.

Both the GAL and the E-mail System may be accessed by users on DHS authorized mobile devices. All content that is accessible to users on their desktops or laptops is also available on their mobile devices, including attachments. All DHS mobile devices have End-to-End Secure Communication. End-to-end security means that the entire message is encrypted from sending device to receiving device. This includes emails and messages between mobile devices. All DHS devices must explicitly meet Federal Information Processing Standards (FIPS) Publication 140-2, *Security Requirements for Cryptopgraphic Modules*.[1] If there is unauthorized access to the network or device, the information transmitted is encrypted and unreadable.

Retention Schedule Update

This PIA Update revises the previous EMSG PIA by clarifying that the appropriate General Records Schedule for information created and stored by the E-mail Delivery System is the National Archives and Records Administration (NARA) General Records Schedule 20, item 1, *Files/Records Relating to the Creation, Use, and Maintenance of Computer Systems, Applications, or Electronic Records*. This General Records Schedule requires that the records be deleted when the agency determines that they are no longer needed for administrative, legal, 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.

Security of Mobile Devices

Mobile device security measures are described in the DHS 4300A Sensitive Systems Handbook, Attachment Q2 *Sensitive Portable Electronic Devices (PED).* Wireless PEDs include wireless-capable laptop computers, personal digital assistants (PDA), smart telephones, two-way pagers, handheld radios, cellular telephones, personal communications services (PCS) devices, multifunctional wireless devices, portable audio/video recording devices with wireless

[1] National Institute of Standards and Technology (NIST), *Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptopgraphic Modules* (May 25, 2001), available at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

capability, scanning devices, messaging devices, and any other wireless clients capable of storing, processing, or transmitting sensitive information.

To protect the data stored within the mobile devices, all DHS authorized devices incorporate authentication and data encryption to reduce the likelihood of content disclosure (at rest and in transit). Encryption of devices precludes the need to remotely remove or "wipe" all of the information on the mobile device since it will be inaccessible to an unauthorized user. All information stored on PEDs is encrypted using NIST-validated encryption schemes consistent with the sensitivity of the information stored on the device. Implementing countermeasures such as file and data encryption helps to ensure the confidentiality of information residing on the device. Applications such as file sharing should be disabled on applicable PEDs, and all file sharing ports should be blocked in both directions, especially when processing sensitive information.

In the event of a security incident or loss of mobile device, DHS and components have specific standard operating procedures they must follow to report a lost or stolen device, in accordance with DHS 4300, Attachment F. Inventory management of mobile devices is managed by component.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

The authority for the collection of information by EMSG has not changed. 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).

The PII contained by the EMSG system is addressed under the DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS) SORN, 77 Fed. Reg. 70792 (Nov. 27, 2012). The system security plan and Authority to Operate from July 30, 2011, remains in effect.

Characterization of the Information

There are no changes to the characterization of information from the original PIA.

Uses of the Information

Information stored within the Directory Services and the E-Mail System is also available to users on their mobile devices. DHS does not support bring-your-own-device at this time. Should the Department implement a bring-your-own-device program, a new PIA will be conducted to assess new privacy risks. Information maintained by EMSG is only viewable on government-issued mobile equipment, such as Blackberries. Users have the same ability to search and look up colleagues from the Global Address List and contacts from their Outlook E-mail Contact Folders on their mobile devices as they do in front of their computers. Users can also access their Outlook calendars. A cached copy of the calendar may remain on the EMSG servers once downloaded to a mobile device.

To interact with mobile devices, the EMSG maintains cached copies of messages relayed through the servers to the remote or mobile devices. A transaction log is kept for every message read by or sent to the devices. Information about an individual's web browsing habits may be retained on the mobile device and/or the EMSG servers. All users are authorized federal employees and all relayed e-mail is expected to be for official use only.

Notice

There are no changes to the notice from the original PIA.

Data Retention by the project

This PIA Update clarifies the appropriate records retention schedule approved by the National Archives and Records Administration by the records maintained by EMSG.

For 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. No changes from the original PIA.

For information Created by the E-Mail Delivery System:

This PIA Update revises the EMSG PIA from 2012 by clarifying that the appropriate General Records Schedule for information created and stored by the E-mail Delivery System is the NARA General Records Schedule 20, item 1, *Files/Records Relating to the Creation, Use, and Maintenance of Computer Systems, Applications, or Electronic Records*. This General Records Schedule requires that the records be deleted when the agency determines that they are no longer needed for administrative, legal, 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.

Information Sharing

There are no changes to the characterization of information from the original PIA.

Redress

There are no changes to the characterization of information from the original PIA.

Auditing and Accountability

All DHS authorized mobile devices must follow the security measures are described in the DHS 4300A Sensitive Systems Handbook, Attachment Q2 *Sensitive Portable Electronic Devices (PED)*. To protect the data stored within the mobile devices, all DHS authorized devices incorporate authentication and data encryption to largely prevent content disclosure (at rest and in transit). All information stored on PEDs is encrypted using NIST-validated encryption schemes consistent with the sensitivity of the information stored on the device. Implementing countermeasures such as file and data encryption helps to ensure the confidentiality of information residing on the device. Applications such as file sharing should be disabled on applicable PEDs, and all file sharing ports should be blocked in both directions, especially when processing sensitive information.

In the event of a security incident or loss of mobile device, DHS and components have specific standard operating procedures they must follow to report a lost or stolen device, in accordance with DHS 4300, Attachment F. Encryption of devices precludes the need to remotely remove or "wipe" all of the information on the mobile device since it will be inaccessible to an unauthorized user.

Responsible Official

David Jones
MGMT/OCIO/ITSO/ESDO
Department of Homeland Security

Approval Signature

Original signed copy on file with DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security