FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

PRIVACY IMPACT ASSESSMENT

Enterprise Communications Services (ECS)

November 2012

FDIC Internal System

Table of Contents

System Overview

The FDIC's Enterprise Communications Services (ECS) system, operated by the Division of Information Technology (DIT), provides a platform for exchanging and managing internal (FDIC to FDIC) and external (FDIC to non-FDIC) electronic business communications. It also provides a directory of authorized users' official business contact information, a calendar of users' availability, an option to receive voicemails as email attachments, and a variety of other features[1] to facilitate electronic business collaboration and organization amongst authorized users.

The primary purpose of ECS is to facilitate the exchange of business-related email communications. Depending on the nature and purpose, business emails have the potential to contain any manner of personally identifiable information (PII) and sensitive information (SI), as relevant and necessary for performing legitimate FDIC business activities. In accordance with FDIC policy, any emails containing PII/SI must be secured utilizing FDIC-approved encryption methods. Any non-business related (personal) information transmitted via ECS is considered incidental and at the risk of individual FDIC users.

The FDIC's Enterprise Communications Services platform is comprised of the following key components, which serve the following purposes:

(a) **Directory Services** – The Directory Services portion of the ECS provides a Corporation-wide Global Address List (GAL). The GAL is an electronic directory of the official, business contact information for authorized users with active FDIC email accounts. Users have the option to include their personal cell phone numbers within the Directory/GAL, which is facilitated and tracked using FDIC's Identity Access Management System (IAMS). Additionally, users may optionally choose to their FDIC Personal Identity Verification (PIV) badge photos included within the Microsoft Active Directory service, which facilitates the display of their photograph within various Microsoft Office products, such as the Outlook or Office Communication Server.

(b) **Calendar and Collaboration Services** – The Calendar and Collaboration Services part of ECS provides a calendar that is fully integrated with a user's email and contacts, and offers a variety of scheduling and collaboration functionalities. The Calendar and Collaboration Services component allows users to create appointments and events, organize meetings, view group schedules, and manage other user's calendars. It also allows users to create shared mailboxes and public folders[2] to collect, organize, and share business information with other users.

(c) **Exchange Servers & Mail Stores** – Exchange servers refer to email-based collaborative communications servers used by the Corporation. Exchange servers facilitate electronic mail communications, calendaring, contacts and tasks; support mobile and web-based access to information; and support mailbox data storage. Inbound and outbound emails are stored in relational database by the back-end servers. A user is able to read and delete his/her sent and received emails by logging into the Exchange client which connects to the servers.

(d) **Blackberry Enterprise Server (BES)** – BES technology enables users to send, receive, and manage email messages on their Personal Digital Assistants (PDAs), as well as access applications such as the Microsoft Exchange calendar, contacts and scheduling on their PDAs. BES connects to the messaging and collaboration

[1] Some other features that ECS offers include scheduling options; creation of tasks, public folders, shared mailboxes; Instant Messaging (IM) capabilities; archiving features, etc.
[2] Public folders may contain any type of Outlook item, such as business messages, appointments, contacts, tasks, journal entries, notes, forms, files, and posts.

software on the FDIC's enterprise network, redirects emails, and synchronizes contacts and calendar information between servers, desktop workstations, and mobile devices.

(e) **Email Cache / Archive Repositories** – ECS features repositories where electronic messages may be cached or archived for business purposes.

(f) **E-Discovery Email (EDEM) Solution** – The EDEM solution facilitates the Legal Division's processing and review of large volumes of electronically stored information (ESI)[3], in support of their litigation discovery efforts and other official business duties[4]. EDEM imports data from the FDIC Enterprise Vault and exports data to the Legal Division's Electronic Litigation System (ELS).

(g) **Enterprise Mobility Platform** – The Enterprise Mobility Platform refers to a suite of productivity and management tools that allows authorized users to securely access select enterprise data and applications via their mobile devices. The wireless email solution provides users the ability to compose, send, receive, and read encrypted and/or signed email messages from a mobile device.

(h) **Secure Email Service** – FDIC's Secure Email Service (currently Zix) allows internal FDIC users to communicate confidential and sensitive information with individuals outside the FDIC (external recipients) through a secure channel. Once the message is sent from an FDIC email address, the external user retrieves the message via the FDIC Secure Email Message Center, a secure website. The recipient's reply to the message is automatically encrypted and returned directly to the original FDIC sender's email inbox. FDIC's Secure Email Service works with messages sent from a laptop, desktop, or mobile devices.

(i) **Data Loss Prevention (DLP) Solution** – To help prevent the loss or breach of PII/SI via email, FDIC uses DLP to monitor emails leaving the FDIC network. DLP is capable of capturing PII/SI that is in violation of the policies/rules that have been defined by the FDIC.

(j) **Enterprise Voicemail (EVM) System** – The Corporation's EVM System includes a robust Modular Messaging System that maintains current voicemail functionality, while providing the capability to integrate voicemail with email and fax. EVM allows voicemails to be converted to email attachments and listened to on a user's laptop, desktop, or mobile device. The content of these digital voicemails could potentially contain personal information, depending on the purpose and nature of the message, along with the voiceprint of the individual leaving the message. FDIC users of EVM are advised against leaving voicemails containing PII/SI.

(k) **Office Communications Server (OCS)** – OCS provides Instant Messaging and audio/video conferencing capability to authorized users. Users are able to view the online availability of those they wish to communicate with. User credential information is obtained from Active Directory to register Instant Messaging users and manage access. As with emails, text-based Instant messages exchanged via OCS have the potential to contain PII/SI and may be retained as a conversation history in Outlook if the user chooses to do so. Authorized users of OCS are advised against sending Instant Messages with PII/SI.

[3] ESI can include tens of thousands of emails, word processing documents, PDF files, spreadsheets, presentations, database entries, and other documents in a variety of electronic file formats, as well as scanned paper records.

[4] The FDIC Legal Division is responsible for the collection, review, redaction, and production of agency records, in support of processing and resolving FDIC legal matters, requests related to litigation discovery, subpoenas, and/or applicable laws, as well as to respond to Freedom of Information Act (FOIA)/Privacy Act (PA) requests.

Personally Identifiable Information (PII) in ECS

Directory, Calendar, & Collaboration Services Information – The information in the calendar and collaboration components (e.g., shared mailboxes, public folders, etc.) is intended to be non-sensitive and business-related. The Directory/GAL contains primarily business contact information for FDIC employees and contractors with active FDIC.gov email addresses, including the person's name, division/office, title, FDIC email address, office location, work telephone number, and physical business mailing address. Users have the option of including their personal cell phone numbers within the Directory/GAL, which is facilitated and tracked using FDIC's Identity Access Management System (IAMS). Additionally, users may optionally choose to have their FDIC PIV badge photos included with in the Microsoft Active Directory service.

Server, Mailbox, & Archived Information – The information used by the Exchange servers to record received and processed emails are the sender's email address, IP address and server name, as well as the recipient's email address and email domain server name. The entire contents emails that are identified by FDIC's message scanning software as containing malware or other banned content are quarantined and retained. These quarantined emails may potentially contain PII/SI depending on their intended purpose and use. All other inbound and outbound emails are stored in a relational database and periodically archived in Enterprise Vault after a set time period. Email messages in mailbox stores or Enterprise Vault could potentially include any type of PII/SI that is necessary for fulfilling a legitimate FDIC business function. Any personal (non-business) emails with PII/SI that are exchanged over the FDIC's network and archived or saved in the Enterprise Vault are considered incidental and at the risk of individual users.

E-Discovery Email (EDEM) Information – EDEM processes FDIC emails, attachments, and other ESI. The information in EDEM is wide-ranging in nature and may relate to any type of Corporate and/or Receivership legal matter, legal privileges, litigation discovery, FOIA requests, subpoenas, etc. As such, the emails, attachments, and other sources of ESI in EDEM may contain a variety of PII/SI relating to bank officers, employees, and customers, such as: dates of birth (DOB), Social Security Numbers (SSNs), driver's license/state identification numbers, Employee Identification Numbers (EINs), home addresses, home phone/cell numbers, personal/corporate financial information (e.g., checking account numbers, PINs, access or security codes, passwords), banking records, contracts, legal documents, records or notes (e.g., divorce decrees, criminal records, or other), personal email addresses, employment status and/or records, and non-public financial institution data.

DLP Information – DLP is capable of capturing SI/PII, which may include SSNs, DOB, financial information, and other personal information that may be linked or linkable to specific individuals. However, DLP will only capture information that is in violation of the policies/rules that have been defined by FDIC.

EVM Information – EVM captures call log information, including the time and originating telephone number of the voicemail. The digital voicemails exchanged via EVM could contain any type of audio-based personal information, depending on the purpose and nature of the message, along with the voiceprint of the individual leaving the message. However, as with traditional email, the EVM system is intended to facilitate business activities. Any personal (non-business) emails with PII/SI that are exchanged over the FDIC's network are considered incidental and at the risk of individual users.

OCS Information – In order to authenticate users and manage access, OCS obtains user network credential information (i.e., user login and password) from Active Directory. However, information about user access is not stored locally on OCS. Call log "metadata" (e.g., date, time, length of conversation, and general application used for communication) is stored in a SQL database. The FDIC "system use banner" advises users to refrain from exchanging SI/PII via IM, so any personal or sensitive data exchanged using IM is considered incidental and at the user's own risk.

Purpose & Use of Information in ECS

The collection and use of the data (e.g., user contact information and email credentials) is relevant and necessary for the purposes of the ECS, which is used to exchange, manage, store, and protect all internal and external electronic business-related communications at the FDIC.

Sources of Information in ECS

The information contained in, and exchanged over, ECS is derived from emails and text-based IM conversations that are sent and received by authorized network users.

- **Email Directory/GAL:** By default, if a user has a network account, he/she has an email account. Via an automated process, the FDIC's IAMS application generations email addresses and accounts for approved users. This business contact information is included in the Directory/GAL. In addition, personal cell phone numbers contained in the Directory/GAL are obtained directly from those FDIC employees who have opted to have their cell phone numbers displayed in the Directory. Some users may choose to have their FDIC PIV badge photos included within the Microsoft Active Directory service. The FDIC PIV badge photographs are collected by FDIC Division of Administration (DOA) staff during the FDIC Identification Card/Badging process.
- **Calendar & Collaboration Services Component:** The information shared in the calendar and collaboration components is input by individual users and is intended to be business-related.
- **Exchange Servers:** Header information for all emails and the contents of these emails are collection electronically by the Exchange servers.
- **Enterprise Vault:** Information is derived via an automated archiving process that periodically moves old email messages from the FDIC's Exchange mailbox server to a central email vault on the FDIC's network.
- **EDEM:** Information is derived from Enterprise Vault.
- **EVM:** The contents of digital voicemails are collected and stored on the EVM Message Storage Server (MSS); a copy of the voicemail is sent to the pertinent ESS server and treated the same way as current emails.
- **DLP:** Data associated with violations of DLP policies/rules is captured and maintained in an Oracle database for a period of time as deemed necessary and in accordance with FDIC's record retention policy.
- **OCS:** OCS users may elect to save their text message conversations in their Outlook folders. In addition, the call logs for these text-based conversations are collected electronically by the back-end OCS archiving servers. OCS user credentials are obtained from Active Directory. Also, users may choose to have their FDIC PIV badge photos included within the

Microsoft Active Directory service. The FDIC PIV badge photographs are collected by FDIC Division of Administration (DOA) staff during the FDIC Identification Card/Badging Process.

Notice & Consent

Users may choose to include their personal cell phone numbers within the Directory/GAL, which is facilitated and tracked using FDIC's Identity Access Management System. Additionally, users may optionally choose to have their PIV badge photos included within the Microsoft Active Directory service, which facilitates the display of their photograph within various Microsoft Office products.

Individuals who use the FDIC's Intranet and Internet networks must read and affirmatively confirm that they will abide by FDIC rules when they log onto the FDIC network and when they transmit email. The requested information (e.g., business contact information and email credentials) collected from FDIC email account holders is necessary to ensure that users do not abuse the FDIC's Intranet and Internet networks. Any data stored on FDIC file shares, databases, and/or transmitted over the FDIC network may be monitored. Therefore, there is no mechanism for individuals to opt out of using or exchanging data via ECS.

Access to Data in ECS

Directory, Calendar & Collaboration Services: The Directory, Calendar, and Collaboration Services (e.g., public folders) are available to users with active, FDIC-issued network credentials and email accounts. Authorized individual users have read-only access to the Directory in order to locate contact information of other FDIC personnel for business purposes. Only authorized DIT administrators can modify the information in the Directory. In terms of access to the Calendar and Collaboration features of ECS, individual network users may access, update, and share their individual calendars with other network users; individual network users may also view the published calendars of other network users.

Exchange Mail Stores & client Mailboxes: Individual authorized users have access to their own respective email inboxes to review and send electronic messages in order to perform their business duties and responsibilities. Only authorized DIT security engineering and security operations support staff have access to email messages that are "quarantined" as containing suspected malware or other banned content. As required, they also have access to the Exchange mail stores that contain all email messages. The purpose of their access is to perform system review, administration and maintenance and to validate and report on events identified by the system, as needed.

Enterprise Vault: Individual users have access to their own archived email, but are not able to access other users' archived messages in Enterprise Vault. Only authorized FDIC Legal, Human Resources (HR), DIT, and Office of Inspector General (OIG) personnel have access to all archived information stored in Enterprise Vault. Their access to Vault information is based on a "need to know" and is necessary in order to fulfill official business inquiries related to litigation, personnel actions, and investigations. Specifically, designated Legal personnel have access to Enterprise Vault on a "need to know" basis in order to conduct searches for legal investigations. A limited number of authorized HR staff members have access in order to search for information relating to personnel investigations. OIG

does not have direct access to the Vault. Rather, DIT personnel search EV on behalf of OIG to product and provide copies of requested messages to the OIG for investigations purposes.

EDEM: Access to EDEM and its support components is limited to the following FDIC users:

- Authorized Case Managers and Case Reviewers in the FDIC Legal Division have access all data in EDEM for purposes of performing their official business duties related to legal case matters. Additionally, designated system administrators in FDIC's Legal Division, Legal Information Technology Unit (LITU) staff, and attorneys in the Litigation Support Group have access to the system and data for purposes of processing and exporting the data to the Legal Division's ELS application.
- Authorized regional area and office staff from the FDIC Legal Division, Division of Resolutions and Receiverships (DRR), and Division of Risk Management Supervision (RMS) serving as Case Reviewers have access to EDEM.
- A limited number of users in DIT have access to EDEM for system administration purposes.

DLP: Access to the data in DLP is based on a business need. Individuals with authorized access to the DLP data include:

- Authorized FDIC Privacy Program staff have access to data within the system in order to validate and report on events identified by the system.
- The Information Security and Privacy Staff (ISPS) Security Protection Engineering Services Section (SPES) have access to data in the system in order to validate events identified by the system.
- The DLP Project/Technical Manager/Administrator has access to the data within the system for administrative purposes and to validate and report on events identified by the system.
- The Chief Information Security Officer (CISO) has access in order to receive and report on events identified by the system.

EVM: As with traditional email, access to digital voicemail is granted to the individual authorized user of each respective mailbox. Authorized EVM administrators only have access if needed to perform system maintenance and/or resolve incidents.

OCS: By system default, individual OCS users have access to their own saved text messages, which are accessible via network authentication. Authorized OCS system administrators may have access to the servers supporting the OCS application, which include the call logs and conversation histories saved by users.

Data Sharing

Other Systems that Share or Have Access to Data in the System:

System Name	System Description	Type of Information Processed
E-Discovery E-mail (EDEM)	EDEM is used by the FDIC Legal Division to improve the discovery process by reducing time and costs associated with the processing and review of large volumes of electronically stored information (ESI). EDEM processes FDIC emails, attachments, and other	DOB, SSN, driver's license/state identification numbers, EIN, home address, home phone number,

System Name	System Description	Type of Information Processed
	ESI.	personal/corporate financial information, banking records, contracts, legal documents, records or notes, personal email addresses, employment status or records, and non-public financial institution data
Data Loss Prevention (DLP)	DLP monitors outbound electronic data at network check points. DLP is capable of capturing SI/PII.	SSN, DOB, financial information, etc.
SCAN-IT 2.86 (SCAN-IT)	SCAN-IT, a component of EDEM, is an application that combines electronic discovery data processing, conventional paper scanning, and printing into one.	ESI and other records collected from FDIC employees and internal FDIC systems

Data Accuracy in ECS

It is the responsibility of each individual user to ensure the completeness and accuracy of the content of any electronic messages/data they choose to transmit over ECS. Individual authorized users may correct inaccurate or erroneous information in the GAL/Directory by contacting the DIT Help Desk.

Data exchanged between ECS components/applications and internal FDIC data sources may be accepted "as-is" or checked for completeness using automated quality control mechanisms.

Data Security for ECS

Access to the data within ECS is limited based on business need. All authorized users who have access to ECS or its components must have the approval of their Manager/Supervisor and the pertinent DIT Program Manager/Data Owner before access is granted. All access granted is on a "need to know" basis. As needed, access to certain components of ECS is further restricted by functional security limits and automated access controls.

System of Records Notice (SORN)

ECS does not operate as a Privacy Act System of Records.

Contact Us

To learn more about the FDIC's Privacy Program, please visit: http://www.fdic.gov/about/privacy/.

If you have a privacy-related question or request, email Privacy@fdic.gov or one of the FDIC Privacy Program Contacts. You may also mail your privacy question or request to the FDIC Privacy Program at the following address: 3501 Fairfax Drive, Arlington, VA 22226.