FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

PRIVACY IMPACT ASSESSMENT

Data Loss Prevention (DLP)

May 2008

FDIC Internal System

Table of Contents

System Overview

The FDIC Division of Information Technology utilizes the Data Loss Prevention (DLP) was application to facilitate compliance with the Office of Management and Budget (OMB) Memorandum M-06-16 (Protection of Sensitive Agency Information) and OMB Memorandum M-07-16 (Safeguarding Against and Responding to the Breach of Personally Identifiable Information). DLP is also used to establish visibility and remediate, if necessary, violations of FDIC Circular 1360.9, *Protecting Sensitive Information*. Using Vontu Network Monitor, the DLP project monitors outbound electronic 'data in motion' at network outlet points, while network 'data at rest' is monitored using Vontu Discover software.

Personally Identifiable Information (PII) in DLP

The DLP application is capable of capturing sensitive information, which may include social security numbers (SSN), dates of birth, financial information, and other personal information that may be linked or linkable to specific individuals. However, DLP only captures information that is in violation of the policies/rules that have been defined by an administrator within the Vontu software. For instance, if a Vontu policy/rule has been defined to identify unencrypted emails to be delivered outside the FDIC that contain more than five Social Security Numbers, then Vontu will capture the data associated with any emails that are in violation of that policy/rule. Similarly, if an unencrypted email containing only four SSNs (the Vontu policy/rule in this example is set to 5 SSN) were destined to be delivered to an address external to FDIC then it would not be in violation of the policy/rule, so no data would be captured in that instance.

Purpose & Use of Information in DLP

The collection and use of data facilitated by this application is relevant and necessary to the purpose for which the application was designed, which is to identify, validate and remediate data leakage events of a sensitive nature.

Sources of Information in DLP

DLP, using the policies/rules defined and configured by FDIC administrators within the Vontu software, monitors internal FDIC network file shares and monitor incoming/outgoing Internet traffic via the following protocols (on various ports): Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Instant Messaging (IM). Data associated with violations of the configured Vontu policies/rules will be captured and maintained in an Oracle database for a period of time as deemed necessary in accord with FDIC's record retention policy.

Notice & Consent

There is no mechanism for individuals to opt-out of monitoring. Any data stored on FDIC file shares, databases, and/or transmitted over the network to the Internet is monitored by DLP.

Access to Data in DLP

Access to the data in the system is based on business need and requires approval of the Privacy Program Manager. An individual's access to data within the system will be restricted based on business need and dependent on the role to which they are assigned within the system. Individuals that have authorized access to the DLP data include:

- The Privacy Program Manager and 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 & Privacy Staff/Security Protection Engineering Section (SPES) Section Chief has access to data in the system in order to validate events identified by the system.
- The DLP Project/Technical Manager/Administrator has access to 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 to data in the system in order to receive and report on events identified by the system.

Data Sharing

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

Currently no other systems share or have access to data within the DLP system. However, in the future, alerts may be exported to the ArcSight Security Incident Event Manager (SIEM) for identification and resolution. The alerts exported by DLP to SIEM will not contain any sensitive or privacy information.

System Name	System Description	Type of Information Processed
N/A	N/A	N/A

Data Accuracy in DLP

Due to the nature of the application, there is no way to validate or verify the completeness of data collected and maintained by the application. Data will not be collected from sources other than FDIC records.

Data Security for DLP

The system uses role-based security to limit access to data collected and maintained by the system. System users are assigned to a specific role based on their business need for access. For example, analysts cannot change the configuration of the system but can perform reporting functions. Additionally, role-based training is provided to users of the system, and they are required to formally review the System Rules of Behavior prior to being provided first-time access to the system and on a periodic basis thereafter.

System of Records Notice (SORN)

DLP currently does not operate under any FDIC Privacy Act SORN.

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.