U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration

FAA

Data Loss Prevention System

DLPS

Responsible Official

John Peery
john.peery@faa.gov
405-397-5161

Reviewing Official

Karyn Gorman
Acting Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

Pursuant to the Federal Information Security Modernization Act of 2014 (FISMA) [1], the Federal Aviation Administration (FAA) implemented the Data Loss Prevention System (DLPS) to help safeguard its sensitive information. The FAA uses DLPS to identify, prevent, and remediate the transmittal and storage of unencrypted Social Security Numbers (SSN) and Credit Card Numbers (CCN) on FAA servers and networks. This update to the DLPS Privacy Impact Assessment (PIA) addresses risks associated with DLPS's capture and storage of emails that may contain unencrypted SSNs/CCNs before they have left the FAA network. In addition, this PIA also addresses risks associated with DLPS's storage of unencrypted suspected SSN/CCN on FAA servers and networks.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[2]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*

[1] (PL 113-283, 44 USC 3554)

[2] Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The FAA's Office of Information and Technology Services (AIT), Information Security and Privacy Service (AIS), Security and Privacy Risk Management staff (Risk Management Staff) use the web-based Symantec DLPS to identify, prevent, and remediate the transmission and storage of unencrypted SSNs/CCNs in FAA Systems (FAA servers and networks).

DLPS scans for unencrypted personally identifiable information (PII) across three threat vectors: *Data in Motion*, *Data in Use*, and *Data at Rest*. DLPS scans FAA systems that store unencrypted SSNs/CCNs and emails sent from the FAA. As a matter of best practice and to minimize the number of false positives, DLPS identifies any string of unencrypted nine- or sixteen-digit numbers to identify potential SSN/CCNs that are found in close proximity to a specific set of keywords. Keyword examples are: "CCN," "CC#", or "credit card num" for sixteen-digit numbers and "SSN," "SS#," or "Social Security Num" for nine-digit numbers. If a nine- or sixteen-digit number exists but is not in close proximity to a keyword, the SSN/CCN policies will not be triggered.

Data in Motion

The DLPS continuously monitors emails sent from the FAA network for potential unencrypted SSNs/CCNs. The FAA uses Microsoft Office 365 (FAA-O365) as its secure email messaging service. DLPS only monitors emails sent from the FAA and does not monitor emails sent to the FAA or sent within the FAA intranet. If a suspected unencrypted SSN/CCN is found, DLPS prevents the email from being sent, and stores it on an encrypted server for remediation purposes. Once an email is identified and the transmission blocked, the name of the owner of the FAA email account and email metadata (metadata on the owner of the email account is provided by the FAA Directory Services) is sent to the DLPS dashboard for the Risk Management Staff to review. The file metadata may include the FAA employee's or contractor's phone number, email address, name, supervisor/Contracting Officer Representative (COR)'s phone number, and supervisor/COR's email address. The Risk Management Staff then follows the applicable "DLPS Findings Review Process," as described below.

Data in Use

The DLPS Windows 10 agent is installed on over 50,000 FAA employee and contractor workstations. It continuously scans these workstations and blocks unencrypted potential SSNs/CCNs from being transferred to:

- Universal Serial Bus (USB) devices
- Local hard drives
- Writable Compact Discs (CDs)
- Digital Versatile Discs (DVDs)
- Being sent via user's FAA-O365 Teams Instant Message
- Hypertext Transfer Protocol (HTTP)/Hypertext Transfer Protocol Secure (HTTPS), and
- File Transfer Protocol (FTP)

Once the DLPS has identified and blocked the transmission of a potential SSN/CCN, it sends the FAA employee's or contractor's name and file metadata to the DLPS for the Risk Management Staff to review.

Data at Rest

The DLPS provides the Risk Management Staff the ability to schedule ad-hoc scans of FAA systems including searches of FAA file shares, document repositories, and websites for files that potentially contain unencrypted SSNs/CCNs. Once the DLPS has identified an unencrypted SSN/CCN, it sends the FAA employee's or contractor's name and file metadata (as described above) to the DLPS for the Risk Management Staff to review.

DLPS Findings Review Process

The Risk Management Staff reviews all instances of system-reported unencrypted SSNs/CCNs reported to the DLPS. The review process requires the Risk Management Staff to access the content of the suspect file/email to verify that the DLPS correctly identified an unprotected SSN/CCN. Once the Risk Management Staff's review is completed and the data identified is not a false positive, review of the incident is passed via email to the FAA's AIS Vulnerability Management Staff. Once their review is complete, the validation outcome is noted in the incident record along with the reviewer's notes supporting their determination of remediation.

Confirmed Findings

If the DLPS finding is validated, the Vulnerability Management Staff looks at the metadata of the file or email, and the FAA Directory Services (Active Directory)[3] to

[3] The FAA Directory Services (Active Directory) is a general support system that supports the FAA's mission by providing an authentication source for customers and services on the FAA network. DLPS collects contact information for all FAA

identify the file owner. To identify the FAA employee or contractor who sent the email or saved the file, the Risk Management Staff uses the email address, the recipient's email address[4], the file owner's name, phone number, address, and line of business[5]. The FAA employee or contractor's line of business may provide the Vulnerability Management Staff additional insight about the business purpose for sending a SSN/CCN. For example, most potential SSN/CCN findings come from the FAA's Office of Human Resource Management (AHR) and are employment related. The Risk Management Staff will then send an email to the FAA's Security Operations Center (SOC) detailing the event, and request a ticket be opened in the Cyber Security Information Management System (CSIMS), for tracking of remediation status. The Vulnerability Management Staff analyzes all CSIMS findings of unencrypted SSNs/CCNs.

The DLPS sends an email to the FAA employee or contractor who failed to encrypt the email containing the SSN/CCN, informing them of the event and instructing them on how to send the email successfully. The DLPS does not include the SSN/CCN in the email sent to the end user. The Risk Management Staff notifies the employee or contractor to redraft the email or recreate the file and encrypt if there is a valid business purpose.

If there is no business purpose for the SSN/CCN to be included in the email or file, the FAA employee or contractor is required to redact the SSN/CCN or delete the email or file. If the FAA employee or contractor refuses to redact the unencrypted SSN/CCN or delete the email or file, the Vulnerability Management Staff refers them to AHR and the FAA's Office of General Counsel (AGC) for disciplinary action.

False Positives

False positives occur when an event is triggered based on the DLPS SSN/CCN policies but has identified the numerical string erroneously. In all instances of a false positive, the event is tagged false positive in the DLPS. When a false positive is triggered, the Risk Management Staff modifies the SSN/CCN policies to account for the false positive and the event is removed from DLPS. If the false positive occurred in an email, the end user is notified of their need to recreate the email and resend it. If the false positive occurred in a file, the file owner does not need to do anything. Once the Risk Management Staff indicates a false positive in the initial pass or the Vulnerability Management Staff

employees and contractors (e.g., names, email addresses, phone numbers, line of business, etc.) from the FAA Active Directory, as necessary, for the Risk Management Staff to be able to track down, and follow up with the person who sent an email or saved a file containing a potential unencrypted SSN/CCN.

[4] The recipient's email address is used for by the Risk Management Staff to follow-up with the employee or contractor to see if there was a business purpose for SSN use and to instruct them to encrypt the SSN/CCN when it is released to them.

[5] This information is used to identify and contact the employee or contractor who saved or sent and unencrypted file or email containing SSN/CCN.

indicates a false positive through their remediation efforts, the DLPS no longer flags that instance of suspected SSN/CCN.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[6], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[7].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

The FAA employs multiple techniques to ensure that individuals are informed of the purpose for which the FAA collects, uses, disseminates, and retains their PII within DLPS. Information about the DLPS program is provided to FAA employees and contractors via broadcast communications. The FAA also requires all employees and contractors to take annual security training, which includes information about DLPS and data protection responsibilities. If a user attempts to send an email, which DLPS subsequently blocks, they will receive an email stating why their email was blocked and what steps they can take to correct the issue.

DLPS records are maintained in accordance with the Department's Privacy Act System of Records Notice (SORN), DOT/ALL 13, Internet/Intranet Activity and Access Records, May 7, 2002 67 FR 30758.

The publication of this PIA further demonstrates DOT's commitment to provide appropriate transparency regarding the handling of such information.

[6] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[7] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

DLPS does not collect SSNs/CCNs directly from individuals and therefore does not provide them with the opportunity to correct or amend their PII within DLPS. DLPS only scans the FAA's systems to ensure that SSNs/CCNs are being stored and transmitted in an encrypted state, as required by FISMA, and to remediate any unauthorized exposure of SSNs/CNNs. Individuals can always reach out to the DLPS System Owner to determine if records are maintained on them.

Additionally, individuals may request searches to determine if any records appear in any FAA system of records. Individuals wishing to know if their records appear in DLPS may inquire in person or in writing to:

Federal Aviation Administration
Privacy Office
800 Independence Avenue, SW
Washington, DC 20591

The written request must include the following information:

- Name
- Mailing address
- Phone number and/or email address
- A description of the records sought, and if possible, the location of the records
- Signed attestation made under penalty of perjury stating your identity

Additional information about the Department's privacy program may be found at www.transportation.gov/privacy. Individuals may also contact the DOT Chief Privacy Officer at privacy@dot.gov.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII. The PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.

DLPS is used to identify, validate, and remediate the transmission of unencrypted SSNs/CCNs in FAA systems, pursuant to its responsibility to provide information security under the Federal Information Security Modernization Act of 2014 (FISMA). The events captured during a DLPS scan are used to identify and contact an FAA employee or contractor who sent an email from the FAA network or saved a file to a FAA server with unencrypted SSNs/CCNs. These events allow the Risk Management Staff to identify suspected storage or transmittal of unencrypted SSNs/CCNs.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

DLPS provides the minimum amount of information necessary for the Risk Management Staff and/or the Vulnerability Management Staff to determine whether there is a valid SSN/CCN finding or a false positive. Further, suspected SSNs/CCNs are masked in the DLPS dashboard. Only the Risk Management Staff and the Vulnerability Management Staff with specific permissions may view the suspected SSNs/CCNs for purposes of validation.

DLPS audit logs are maintained and disposed of in accordance with National Archives and Records Administration (NARA), General Records Schedule (GRS) 3.2, Item 030, *System access records*, as they are created as part of the user identification and authorization process to gain access to DLPS. Records are used to monitor inappropriate systems access by users. These records are destroyed when business use ceases. Information technology operations and other maintenance records, which are created in DLPS, are disposed of in accordance with General Records Schedule 3.1, item 020, General Technology Management Records. These records are destroyed three years after agreement, control measures, procedures, activity or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

FAA uses DLPS to identify, prevent, and remediate the transmittal and storage of unencrypted SSNs/CCNs on FAA servers and networks. PII maintained within the DLPS is used only for the purpose of validating that an unencrypted SSN/CCN was captured, and identifying and contacting an FAA employee or contractor who sent an email from the FAA network or saved a file to a FAA server with unencrypted SSNs/CCNs.

If a valid event of SSNs/CCNs being unencrypted occurs, the Risk Management Staff gathers contact information, including the name, phone number, email address, supervisor, supervisor phone number, and supervisor email address of the file owner from FAA Directory Services. The Risk Management Staff then sends an email to the FAA SOC, which includes the CSIMS ticketing system, and is used to track the remediation of the event. This information is only used by the FAA SOC to remediate the issue, and is covered pursuant to the routine uses set forth in DOT/ALL 13, Internet/Intranet Activity and Access Records; specifically, "To provide information to any person(s) authorized to assist in an approved investigation of improper access or usage of DOT computer systems."

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

DLPS does not collect information directly from the public or any other primary source; data quality and integrity depends on the FAA systems performing the original collection. The Risk Management Staff use metadata and FAA Directory Services to identify the FAA employee or contractor who sent an email from the FAA network or saved a file to a FAA server with unencrypted SSNs/CCNs. FAA Directory Services is updated frequently to ensure contact information for FAA employees and contractors are accurate.

When DLPS identifies a file or email containing potential unencrypted SSNs/CCNs, the Risk Management Staff first reviews the context of the file or email sent to determine if an actual unencrypted SSN/CCN has been involved. If the Risk Management Staff and the Vulnerability Management Staff determine the finding to be valid, then they look at the metadata of the file or email to identify the file owner. The remediation actions of Vulnerability Management Staff are limited to the choices that are available in DLPS. Those actions are: *New, Escalated, Investigation, Resolved, Dismissed.* In all instances of a false positive, the event is tagged as a false positive in the DLPS. When a false positive is triggered, the Risk Management Staff modifies the SSN/CCN policies to account for the false positive and the event is removed from DLPS. If the false positive occurred in an email, the end user is notified of their need to recreate the email and resend it. If the false positive occurred in a file, the file owner does not need to do anything. Once the Risk Management Staff indicates a false positive in the initial pass or the Vulnerability Management Staff indicates a false positive through their remediation efforts, the DLPS no longer flags that instance of suspected SSNs/CCNs.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

The FAA protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the FISMA and are detailed in Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006, and NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated January 22, 2015.

DLPS is a web-based system that is only accessible within the FAA network. DLPS implements administrative, technical, and physical measures to protect SSNs/CCNs against loss, unauthorized access, or disclosure. Specifically, DLPS takes the following steps to safeguard SSNs/CCNs:

- **Identification and authentication**: Authorized users authenticate to the system using their PIV-credentials, i.e. two-factor authentication. Authorized users are only able to access the system within the FAA secured network.
- **Roles and permission**: DLPS access is limited to members of the Risk Management Staff. Further, DLPS manages access to SSNs/CCNs with user roles. Only users assigned a role within the system can authenticate into the system. Their access is limited to the role to which they are assigned. A DLPS user with scanning capability does not have access to view the information gathered during the scan. Remediation roles can view the captured data, but cannot execute scans, change policies, etc.

DLPS automatically masks potential SSNs/CCNs, so that only Risk Management Staff with appropriate permissions may view the full SSNs/CCNs. Additionally, emails and attachments, which contain SSNs/CCNs, are destroyed three years after all follow-up actions have been completed.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

The FAA's AIS Security Governance Division is responsible for the administration of FAA Order 1370.121A, *FAA Information Security and Privacy Program & Policy*. FAA Order 1370.121A defines the various privacy requirements of the *Privacy Act of 1974*, as amended (the Privacy Act), the *E-Government Act of 2002* (Public Law 107-347), the *Federal Information Security Management Act (FISMA)*, DOT privacy regulations, OMB mandates, and other applicable DOT and FAA information technology management policies and procedures. In addition to these, other policies and procedures will be consistently applied, especially as they relate to the access, protection, retention, and destruction of PII. Federal and contract employees are given clear guidance on their duties, as they relate to collecting, using, processing, and security privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training. In addition, staff are required to acknowledge understanding of the FAA Privacy Rule of Behavior (ROB) and agree to them before being granted access to FAA information systems. The DOT and FAA Privacy Offices will conduct periodic privacy compliance reviews of DLPS relative to the requirements of OMB Circular A-130, *Managing Information as a Strategic Resource*.

Responsible Official

John Peery
System Owner
Security and Privacy Risk Management

Approval and Signature

Karyn Gorman
Acting Chief Privacy Officer
Office of the Chief Information Officer