U.S. Department of Transportation

Office of the Secretary (OST)

Privacy Impact Assessment
Security Operations System (SOS)

Responsible Official

Terry Brewster
Associate Director
Office of Security
terry.brewster@dot.gov

Approving Official

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

Executive Summary

Within the Department of Transportation (DOT), the Security Operations Systems (SOS) are used by Office of the Secretary of Transportation (OST), Office of Security, to support the Interagency Security Committee requirements for physical security operations and processes. The SOS provides physical security controls, real-time alarm monitoring and video monitoring. The SOS is composed of two primary subsystems: the automated *Physical Access Control System (PACS*) and *the Video Management System (VMS).* The PACS and VMS are physically located throughout the DOT Headquarters in Washington, DC. OST has the authority to operate and maintain records in the SOS IT system under 49 U.S.C. 114, Chapter 1, Transportation Security Administration and 49 CFR 1.38, Delegations to the Assistant Secretary for Administration.

The Office of Security is publishing this Privacy Impact Assessment (PIA) in accordance with the E-Government Act of 2002 because the SOS components collects, uses and maintains Personally Identifiable Information (PII) including first and last name, address, picture and signature from the public.

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.[1]

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:

[1] 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).

- *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*
- *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 SOS are used in support of security operations processes including monitoring performance of security checks by guard personnel; facility entry control; and monitoring of electronic access (intrusion detection) systems. SOS is composed of two primary subsystems: the automated Physical Access Control System (PACS) and the Video Management System (VMS). The SOS is managed by the OST Office of Security which is responsible for the physical security of DOT assets and people. The SOS provides physical security controls, real-time alarm monitoring and video monitoring. SOS makes it possible for the security guards at entrances to DOT headquarters buildings to match the face of the person coming in with the face on the Personal Identity Verification (PIV) card and with the picture and information coming up on the computer used by the security guard. Components of SOS make it possible to detect any tampering of the badge or if a valid badge is being used by a person other than the one that the badge was issued to.

Physical Access Control Systems (PACS)

The PACS is divided into two sub systems consisting of the Physical Access Control (PAC) which manages the physical gateway to buildings at DOT Headquarters and Visitor Management, which is used to collect information on non-DOT visitors to the DOT Headquarters buildings.

Physical Access Control (PAC)

The SOS PACS is a Lenel OnGuard Physical Access Control System. This system provides physical access control to aid the security organization with employee identification and authorization (through use of DOT Badge Credential) and physical intrusion detection for the DOT Headquarters building located in Washington, DC. The PACS is a distributed system with a physical presence throughout most of DOT Headquarters.

The SOS PACS receives last name, first name, middle name, suffix, picture, DOT Mode, organization name, PIV card number, PIV issue date and PIV expiration date from the Federal Aviation Administration (FAA) PIV solution, the Identification Management System PIV Authentication Database (IDMS PAD). This information is needed to create a card holder in the SOS Lenel system. The FAA is the owner of the Card Management System (CMS) that is used to provision PIV cards that both DOT and FAA use to request, enroll, activate and issue the card to the card holder. Once an employee is issued a PIV card, or when a PIV card is canceled, it automatically populates the SOS PACS system so the new card holder can access the DOTHQ, or when cancelled in CMS, SOS PACS is updated to show that the individual's card is no longer active and to not allow access.

To import data from the CMS system into the PACS system the Office of Security is required by the Federal Information Security Modernization Act (FISMA) to maintain an Interagency Agreement (IAA) with the FAA Office of Security and Hazardous Materials Safety (ASH) in support of this interconnection.

Visitor Management

The Visitor Management system is an integrated component of the Lenel Onguard System. It is used to collect information on visitors (individuals who have not been issued a DOT badge credential) and their visit date and entry times. Visitor shows a valid government issued photo ID in order to be processed for entry and receive a visitor badge. On duty Security Officer utilizes an ID scanner to read the data on the card and automatically populate the database. If the scanner is unable to function with the card, the data is manually entered by the Security Officer, utilizing the ID as the data source. An electronic record is created in Visitor Management System for the visit. Visitors must be escorted to enter the building. They also must be escorted to exit the building. Badges are collected prior to exiting.

VIDEO MANAGEMENT SYSTEM (VMS)

The SOS VMS is a Bosch Video Management System that monitors live or recorded video events in and around the DOT headquarters buildings and respond to life safety, homeland security, property protection, and other emergency events. The VMS consists of cameras and emergency call box locations throughout the Headquarters parking garage. The VMS provides the capability to protect our employees, visitors, sensitive information, critical IT systems, servers and other physical assets. The VMS stores digital video which is retained for 30 days and then overwritten by the system. Due to the nature of the system and placement of cameras, the system may capture unintended video images of the general public as they pass the building or, perhaps, license plates of vehicles passing by the property.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template 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[2], 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[3].

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.

DOT and SOS System of Records Notices (SORNs) provide transparency about privacy practices regarding the collection, use, sharing, safeguarding, maintenance, and disposal of information about individuals covered under the Privacy Act of 1974, as amended. SOS contains information on individuals that includes last name, first name, middle name, signature, suffix, picture, DOT mode and organization name and addresses. PII in the system may be retrieved in the system by name, address, or some combination thereof. Social Security Numbers are not collected or maintained in the system.

DOT protects records subject to the Privacy Act for each subsystem in accordance with the following published System of Records Notices (SORNs): DOT/ALL 9 - Identification Media Record Systems - 67 FR 62511 - October 7, 2002 and DOT/OST 046 - Visit Control Records System - 65 FR 19555 - April 11, 2000. There are no exemptions claimed for either system.

There are signs at DOT entrances informing individuals that they are under surveillance. These signs are posted near turnstiles.

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

[3] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

The publication of this PIA further demonstrates DOT's commitment to provide appropriate transparency into SOS IT system. Information on the Department's privacy program may be found at www.transportation.gov/privacy.

Individual Participation and Redress

DOT should provide 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 be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Under the provisions of the DOT's Privacy Act/Freedom of Information Act (FOIA) procedures, individuals may request searches of SOS to determine if any records have been added that may pertain to them. The Freedom of Information Act (FOIA) is a federal law that gives you the right to access any U.S. Department of Transportation (DOT) records unless DOT reasonably foresees that the release of the information in those records would harm an interest protected by one or more of the nine exemptions (such as classified national security, business proprietary, personal privacy, investigative documents) or release is prohibited by law. Video recordings are searchable by the Office of Security. If court orders, subpoena, FOIA requests, or an inquiry from Human Resources come through the Office of General Counsel the video recordings can be searched. The video is searched around the time recorded when PIV card was read while entering or leaving the building. However, the video recordings are kept for 30 days only.

Notification procedure: Requests should be submitted to the attention of the official responsible for the record at the address below:

Office of Security, M-40
Office of the Assistant Secretary for Administration
Department of Transportation
1200 New Jersey Ave, SE
Washington DC, 20590
Email: privacy@dot.gov
Fax: (202) 366-4677

Department policy requires the inquiry to include the name of the individual, mailing address, phone number or email address, a description of the records sought, and if possible, the location of the records.

Contesting record procedure: Individuals wanting to contest information about them that is contained in this system should make their requests in writing, detailing the reasons for and why the records should be corrected. Requests should be submitted to the attention of the OST Official responsible for the record at the address below:

Office of Security, M-40
Office of the Assistant Secretary for Administration
Department of Transportation
1200 New Jersey Ave, SE
Washington DC, 20590
Email: privacy@dot.gov
Fax: (202) 366-4677

Privacy Act request for records covered by system of records notices not published by the Department are coordinated with the appropriate customer privacy official and acted upon accordingly.

Additional information about the Department's privacy program may be found at https://www.transportation.gov/privacy-program/about-us. Individuals may also contact the DOT Chief Privacy Officer at: privacy@dot.gov. For questions relating to DOT's Privacy Program please go to http://www.dot.gov/privacy

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 its collects, uses, maintains, or disseminates PII.

SOS is used in support of security operations processing including monitoring of electronic access and intrusion detection systems. PII maintained in the system is received directly from individuals and from FAA and aligns with the purpose of the collection. SOS makes it possible for the security guard at entrances to DOT buildings to match the face of the person coming in with the face on the PIV card and with the picture and information coming up on the computer used by the security guard. Components of SOS make it possible to detect any tampering of the badge or a valid badge being used by a person other than the one person who was issued the badge. The information maintained and collected are only used for the purpose for which it was collected pursuant to the following legal authorities:

- Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
- 49 U.S.C. 114, Chapter 1, Transportation Security Administration
- 49 CFR 1.38, Delegations to the Assistant Secretary for Administration.

SOS data is used consistent with the purposes for which it was collected as described in SORNs DOT/ALL 9 - Identification Media Record Systems - 67 FR 62511 - October 7, 2002 and DOT/OST 046 - Visit Control Records System - 65 FR 19555 - April 11, 2000.

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. DOT should retain PII for only if necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

The VMS stores digital video which is retained for 30 days and then overwritten by the system. Due to the nature of the system and placement of cameras, the system may capture unintended video images of the general public in performance of its mission. To provide complete security coverage, the cameras inadvertently capture images of individuals and the licenses plates of vehicles that pass through the cameras' field of vision. Records are not kept indefinitely. At times there are court orders, subpoena, or FOIA requests or inquiry from Human Resources (HR) that come through Office of General Counsel that require holding records indefinitely. Office of general Counsel must approve such requests and a Senior Executive Service (SES) must sign the document. However, these are temporary and as soon as the hold is lifted records are retained according to approved records schedule.

NARA's General Records Schedule (GRS) 5.6 - Security and Protective Services Records covers various components of SOS. However, different item numbers from 090 to 111 are applicable to different components. SOS components are listed below with corresponding item of GRS:

PACS-Physical Access Control:

GRS 5.6, item 090 – **Facility Security Management Operations Records.** Disposition: Temporary. Destroy when 30 days old, but longer retention is authorized if required for business use.

PACS-Visitor Management:

GRS 5.6, item 111: **Visitor Processing Records – Facility Security Areas Designated by the Interagency Security Committee as Facility Security Levels I through IV**: Registers or logs recording names of outside contractors, service personnel, foreign national and other visitors, employees admitted to areas, and reports on vehicles and passengers. Disposition: **Temporary**. Destroy when 2 years old, but longer retention is authorized if required for business use.

Video Management System:

GRS 5.6, item 090 - **Facility Security Management Operations Records.** Disposition: Temporary. Destroy when 30 days old, 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.

SOS collects the minimum necessary PII in its system to ensure compliance with regulations and agency mission. PII information is not used in any manner that is not specified in notices and is only used for the purposes collected. SOS does not publicly post any PII information. The system does not interface with, nor are they interconnected with other automated information resources. Data in this system is not shared with other systems. At times there are court orders, subpoena, or FOIA requests or inquiry from HR that come through Office of General Counsel that require holding records indefinitely. Office of general Counsel must approve such requests and an SES has to sign the document. However, these are temporary and as soon as the hold is lifted records are retained according to approved records schedule. Access to the data in the system is limited to those who have a need to know and aligns with their responsibilities.

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).

The SOS IT system ensures that the collection, use, and maintenance of information collected for operating the PACS, Visitor Management and Video Management systems are relevant to the purposes for which it is to be used, and to the extent necessary for those purposes; and it is accurate, complete, and up to date. PII maintained in PACS originates from FAA. The FAA is responsible for ensuring the data provided to SOS is accurate and complete. PACS manages the physical access to buildings at DOT Headquarters by validating data presented on the PIV card against FAA information. Video Management collects information on visitors, including the date and time of visits. Information n the system is managed by submitting visitors PII on ID scanners, which issues visitors cards and track the dates. Video data is used to monitor individuals that enter DOT.

Security

DOT shall implement administrative, technical, and physical measures 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.

SOS takes appropriate security measures to safeguard PII and other sensitive data. SOS applies DOT security standards, including but not limited to routine scans and monitoring, back-up activities, and background security checks of technical employees and contractors.

The DOT network has been designed for protection from internet attacks and there are protective devices strategically placed to prevent unwanted attacks from within the network. DOT has employed intrusion detection/prevention and firewall devices throughout the network to protect the network from malicious attacks.

Antivirus software is utilized for malicious code protection on systems where real-time scans on media are performed. A full system scan is performed on a weekly basis and virus definitions are automatically updated on all servers and all the clients.

There are formal procedures in place for granting access to SOS. SOS does not permit any guest accounts or shared accounts and only users with authorized approvals may access the information system and user account reviews are completed monthly. DOT employees are required to adhere to information system security controls. The SOS is a Role-Based Access Controlled (RBAC) configuration where it identifies the user groups that are required for the administration, operation and maintenance of the system and the privileges needed for personnel in these groups. Only the Admin role, under the direction of the System Owner, can administer and/or configure system functions. The roles-based access controls are used to apply the concept of least privilege.

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.

OST Personnel Security is responsible for identifying, training, and holding Agency personnel accountable for adhering to DOT privacy and security policies and regulations. The Department will follow the Fair Information Principles as best practices for the protection of information associated with SOS. In addition to these practices, policies and procedures are consistently applied, especially as they relate to protection, retention, and destruction of records. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing data. Guidance is provided in the form of mandatory annual Security and privacy awareness training as well as Acceptable Rules of Behavior. The Department Chief Privacy Officer conducts regular periodic security and privacy compliance reviews of SOS consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems.

SOS audit logs are periodically reviewed for any anomalies. The SOS auditing system captures account maintenance and events. The System Owner, Information Systems Security Manager (ISSM) and/or Cybersecurity Management Center (CSMC) will determine the frequency and any changes which need to occur on the system due to the current threat environment. Only authorized system, database, and application administrators have rights sufficient to access audit

logs based on their particular roles. The logged auditable events are adequate to support after-the-fact investigations based on previous requests made by the CSMC.

SOS Rules of Behavior documents are in place that outline specific guidelines for usage of SOS information systems and acknowledge that SOS users understand their roles and responsibilities relative to SOS system access and usage.

The DOT Order 1351.37 Departmental Cybersecurity Policy ensures that the SOS System Owner is responsible for ensuring information system security awareness training is provided to new employees automatically, and re-assigned annually, to employees and contractors with access to SOS. Personnel who are assigned to a DOT project with access to DOT information or information systems complete annual security awareness training and that evidence of completion is obtained and provided to the appropriate Information System Security Officer (ISSO) or Information System Security Manager (ISSM).

The DOT OST CIO's office documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. DOT Security Awareness Training is administered and maintained through DOT Learns online training system.

Responsible Official

Terry Brewster
Associate Director
Office of the Security

Approving Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2024.05.17 12:50:37 -04'00'