Privacy Impact Assessment

for the

Checkpoint Information Management Web Application

DHS Reference No. DHS/TSA/PIA-052

May 16, 2022

Homeland Security

Abstract

The Transportation Security Administration (TSA) performs a wide variety of transportation security functions, including, among others, the physical screening of transportation passengers and transportation sector workers. The traveling public often notices transportation security functions at TSA airport security checkpoints, but they also occur at other locations such as airport gates, airport worker sterile area access points, and national security events. Information regarding incidents that occur at locations where these transportation security functions are performed is typically collected on paper forms and then subsequently entered manually into various reporting systems. To promote efficiency and uniformity in the reporting of incidents, TSA has developed a web application accessible from TSA-issued devices, the Checkpoint Information Management (CIM) Web Application, to permit the electronic submission of incident reports. The application will standardize and automate incident reporting, promote timely and actionable sharing of information, and permit improved trend and pattern analysis for more effective implementation of transportation security measures. Although the intent is to standardize and automate incident reporting across the organization, TSA initially plans to test the Checkpoint Information Management application at a limited number of airports. This Privacy Impact Assessment (PIA) is conducted pursuant to the E-Government Act of 2002 because the application database collects personally identifiable information (PII) on members of the public.

Introduction

TSA is responsible for security in all modes of transportation.[1] Among its responsibilities, TSA provides for the screening of all passengers and property.[2] TSA also has broad authority to enforce its transportation security regulations and orders; receive, assess and distribute intelligence information related to transportation security; assess threats to transportation security; and serve as the primary liaison for transportation security to the intelligence and law enforcement communities.[3] TSA generates written reports on various incidents that occur in connection with these functions, including on such matters as the discovery of prohibited items or other occurrences of prohibited activity during the screening of persons and their property, incidents requiring law enforcement action, security breaches, accidents at the checkpoint, illnesses, and other incidents at airport gates and airport worker sterile area access points. Incident information is shared with TSA employees who have a need to know and is stored in a variety of TSA systems, including TSA Airport Information Management (AIM),[4] Performance and Results Information System

[1] The Aviation and Transportation Security Act (ATSA), 49 U.S.C. § 114 et. al.
[2] 49 U.S.C. § 44901.
[3] 49 U.S.C. § 114(f), (u).
[4] TSA Airport Information Management is a database used by TSA Security Operations to record data regarding checkpoint screening operations. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION

(PARIS),[5] Tactical Information Sharing System (TISS),[6] Web-Based Emergency Operations Center (WebEOC),[7] and Transportation Vetting System (TVS)[8] to assist with enforcement, intelligence, and data analytics, among others. For example, information concerning a prohibited item brought to the checkpoint, such as a firearm, is initially recorded on a paper incident form, then manually entered into the appropriate electronic database (e.g., Performance and Results Information System), and ultimately shared with authorized employees in the appropriate office for enforcement action against the individual.

In order to improve efficiency and uniformity of incident reporting, as well as promote timely and actionable sharing of information, TSA has developed the Checkpoint Information Management application to collect incident information electronically in near-real time. Although the Checkpoint Information Management will initially be used at select airport checkpoints, it can be implemented wherever TSA performs its transportation security functions. Use of the web application will permit the near instantaneous transmission of information to individuals who have responsibility for securing the transportation venue and responding to threats. Checkpoint Information Management will also reduce the potential for human data entry error by eliminating the manual entry of information on a paper form into various TSA electronic systems and permit more timely memorialization of incident facts in near real time for timely action on matters like security violations. It will also serve as an operational tool to improve data analytics by providing decision makers with information to conduct trend and pattern analyses.

SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR THE TSA ENTERPRISE PERFORMANCE MANAGEMENT PLATFORM, DHS/TSA/PIA-034, *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

[5] The Performance and Results Information System is a database used by TSA Security Operations to document violations of TSA security requirements and related investigative and enforcement measures. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR THE PERFORMANCE AND RESULTS INFORMATION SYSTEM, DHS/TSA/PIA-038, *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

[6] The Tactical Information Sharing System is a database used by the Federal Air Marshal Service to document and share information relating to suspicious incidents within the transportation domain. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR THE TACTICAL INFORMATION SHARING SYSTEM, DHS/TSA/PIA-015, *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

[7] The Web-Based Emergency Operations Center is a database used by TSA to record and track reportable incidents within the transportation domain. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR THE TSA OPERATIONS CENTER INCIDENT MANAGEMENT SYSTEM, DHS/TSA/PIA-029, *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

[8] The Transportation Vetting System is a database used by TSA Intelligence and Analysis to, among other uses, support investigations and eligibility determinations regarding certain transportation workers and other individuals vetted by TSA, as well as to record information relating to air travel by Known or Suspected Terrorists. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR THE TSA ENCOUNTER ANALYSIS BRANCH. DHS/TSA/PIA-039, *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

Authorized TSA employees will initially download the application onto a TSA-issued device, log in, and enter their location.[9] Once an incident occurs, an authorized employee will log into the device and generate an incident report. The authorized employee will enter the type of incident using the reporting options provided in the application. The application will provide prompts for common incident types and permits data entry. For example, for checkpoint incident reports, fields will be provided to input information regarding location, individuals involved in the incident, and whether notifications were made such as to law enforcement; discovery of prohibited items; a description of screening complaint, injuries, or claims of loss or damage to property; the reporting officer's summary; and relevant attachments.

After the report is entered, Checkpoint Information Management information is uploaded to an intermediate server and may be shared with authorized employees who have approved access to the Checkpoint Information Management system and a need to know the information. Once finalized, reports may be directed to different data systems depending on the type of incident selected in the Checkpoint Information Management application, or channeled by email to appropriate TSA stakeholders, such as Federal Air Marshals, TSA Security Operations, and TSA Intelligence & Analysis, for operational response and entry into appropriate TSA systems (Tactical Information Sharing System, Airport Information Management, Performance and Results Information System, or Web-Based Emergency Operations Center).

Data is not stored on the device except as it is temporarily present in device memory, i.e., Random Access Memory (RAM). As the authorized employee moves from page to page within the application, the data is transmitted to the Checkpoint Information Management server and is removed from device Random Access Memory. If the user wants to go back a page or query another report, then the data is pulled for only that page from the server to the user's device. If the user closes the application or the device times out, then the device management software implements an erase of the device Random Access Memory.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[10] articulates concepts of 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. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure

[9] Generally, the authorized employee will only initiate and submit incident reports at their own airport; however, under limited circumstances, employee-based roles could permit initiation and submission at other airports/locations. Employee-based roles and access is determined by the individual employee's job function, duties, role, and location. Personnel are only provisioned access after their need to know is determined.
[10] 5 U.S.C. § 552a.

that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[11]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[12] The Fair Information Practice Principles account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[13] and the Homeland Security Act of 2002, Section 222.[14] This Privacy Impact Assessment is conducted as it relates to the DHS construct of the Fair Information Practice Principles. This Privacy Impact Assessment examines the privacy impact of the Checkpoint Information Management application as it relates to the Fair Information Practice Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate.

The Checkpoint Information Management application collects information on individuals involved in incidents, such as individuals who were found to be carrying prohibited items or otherwise engaged in prohibited activity during the screening of persons and their property; incidents involving a law enforcement response; other reportable incidents (e.g., breaches, theft, injury); or to document the screening of persons designated for enhanced screening and their co-travelers. Generally, information collected on incidents at the checkpoint will be obtained directly from the passenger when possible. For other incidents during other transportation security functions or that require a law enforcement response, the passenger may not be directly involved in the collection of information that will be reported. This Privacy Impact Assessment serves to notify the public that the Checkpoint Information Management application may be used to generate and submit the reports that TSA generates associated with its security activities.

---

[11] 6 U.S.C. § 142(a)(2).
[12] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[13] 44 U.S.C. § 3501 note.
[14] 6 U.S.C. § 142.

Privacy Risk: There is a privacy risk that individuals will not know about the collection or use of their personally identifiable information.

Mitigation: The risk is partially mitigated. Most individuals involved in incidents are aware that they have been involved in an incident. Their participation in information collection is regularly required by TSA for reporting. For example, an individual reporting a theft at a checkpoint is aware that personally identifiable information is collected by TSA regarding the incident. There are some reports, however, that do not involve the individual in a manner that makes the collection of information apparent (e.g., persons may be aware that they received enhanced screening but not be aware that there is reporting associated with that screening). This Privacy Impact Assessment provides notice that such activities will result in reporting within TSA.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

TSA involves the individual when preparing most incident reports. Identity is verified against the individual's identification document, and photographs of the identification document and any prohibited item may be taken. Additional identifying information may be requested from the individual, such as their home address or identification document information (e.g., driver's license number, passport, military identification card). If the individual is reporting a theft or injury, then relevant information will be collected involving the individual's participation.

Individuals may request access to and correction of documents by submitting a request under the Privacy Act or Freedom of Information Act (FOIA) to the TSA Freedom of Information Act Office at the below address or https://www.dhs.gov/foia. Further information on how to submit a request can be found at www.tsa.gov/FOIA.

Freedom of Information Act Officer
Transportation Security Administration
TSA-20
6595 Springfield Center Drive, Springfield, VA 20598-6020

To a large extent, TSA will involve the individual in the collection of personally identifiable information and provides mechanisms for appropriate access, correction, and redress.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

The Checkpoint Information Management application provides an efficient, accurate, and more timely means of submitting incident reports to appropriate TSA personnel and systems. It also encourages greater uniformity in reporting. The information is used for operational response by Federal Air Marshals, TSA Security Operations, and TSA Intelligence & Analysis, as well as for enforcement of security regulations and statistical purposes under TSA legal authorities. The Checkpoint Information Management application provides a web application to accomplish existing paper-based processes and does not expand any uses of or access to information.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

The Checkpoint Information Management application is an electronic means of submitting incident reports. It includes prompts that are not changeable by the user for preparing standardized reports, which ensures that only relevant and necessary information is submitted. Data is stored only temporarily in the device's Random Access Memory while the report is uploaded to the Checkpoint Information Management server or, for reports involving individuals selected for enhanced screening, to the TSA Transportation Vetting System. The Checkpoint Information Management application does not collect any personally identifiable information beyond what is already legally collected through various TSA systems. Each system has its own approved data retention schedule listed in separate compliance documentation for that system.

Privacy Risk: There is a risk that more personally identifiable information will be collected than is relevant or necessary.

Mitigation: The risk is mitigated. The Checkpoint Information Management application uses prompts and defined fields to collect information and pre-populates any personally identifiable information fields, which reduces the risk that more personally identifiable information will be collected than is relevant or necessary. In addition, using pre-populated defined fields further reduces the risk from the current paper-based processes.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

The Checkpoint Information Management application is designed to only direct reports to the previously specified databases, thereby limiting the purpose for which the reports can be used to that which was intended by the system. Rules of behavior and approved access rights based on permission level ensures that any change to the dataflow will be reviewed to verify that the reports are utilized for authorized purposes. It does not share personally identifiable information outside of TSA.

Privacy Risk: There is a risk that personally identifiable information will be used for other purposes.

Mitigation: The risk is mitigated. Checkpoint Information Management is a web application designed to feed incidents to the data systems intended to receive the report. It integrates administrative, technical, and physical security controls that protect personally identifiable information against unauthorized use by defining the intended uses during the creation of the web application. Those controls include approved access rights based on permission level.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

The application is expected to improve upon current reporting by providing a more uniform and immediate means of submitting incident reports. It will also provide prompts for fields to be completed and will pre-populate certain passenger information; thus, helping reduce the potential for data entry or transcription error. Additionally, the Checkpoint Information Management application is designed to collect incident information in near-real time to improve accuracy, relevancy, timeliness, and completeness of the data.

Privacy Risk: There is a risk that inaccurate information will be collected.

Mitigation: The risk is mitigated. The Checkpoint Information Management application provides improved data quality and integrity by providing for more uniform and immediate reporting. Certain fields will be prepopulated with passenger data pulled from reservation information submitted by the individual to TSA. Other fields will utilize checkboxes and prompts to prepare reports on incidents. Electronic preparation and submission of reports will eliminate clerical errors that have occurred during the collection of information by hand and the transcription of paper-based reports to electronic records.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

The Checkpoint Information Management application is a secure application loaded onto secure TSA-issued devices (typically government-issued phones). Access to the device requires the user to select either a biometric sign-on or user Personal Identification Number (PIN).[15] The devices themselves will be issued to a limited number of supervisory personnel. A desktop application may also be developed, and access will be through DHS Personal Identity Verification (PIV)-card or username and password.

Data is not stored on the device except as it is temporarily present in device memory (i.e., Random Access Memory). As the user moves from page to page within the web application, the data is transmitted to the Checkpoint Information Management server and is removed from device Random Access Memory. If the user wants to go back a page or query another report, then the data is pulled for that page from the server to the user's device. If the user closes the application or the device times out, then the device management software implements an erase of the device Random Access Memory. Checkpoint Information Management is a secure web application available to authorized TSA users. The electronic device housing the Checkpoint Information Management application requires the user to use either biometric sign-on or a Personal Identification Number. A desktop application may also be developed, and access will be through Personal Identity Verification-card or username and password.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

TSA employees take annual privacy training developed by the DHS Privacy Office. In addition to administrative controls imposed by the operating protocols associated with existing incident reporting, the Checkpoint Information Management technical controls also enforce access controls and accountability. TSA employees are also provided with instructions, modules, and rules of behavior for the proper operation of Checkpoint Information Management prior to use.

[15] The Checkpoint Information Management application itself is not collecting biometrics. This security functionality is conducted through the TSA-issued device itself.

Conclusion

In order to improve efficiency and uniformity of existing incident reports, as well as promote the timely and actionable sharing of information, TSA has developed the Checkpoint Information Management application. The application will initially be piloted at TSA checkpoints, but it can be implemented wherever TSA performs its transportation security functions.

Contact Official

Joshua Alcorn, Ph.D.
Research and Capabilities Analysis/TSA
Josh.Alcorn@tsa.dhs.gov

Responsible Official

Peter Pietra
Privacy Officer
DHS/TSA

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717