Privacy Impact Assessment for the

TSA Operations Center Incident Management System

July 7, 2008

UContact Point
Jim Quinlan
Chief of Staff, Transportation Security Operations Center
(571)227-(b)(6)

Reviewing Officials
Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration
TSAPrivacy@dhs.gov

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov

Abstract

Under the Aviation and Transportation Security Act (ATSA), the Transportation Security Administration (TSA) has "responsibility for security in all modes of transportation."[1] TSA uses an operations center incident management system called WebEOC to perform incident management, coordination, and situation awareness functions for all modes of transportation. The system will store information that it receives about the following categories of individuals: 1) individuals who violate, or are suspected of violating transportation security laws, regulations, policies or procedures; 2) individuals whose behavior or suspicious activity resulted in referrals by Ticket Document Checkers (TDC) to Behavior Detection Officer (BDO) or Law Enforcement Officer (LEO) interview (primarily at airports); or 3) individuals whose identity must be verified, or checked against Federal watch lists. Individuals whose identity must be verified includes both those individuals who fail to show acceptable identification documents to compare to boarding documents and law enforcement officials seeking to fly armed. The system also collects and compiles reports from Federal, state, local, tribal, or private sector security officials related to incidents that may pose a threat to transportation or national security. Daily reports will be provided to executives at TSA and the Department of Homeland Security (DHS) to assist in incident and operational response management.

Overview

TSA has a statutory mandate to provide security in all modes of transportation. The Transportation Security Operations Center (TSOC) correlates and fuses real-time intelligence and operational information across all modes of transportation, and coordinates within DHS and with other Federal, state and local homeland security agencies for prevention of, and response to transportation-security related incidents. To assist in performing these functions, TSA uses a Commercial-Off-The-Shelf (COTS) web-based operations center incident management communications system that provides real-time information sharing by linking Federal, state, local, tribal, and worldwide sources. The system will store information that it receives about the following categories of individuals: 1) individuals who violate, or are suspected of violating transportation security regulations, policies or procedures; 2) individuals whose suspicious activity resulted in Behavior Detection Officer (BDO) or Law Enforcement Officer (LEO) interview; or 3) individuals whose identity must be verified, or checked against Federal watch lists. The system also collects and compiles reports from Federal, state, local, tribal, or private sector security officials related to incidents that may pose a threat to transportation or national security. The data received on a regular or recurring basis includes personally identifiable information (PII) more fully described in Section 1.1 such as name, home address, telephone number, date of birth, passport number, driver's license number, and data related to suspicious activity reports, of individuals who violate, or are suspected of violating TSA security regulations, policies or procedures. Some suspicious activity reports originate in reports from the public to transportation industry and government security hotlines such as those operated for General Aviation and commercial trucking sectors.

Reports are submitted to ascertain, as quickly as possible, the individual's identity, whether they are already the subject of a terrorist or criminal investigation, or to analyze suspicious behavior that may signal some form of pre-operational surveillance or activity, to provide an information source for

1.4 How is the information collected?

Information is collected directly from passengers by TSA employees or LEOs, and is relayed telephonically or electronically to the TSOC. In the future, it may be possible for TSA employees at airports or other locations to enter data directly into the system.

1.5 How will the information be checked for accuracy?

The information contained in the system will be provided by government or non-government sources. Information obtained from government entities will remain associated with the source government entity, which may be contacted by authorized law enforcement or government personnel accessing that information to verify its accuracy and update its status.

Information from non-government entities related to incidents or reports of suspicious activities will be entered into the system and will, generally, be concurrently referred to a law enforcement agency for investigation. Authorized users have the ability to add updated information, which will remain associated with the initially submitted information.

TSA expects that individuals whose identity is being verified will provide accurate information. TSA provides a form to individuals to assist with accurately transmitting the name and address of individuals who lack an acceptable identity document to perform the identity verification process. In addition, the process involves a certain amount of interaction between the individual and verifier that allows for accurate information transmission.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Homeland Security Presidential Directive (HSPD)-5 of February 28, 2003 requires all Federal departments and agencies to adopt National Incident Management System (NIMS) information sharing standards to effectively and efficiently prepare for, respond to, and recover from domestic incidents. This system assists in accomplishing this purpose.

Additionally, under the Aviation and Transportation Security Act, the TSA administrator is responsible for overseeing transportation security (P.L. 107-71) and has the authority to establish security procedures at airports (49 C.F.R. § 1540.107). TSA is responsible for providing for the screening of all passengers and property (49 U.S.C. § 44901). TSA has broad authority to 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 (49 U.S.C. § 114(f)).

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The privacy risk associated with the collection of this information is the possibility of inappropriate dissemination of personally identifiable information. In instances where personally identifiable information is relevant or necessary to be collected, it will be protected with additional safeguards, including masking, so that only those individuals with appropriate access and a need to know will be able to review the personally identifiable information collected. Privacy risks associated with the use of commercial databases are mitigated through verbal interaction with the passenger and by only using commercial data for the limited purpose of verifying identity. There is also a privacy risk associated with collecting information on individuals who may lack acceptable identification because it was lost or stolen and may not have involved wrong-doing on the individual's part. The privacy risk is mitigated by noting the circumstances of the failure to provide identification and the results of the verification process.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

The information collected enables the TSA to process and disseminate information related to transportation security incidents or individuals who violate, or are suspected of violating transportation security laws, regulations, policies or procedures; individuals whose suspicious activity resulted in BDO or LEO interview; or to verify an individual's identity in order to permit them access to the secure area. Information collected from individuals who fail to present acceptable identification matching boarding documents will be used to search databases, including commercial databases, in order to present knowledge based queries to verify the individual's identity. TSA will check immigration databases to assist foreign nationals in verifying identity. TSA may also perform other searches of publicly available data to assist in verifying identity. LEOs seeking to fly armed will be checked for proper authorization from their employing agency. The information is also used for TSA to provide an operational response. It allows users to draw links and patterns that might not otherwise be readily apparent. TSA uses the information to build the Common Operational Picture (COP). The COP is a merger of all relevant and available information associated with emerging events or incidents in a consolidated format to facilitate decision-makers. TSOC develops a daily report for senior TSA executives, Federal Security Directors (FSDs), and DHS Administrators.

2.2 What types of tools are used to analyze data and what type of data may be produced?

In the ordinary course of business, the system will be used to search for trends, patterns, or incident information to determine threats to transportation security. The system does not use algorithms to predict terrorist or criminal activity by individuals.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

This system uses publicly available data and media websites to obtain and assess information from relevant sources that could have an immediate impact on the security of the national transportation infrastructure. It may also use commercial data and publicly available data to assist in verifying individual identity. TSA will use a variety of means to verify the identity of the individual, including asking knowledge based questions based on information in commercial databases (for example, date of birth, residence, etc) and publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

In instances where collection of personal information is necessary, it may only be viewed by appropriate personnel with the correct user roles and need to know. This ensures that privacy and information safeguarding requirements are met by limiting access to sensitive information, such as personal information, only to those users whose operational role and mission warrants such access. The privacy information within the system is further protected by the use of identification and authentication controls, access control lists, and physical access control to the application and database servers.

Section 3.0 Retention

3.1 What information is retained?

TSA will retain transportation security incident information, including, where collected, information about individuals who violate, or are suspected of violating transportation security laws, regulations, policies or procedures; information about individuals whose suspicious activity results in BDO or LEO interview; or information about individuals whose identity must be verified or checked. Such information may include the full names of individuals, aliases and nicknames, date of birth, place of birth, age, sex, race, nationality, languages spoken, passport number, driver's license number, and telephone number, home and business addresses; Social Security Numbers, height and weight, eye color, hair color, style and length, facial hair, scars, tattoos and piercings, clothing (including colors and patterns) and eyewear, description of personal carry-on and/or baggage items,

3.2 How long is information retained?

Most information in the Web EOC system will be retained for three years. The hard copy form used to collect name and address to verify the identity of individuals who do not bring identification to the TSA screening checkpoint at an airport will be retained for 30 days, unless enforcement action or litigation results, in which case the information will be retained in accordance with the appropriate NARA-approved records retention schedule.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. In the ordinary course, the information falls within TSA's Aviation Security records retention schedule.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Given the incident management, coordination, situational awareness, investigation, and operational response functions of the system, the NARA-approved retention period is reasonable.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

The information may be shared with DHS employees and contractors who have a need for the information in the performance of their duties. It is expected that information typically will be shared with TSA employees or contractors in the following TSA offices: Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS), Office of Chief Counsel, Office of Transportation Threat Assessment and Credentialing (TTAC), Office of Security Operations, Transportation Sector Network Management Office (TSNM), Office of Inspection, and all those agency components whose legitimate law enforcement or governmental terrorism-related missions require access to the information. While it is not routinely shared outside of TSA, TSA may need to share information within DHS, specifically with U.S. Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE).

In order to respond to complaints from individuals, the information may also be shared with the Office of Privacy Policy and Compliance, the Ombudsman, or the Office of Civil Rights and Civil Liberties. To respond to congressional inquiries, the information may be shared with the Office of Chief Counsel and the Office of Legislative Affairs. Where access to sensitive information, such as personal information, is determined to be necessary, access will be based on a need to know. All information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a.

Access to personally identifiable information is only provided to system users that have the appropriate clearance and a need to know in the performance of official duties.

The TSOC will provide recipients of the daily report, such as TSA and DHS senior administrators and policy-makers, a bulk snapshot of the previous day's incidents which provides a real-time situational awareness picture to facilitate incident management.

4.2 How is the information transmitted or disclosed?

System users are able to query the daily reports directly over a secure network. In the case of briefings provided to senior management, the reports can either be passed as an encrypted file or hand delivered in the form of encrypted magnetic media or hard-copy printed reports.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The privacy risk associated with sharing this information is the opportunity for improper dissemination of personally identifiable information to individuals who do not have authority to receive or access the information. To mitigate this risk, TSA will only share this information with TSA and DHS employees and contractors who are authorized access and have a need for the information to perform their official duties in accordance with the Privacy Act. Employees authorized to access the data receive appropriate privacy and security training and have necessary background investigations and security clearances for access to sensitive or classified information. Privacy protections include strict access controls, including security credentials, passwords, real-time auditing that tracks access to electronic information, and mandated training for all employees and contractors.

Section 5.0 External Sharing and Disclosure

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Because the purpose of the system is to increase information sharing for homeland security purposes, users may be government officials, law enforcement personnel, non-government organizations, and private sector individuals whose professional duties and interests make them stakeholders of the DHS mission. System users will be provided access only to information that is relevant to their official duties.

All information that is relevant to a system user will be made available to the particular user, but PII is provided only in instances where the user has the appropriate clearance and need to know. For example, transportation security alerts, trend analyses, and many incident summaries likely would not contain PII or the PII would be masked.

TSA may also share information with Federal, state, or local law enforcement or intelligence agencies or other organizations in accordance with the Privacy Act and the routine uses identified in the applicable Privacy Act system of records notice (SORNs).

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes. The information is shared in accordance with Privacy Act system of records notice (SORNs) DHS/TSA 001, Transportation Security Enforcement Record System (TSERS), primarily routine uses 1, 2, 3, 7, 8, and 16, DHS/TSA 002, Transportation Security Threat Assessment System, primarily routine uses 1, 2, 3, 7, and 9, and DHS/TSA 011, Transportation Security Intelligence Service (TSIS) Operational Files, primarily routine uses 1, 5, 9, 12, 15, 16, and 17.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Users are able to query the system directly over a secure network. System users are required to read and acknowledge the rules of behavior of the tool, policies associated with their organization, and the laws and policies of the jurisdictions in which they operate prior to accessing the system. For members of the National Capital Region Coordination Center (NCRCC), the NCRCC management has established an MOU with component members. This MOU grants NCRCC members' access to both the TSA Network and subsequently to system.

In order to access the system, users outside of the TSA Network must use a secure socket layer connection to the extranet server. Information is shared outside the Department in accordance with the applicable Privacy Act routine uses. In addition, Federal agencies and their contractors are subject to information security requirements of the Federal Information Security Management Act (FISMA), Title III of the E-Government Act, Pub. L. 107-347.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

The privacy risks associated with the sharing of this information is the possible dissemination of personally identifiable information to unauthorized external entities. This risk is mitigated by TSA limiting the sharing of this information to those who have an official need to know it and by sharing only in accordance with published routine uses or under the Privacy Act. Categorizing the information when it is included in the system, in coordination with enforced role and rule-based access, minimizes the number of people with access to personally identifiable information. TSA is further mitigating these risks by disseminating this information by incident number or date, therefore eliminating personal identifiers from the subject.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information?

In instances where personal information is collected in order to verify identity, the individual is provided an 5 U.S.C. 552(e)(3) notice prior to the collection of information. Where PII is collected as part of a criminal investigation, TSA will not provide notice and has previously published a Final Rule after public comment to exempt TSA from the notice requirement in such circumstances. In instances where TSA receives personal information as part of suspicious activity reports, the individual is unlikely to have knowledge that his/her information has been submitted to the system and there is no opportunity for TSA to provide notice. The following SORNs provide notice to the individual where TSA collects information associated with transportation security incidents: DHS/TSA 001, Transportation Security Enforcement Record System (TSERS), DHS/TSA 002, Transportation Security Threat Assessment System, and DHS/TSA 011, Transportation Security Intelligence Service (TSIS) Operational Files.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

In some instances, an individual has the right to decline providing personally identifiable information. By way of example, individuals whose identity TSA must verify may decline to provide the information; however, failure to furnish the requested information may result in an inability to grant the individuals access beyond the TSA screening checkpoint. For personal information that may be associated with suspicious activity reports, there is no opportunity to decline to provide information.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

In instances where personal information is collected in order to verify identity, the individual is provided an 5 U.S.C. 552(e)(3) notice prior to the collection of information. Individuals will be aware of the collection of information, even without notice, in all cases except suspicious activity reports in which there is no opportunity to provide notice.

Section 7.0 Access, Redress and Correction

7.1 What are the procedures that allow individuals to gain access to their information?

For individuals seeking access to their information in the system, such persons may request access to their information by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request to TSA in writing by mail to the following address:

Transportation Security Administration, TSA-20, East Tower
FOIA Division
601 South 12th Street
Arlington, VA 22202-4220

FOIA/PA requests may also be submitted by fax at 571-227-1406 or by filling out the Customer Service Form (URL: Thttp://www.tsa.gov/public/contactus). The FOIA/PA request must contain the following information: Full Name, address and telephone number, and email address (optional). Please refer to the TSA FOIA web site (http://www.tsa.gov/public). In addition, individuals may amend their records through the redress process as explained in paragraph 7.2 below.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Individuals can submit a request to correct records under the Privacy Act.

7.3 How are individuals notified of the procedures for correcting their information?

Although individuals likely will not know the system contains information on them in light of the investigative nature and sensitivity of the information, the TSA FOIA page, accessible through the TSA public website, contains a link permitting any individual to send information to TSA via a designated email address reserved for that purpose. The FOIA page also contains a fax number and a mailing address for the same purposes for those who prefer to use those means to contact TSA. All communications received, regardless of method, will be entered into and remain on record within the system pursuant to its NARA-approved record retention schedule and will be subject to audit.

7.4 If no formal redress is provided, what alternatives are available to the individual?

The development of the system and the processes governing its use included detailed consideration of the impact of erroneous data on individuals as well as on the official users of the information within the system. Having verified and accurate information is the ultimate goal of all of the law enforcement, intelligence community, and other governmental officials using the system. The redress procedure indicated in 7.2, above, will help to ensure that the information is accurate. TSA will ensure the integrity

of the system information based upon information provided by individuals, as well as any updates received from law enforcement and other government authorities.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

If an individual believes that he or she has suffered an adverse consequence related to the system, that individual will be able to provide any information that they deem relevant with a request that it be included within any record maintained in the system regarding a particular incident, activity, transaction, or occurrence. TSA will ensure the integrity of the system information based upon information provided by individuals, as well as any updates received from law enforcement and other government authorities.

Section 8.0 Technical Access and Security

8.1 What procedures are in place to determine which users may access the system and are they documented?

Procedures to determine which users may access the WebEOC system are documented in the System Security Plan. Users are granted access by the TSOC Director or the Watch Floor Director. An access control list of users is maintained in system and a list of all users with access to the system is kept separately for auditing purposes.

Users must register to verify registrant eligibility for specific communication tools and collaboration spaces within the system. The system access control is role-based. Controls and access limitations are in place to ensure that sensitive information is protected from unauthorized access or exchange. Additional controls may be established to further define access to emergent, incident, and event-based information as required. In all cases access will be in accordance with applicable law and TSA policy.

Certain TSA staff, including watch and technical support personnel, will have access to all system communication and collaboration tools. Staff communicates and collaborates with other system users and receives, research, and responds to requests for information regarding terrorism-related suspicious activities. IT specialists and technical and operational program managers will access the system to ensure system performance and to audit the use of the system. Analysts throughout law enforcement, government, and in some cases private sector security management may have access to the activity-based informational areas of the system. All of these analyst users and other registered users, whose identity and need for access have been validated, will have varying levels of access to the system.

Physical and procedural safeguards are also employed to protect the hard copy form used to collect information to verify the identity of individuals who do not bring identification to the TSA screening checkpoint.

8.2 Will Department contractors have access to the system?

Yes. Currently there are several technology contractors who have access to the system as they build the information network and the database. Such contractors or other IT professionals will be registered and managed using the same auditing and controls as every other system user. Strict adherence to access control policies is automatically enforced by the system in coordination with and through oversight by TSA IT Security Officers. All contractors performing this work are subject to requirements for suitability and a background investigation as required by TSA Management Directive 1400.3, TSA Information Security Policy.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All TSA and assigned contractor staff receive TSA-mandated privacy training on the use and disclosure of personal data. Compliance with this training requirement is audited monthly by the TSA Privacy Officer, and failure to complete the training is reported to program management for remedial action. CDROM-based training modules are provided for stakeholders that do not have access to TSA Network Resources. Additionally, all staff must hold appropriate credentials for physical access to the sites housing the security threat assessment databases and management applications. In addition, all government and contractor personnel must complete annual information technology security training as required by FISMA. The business rules associated with the protection of the information, and the basis for those rules will be a component of all computer based training modules associated with the system.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes. Certification and Accreditation was completed and the Authority to Operate was granted on April 30, 2006.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Role-Based Access Safeguards. The system technology will safeguard information by limiting a user's ability to view or update particular fields of information based upon the user's role.

Auditing Measures. Whenever data is entered, updated, or viewed a record of that activity is captured and maintained within the system and can be retrieved based upon the user or the record.

Compliance will also be ensured through adherence to all FISMA required documentation to include National Institute of Standards and Technology (NIST) risk management methodology. Creation and maintenance of all required security documentation will ensure there is an IT security risk management program in place. Security documentation includes, but are not limited to, System Security Plan (NIST publication 800-18), Risk Assessment (NIST publication 800-30), Federal Information Processing Standard

(FIPS) number 199, Data Categorization, Self-Assessment (NIST publication 800-26) and other pertinent System Development Life Cycle (SDLC) artifacts.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The privacy risk associated with access and security controls is the unauthorized or inappropriate access of data in the system or access to the facility. The data in the system is secured in accordance with applicable Federal standards. Security controls are in place to protect the confidentiality, availability, and integrity of personal data, including role-based access controls that enforce a strict need to know policy. Physical access to the system is strictly controlled with the use of proximity badges. The system is housed in a controlled computer center within a secure facility. In addition, administrative controls, such as periodic monitoring of logs and accounts, help to prevent and/or discover unauthorized access. Audit trails are maintained and monitored to track user access and unauthorized access attempts. The protection of data contemplated under this assessment will be governed by the applicable System Security Plan for this system.

Section 9.0 Technology

9.1 What type of project is the program or system?

The WebEOC system is a commercial off-the-shelf major application which has been purchased and adapted for use by TSA to develop a database which will allow for prevention, mitigation, response or recovery activities in response to an actual or possible security event. It was purchased by TSA and installed and maintained by TSA contractors at an off-site hosting center.

9.2 What stage of development is the system in and what project development lifecycle was used?

The system is currently in the operation and maintenance phase of the systems development lifecycle. The project used for development and implementation of system was the TSA systems development lifecycle model.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No. The system does not employ additional technology that may raise privacy concerns. It serves only as an information sharing platform for incident reports from transportation security stakeholders. In order to support privacy protections, TSA has developed an information technology infrastructure that will protect against inadvertent use of PII not required by the government. Access to this information is limited

to those individuals authorized to have access based on their role. TSA has implemented procedures to ensure appropriate system accesses are revoked for employees, contractors, or other users when notified that they no longer have a need for using the tool.

Approval Signature

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Homeland Security

DHS Joint RequirementsCouncil
Information Sharing Portfolio Team (ISPT)
TSA COP/CIP Requirements Workshop Agenda
November 2, 2015, 1:00 pm - 5:00 pm
Meeting Location: 601 12th Street South, Arlington, VA

TSA HQE 6th Floor SCIF

Time	*Topic*	*Notes*
1:00 pm	Greetings/Introductions/Objectives	TSA – George Petersen
1:05 pm	TSA Capabilities Brief **(classification: TS/SCI)**	TSA – Mike Henderson

TSA HQE1-001S

Time	*Topic*	*Notes*
2:00 pm	Greetings/Introductions/Objectives	TSA – George Petersen
2:05 pm	DHS Unity of Effort Overview - COP/CIP Demo - Role of the JRC - TSA IBSV Related Activities - ISPT Related Activities o Resource Planning Guide o Capability Analysis Report - DHS Data Framework	DHS CIO – David Lilley TSA IBSV – George Petersen ISPT – Dr. Ken Clark ISPT – Dominic Bodoh, Carlos Lizardi DF PMO – Paul Reynolds /Lori Vislocky
3:35 pm	Facillitated Requirements Breakout Session	DHS S&T – Kevin Roney TSA MAPI
5:00 pm	Conclusion	TSA – George Petersen

Privacy Impact Assessment Update for the

TSA Operations Center Incident Management System

DHS/TSA/PIA-029(a)

August 25, 2015

Contact Point
John Bogers
System Owner
Transportation Security Operations Center
Transportation Security Administration
TSA-ocims@tsa.dhs.gov

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343- (b)(6)

Abstract

The Transportation Security Administration (TSA) Transportation Security Operations Center (TSOC) serves as TSA's coordination center for transportation security incidents and operations. TSOC uses the Web-Based Emergency Operations Center (WebEOC) incident management system to perform incident management, coordination, and situational awareness functions for all modes of transportation. The system maintains information including personally identifiable information (PII) in connection with its operations. The system also collects and compiles reports from federal, state, local, tribal, foreign, and international sources and private sector security officials on incidents related to threats to transportation or national security. TSA is updating this Privacy Impact Assessment (PIA), last published on July 12, 2010, to reflect that the system receives information about individuals on watchlists and their co-travelers; logs Amber Alerts[1] and disseminates them to the field; collects open-source information relating to transportation security or operations matters; and collects PII related to other incidents reported to TSA including significant public health-related risks to the traveling public and certain TSA employee information.

Overview

TSA has broad authority to 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.[2] The Transportation Security Operations Center (TSOC) correlates and fuses real-time intelligence and operational information across all modes of transportation, and coordinates within DHS and with other federal, state, and local homeland security agencies for prevention of, and response to, transportation security-related incidents. TSA uses the Web-Based Emergency Operations Center (WebEOC) to store real-time information from federal, state, local, tribal, foreign, and international sources and private sector security officials to assist in performing transportation security functions. WebEOC stores information on individuals and witnesses involved in security incidents including: 1) individuals who violate or are suspected of violating transportation security laws, regulations, policies, or procedures; 2) individuals whose behavior or suspicious activity results in referrals to a Behavior Detection Officer or Law Enforcement Officer; and 3) individuals whose identity must be verified or checked against federal watch lists, including individuals who fail to show acceptable identification documents to compare to boarding documents and law enforcement officials who seek to fly armed.

---

[1] The AMBER Alert™ Program is a voluntary partnership between law-enforcement agencies, broadcasters, transportation agencies, and the wireless industry, to activate an urgent bulletin in the most serious child-abduction cases.

[2] 49 U.S.C. §114(f).

Reason for the PIA Update

TSA is updating this PIA, last published July 12, 2010, to reflect that TSA's Secure Flight System sends information to WebEOC regarding individuals who are a match to the Terrorist Screening Center's Terrorist Screening Database (TSDB) and their co-travelers, individuals on the Center for Disease Control's (CDC) Do Not Board list, and individuals who appear to be using lost or stolen travel documents for air travel. WebEOC stores information on known or suspected terrorists (KST) for TSA operational purposes including notifying field personnel of expected travel, and logs Amber Alerts to track the status of alerts issued to the field. WebEOC stores PII related to other matters reported to TSA, such as significant public health-related events posing risks to the traveling public.

WebEOC stores open-source information[3] related to transportation security matters for enhancing situational awareness and operational purposes. TSA monitors public open-source information, including social media, to gain situational awareness on events impacting transportation security or operations. It may use the information to assist in assessing threats and planning or managing an operational response. For example, a social media posting regarding the location a tornado touched down may assist with assessing impacts to transportation facilities or to the TSA workforce. Searches are performed based on keywords and concepts in reporting guidance that has been reviewed for privacy and civil liberties concerns. Search terms may be modified on occasion to reflect emerging or temporary threats.

WebEOC also stores TSA employee and contractor PII associated with such matters as medical evacuations, workplace violence, controlled property such as lost badges, continuity of operations (COOP) activities and exercises, and national or local emergencies.

PII is stored in separate modules within WebEOC based upon the type of information. For example, TSA employee PII may be stored in COOP, Critical Incident Management, or Federal Security Director Local Log modules; open-source information is stored in the Transportation Suspicious Incident Reports module. Access to each module is restricted at the user level to individuals with a need to know the information in the performance of their duties.

Privacy Impact Analysis

Authorities and Other Requirements

No changes.

---

[3] Open source information refers to a broad array of information and sources that are generally available, including information obtained from the Internet and media (e.g., newspapers, social media sites, radio, television), professional and academic records (e.g., papers, conferences, professional associations), and public data (e.g., government reports, public records, demographics, hearings, speeches).

Characterization of the Information

In addition to the information previously identified in prior PIAs, WebEOC collects and stores Secure Flight Passenger Data (SFPD)[4] regarding individuals who are a match to the TSDB and their co-travelers, individuals on the CDC's Do Not Board list, individuals who appear to be using lost or stolen travel documents for air travel[5], KST information, and PII related to matters reported to TSA, including significant public health-related risks to the traveling public.

To enhance situational awareness, assess threats, and assist with planning or managing an operational response, TSA may collect open-source information related to transportation security matters. Open-source information may include publicly available information or postings on social media sites regarding threats to transportation or national security, or simply matters potentially impacting TSA operations. Social media may also be a source of initial notification for transportation security or operations events. Open-source collection is accomplished through the use of search terms that have been reviewed for privacy and civil liberties impacts. TSA respects individual privacy settings when conducting open-source collection. Open-source information is assessed or corroborated prior to operational response.

Finally, WebEOC stores PII of TSA personnel reported to TSOC, such as medical evacuations, internal investigations, workplace violence, and lost badges. WebEOC will also store work status and contact information reported to TSOC by employees and managers during continuity of operations (COOP) activities, exercises, and national or local emergencies.

Privacy Risk: There is a risk of over-collection associated with the expansion of information collected by the system, including over-collection of open source information.

Mitigation: The risk is mitigated by only collecting information related to the TSOC mission as the coordination center for transportation security incidents and operations. Much of the information is already collected by TSA elsewhere and does not represent an expansion so much as centralizing existing information for coordination purposes. Open source information, including information collected from social media, is limited to transportation mission-related information that is available to the general public.

---

[4] SFPD consists of name, gender, date of birth, passport information (if available), redress number (if available), Known Traveler Number (if available), reservation control number, record sequence number, record type, passenger update indicator, traveler reference number, and itinerary information. For more information on the Secure Flight program and SFPD, see DHS/TSA/PIA-018 Secure Flight Program and its associated updates, available at www.dhs.gov/privacy.

[5] TSA checks passenger reservation data including passport information against watch lists of lost and stolen travel documents, including international passports. For additional information, please see DHS/TSA/PIA-018(g) Secure Flight Program PIA (December 8, 2014), available at www.dhs.gov/privacy.

Uses of the Information

The information collected within WebEOC continues to be used for incident management, coordination, and situational awareness purposes. WebEOC will store TSA employee and contractor information to manage certain internal operations, such as medical evacuation, workplace violence, and lost badge reporting. TSA will also use the collected employee and contractor information for COOP activities and exercises and national or local emergencies.

Privacy Risk: There is a privacy risk of inappropriate use of the additional employee and contractor information to WebEOC storage.

Mitigation: The risk is mitigated by integrating administrative, technical, and physical security controls that protect PII against unauthorized disclosure. System users and managers receive privacy training. For log entries, incidents or reports are entered in real-time and the latest entry updates the entry.

Notice

Airline passengers receive notice that their information is submitted to TSA through Secure Flight; accordingly KST, co-traveler, CDC Do Not Board, public health threat, and individuals using lost/stolen travel documents receive notice.

TSA does not provide notice to individuals on the Amber Alert list, or to individuals identified in open-source information, except to the extent this PIA acts as notice.

Privacy Risk: There is a privacy risk that individuals who post PII on open source venues will not receive notice that TSA may collect their information.

Mitigation: The risk is mitigated by the fact that the information is taken from open sources that are available to the general public and typically posted by the individual. TSA respects privacy settings and only collects information that is available to the general public. PII is stripped from open-source reporting when it is not relevant to the event. For example, a social media posting that there is a fight on a plane does not require the PII of the individual poster. Information learned from open-sources is corroborated or evaluated for credibility prior to operational response.

Data Retention by the Project

TSA updated its retention schedule for WebEOC records from three years to ten years. TSA extended the retention period for these records to facilitate the review of incidents for trends over an extended time period. Maintaining information beyond three years also permits TSA to conduct queries to identify repeat offenders related to transportation or national security incidents.

Information Sharing

TSA shares information with CBP regarding individuals who are a match or a potential match to the TSDB and their co-travelers, individuals on the CDC Do Not Board list, individuals who appear to be using lost or stolen travel documents for air travel, and on significant public health-related matters or risks to the traveling public.

There are no new privacy risks as a result of this update. Expanding the categories of information shared with CBP does not create a new privacy risk because the types of information are similar to those previously shared.

Redress

No changes.

Auditing and Accountability

No changes.

Responsible Official

John Bogers
System Owner
Transportation Security Operations Center
Transportation Security Administration

Approval Signature

Original signed PIA on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

Public Affairs Guidance

Visible Intermodal Prevention and Response (VIPR)

LAST MODIFIED

11.02.15

GUIDANCE

- Reactive
- Media inquiries should be coordinated with the Office of Public Affairs

PRODUCTS

- Background
- Talking Points
- Q&As

BACKGROUND

Under the *Aviation and Transportation Security Act* (ATSA) and the *Implementing Recommendations of the 9/11 Commission Act of 2007*, TSA has broad responsibility to enhance security in all modes of transportation nationwide. TSA's Visible Intermodal Prevention and Response (VIPR) teams are part of a nationwide transportation security program that serves all modes of transportation.

Following the Madrid train bombing, TSA developed the VIPR program to allow TSA security and law enforcement assets to augment federal, state, and local law enforcement and security agencies in the transportation domain.

TSA's VIPR teams provide a full range of law enforcement and security capability; the exact makeup of VIPR teams is determined jointly with local authorities but can include federal air marshals (FAMs), transportation security officers (TSOs), TSA certified explosive detection canine teams, TSA transportation security inspectors, explosives operational support, security and explosive screening technology, and local law enforcement officers.

TSA VIPR teams can be deployed at random locations and times in cooperation with local authorities to deter and defeat terrorist and organized criminal activity; or teams may be deployed to provide additional law enforcement or security presence during specific alert periods or special events. TSA routinely conducts thousands of VIPR operations each year in transportation systems nationwide.

Experience shows that regional planning and implementation provide the greatest security impact by aligning the frequency of deployments with risk reduction benefits for specific locations. VIPR teams work with local security and law enforcement officials to supplement existing security resources; provide a deterrent presence and detection capabilities; and introduce an element of unpredictability to disrupt potential terrorist planning or operational activities.

TALKING POINTS

- TSA's VIPR teams are specifically authorized by the *Implementing Recommendations of the 9/11 Commission Act of 2007* to "augment the security of any mode of transportation at any location within the United States."
- TSA's VIPR teams conduct operations that promote confidence in and protect all modes of transportation to detect, deter, and defeat terrorist activity.
- TSA has conducted thousands of Visible Intermodal Prevention and Response, or VIPR operations, since 2005. These partnerships with local authorities support mass transit security through unpredictable VIPR team deployments – serving as visible deterrents to mitigate evolving threats.
- The TSA has broad responsibility to ensure the safety and security of the traveling public in all modes of transportation. At the request of our federal, state, local, or industry stakeholders, TSA can tailor a VIPR team to meet the specific goals of any law enforcement or security operation in our Nation's transportation domain. (*Aviation and Transportation Security Act* (ATSA)
- VIPR teams can be composed of a variety of TSA, federal, state, and local law enforcement and security assets including: federal air marshals, TSA certified explosive detection canine teams, transportation security officers, behavior detection officers, TSA transportation security inspectors, local law enforcement officers and security technology.
- Specifically, these teams can be deployed, at the request of a stakeholder, to augment existing law enforcement and security resources. The combined resources of our stakeholders and TSA assets ensures the teams can be rapidly deployed, during periods of heightened alert or following an incident that impacts our Nation's transportation systems.
- TSA VIPR teams are specifically authorized by the Implementing Recommendations of the 9/11 Commission Act of 2007 to "augment the security of any mode of transportation at any location within the United States." In order to fulfill this mission, TSA creates relationships with our various stakeholders and coordinates joint operations, promoting communication and teamwork throughout all levels of government to ensure the safety of the traveling public.
- These VIPR teams were first implemented in 2005 and TSA has conducted thousands of VIPR operations – serving as visible deterrents to mitigate evolving threats.
- What is important to remember: In the wake of the tragic events of 9/11, your federal, state, and local governmental agencies have been committed to developing partnerships and increasing interagency communications to ensure the safety of our Nation's transportation systems. TSA VIPR teams provide the mechanism through which our law enforcement and security stakeholders can establish solid working relationships to protect you today, as well as in the event of a catastrophic event.
- VIPR teams provide additional detection and response capabilities, and expand the unpredictability of security measures to deter and disrupt potential terrorist activity.
- TSA's VIPR teams can be deployed to augment existing law enforcement and security resources during public events that have the potential to draw large crowds into the transportation domain.
- VIPR teams can be rapidly deployed, in coordination with state and local law enforcement and security officials, to enhance local law enforcement or security efforts during periods of heightened alert or following an incident that impacts our Nation's transportation systems.

- TSA VIPR operations are conducted in partnership with law enforcement and security authorities in all modes of transportation, including: Commercial Aviation, Air Cargo, General Aviation, Mass Transit, Maritime, Freight Rail, Highway Infrastructure, and Pipeline.
- There is no credible information to suggest a specific threat at this time.

QUESTIONS and ANSWERS

Q. **Why are Federal Air Marshals involved in an effort outside of aviation?**

A. The Federal Air Marshal Service is the law enforcement arm of TSA. In this role, they have jurisdiction in all modes of transportation. Legal authority in this effort is stipulated in the Aviation and Transportation Security Act [49 U.S.C. § 114(p)]. In the wake of the 9/11 attacks, and in response to the terrorist attacks experienced in London and Madrid, federal, state, tribal, and local law enforcement, and industry security partners throughout the United States have committed to an increased presence throughout mass transit systems. Federal Air Marshals are integral to augmenting these ongoing terrorism detection, deterrence, and response efforts.

Q. **What is TSA/DHS's authority to conduct VIPR operations?**

A. TSA's VIPR program is part of the broad responsibility that Congress gave to TSA in the *Aviation and Transportation Security Act* (P.L. 107-71) to protect all modes of transportation. More recently, in the *Implementing Recommendations of the 9/11 Commission Act of 2007* (P.L. 110-53) at section 1303, Congress explicitly authorized the VIPR program. At the request of our stakeholders, TSA coordinates the deployment of teams to augment security of any mode of transportation within the United States.

Q. **Will VIPR team assets be reporting to local law enforcement?**

A. VIPR teams are deployed in coordination with local law enforcement to perform specific counter terrorism operations. All assets assigned to the VIPR team will conduct security and law enforcement operations in accordance with a pre-approved and agreed upon operation plan.

Q. **Why is TSA deploying these teams now? Is there a specific threat?**

A. TSA VIPR teams have been working with our stakeholders since 2005. These teams provide a mechanism for all stakeholders responsible for law enforcement and security of our Nation's transportation systems. We have conducted thousands of operations in coordination with our stakeholders and continue to ensure communication and operational capabilities designed to protect the traveling public are enhanced. There is no credible information to suggest a specific threat at this time. TSA VIPR teams deploy at the request of our stakeholders thousands of times each year both randomly, to create a random deterrent to terrorism and organized criminal activity, and for special events and holidays that involve a large number of people using transportation systems.

Q. **Has TSA done this in the past?**

A. TSA VIPR teams are routinely deployed nationwide in coordination with our law enforcement, security, and industry partners to ensure the safety and security of the traveling public. Thousands of VIPR operations are conducted annually. TSA began the VIPR program in 2005.

Q. **What will VIPR teams do?**

A. VIPR teams will work with local law enforcement to provide a visible deterrent in aviation and mass-transit systems. The teams will have a wide range of law enforcement and security capabilities including behavior observation, security screening and explosives detection in addition to traditional law enforcement abilities. The composition of the teams varies based on the request of our partners and the environment in which they are deployed.

Q. **How many personnel will be involved?**

A. The VIPR team program is designed to enable team size and composition to vary and be tailored to the specific mission. The teams generally can consist of local law enforcement officers, federal air marshals, canine teams, transportation security inspectors, transportation security officers, and other local and/or TSA assets as deemed appropriate for the mission.

Q. How many teams are there?

Currently, there are 31 dedicated, TSA VIPR teams operating in conjunction with our federal, state, and local law enforcement stakeholders. Due to a Congressional enhancement to the program,

Q. How much funding does the program?

Congress has allotted 57 million to the VIPR program in order to enhance the security posture of our Nation in all modes of transportation.

Q. In response to a VIPR Operation at a trucking weigh stations in conjunction with Tennessee authorities, the American Trucking Associations stated : "Adding security personnel at weigh stations in unfamiliar federal uniforms is not likely to raise the comfort level of commercial drivers entering weigh stations, unless there is a threat to the highway sector. It doesn't seem like the best use of TSA resources unless there is information or intelligence that supports increased highway security." What is TSA's response?

Each VIPR operation is planned and carried out at the request of and with stakeholder involvement from planning through deployment. Operations are conducted in conjunction with federal, state, local, tribal and industry partners who have primary jurisdiction for the area of responsibility.

We are there to augment the law enforcement and security efforts. VIPR operations are a way to establish and maintain professional working relationships with stakeholders to carry out the transportation security goals of both our partners and TSA. It is absolutely essential in today's world that we have those relationships forged in advance of a real world event occurring. It is this type of VIPR operation that enables TSA to leverage resources quickly to be able to rapidly respond in the event those resources are needed.

What is important to acknowledge is that during the Tennessee Highway VIPR operation, we deployed law enforcement assets to augment the uniformed presence at the weigh station, at the request of the stakeholder. The transportation security officers that were seen at the weigh station were handing out flyers and informing the commercial vehicle operators of TSA's First Observer program. This program is exclusively for our Nation's commercial vehicle operators, providing the industry with training on effectively observing, assessing and reporting suspicious individuals, vehicles, packages and objects. This operation allowed our employees to interact with the industry on an individual basis, which is the best method of communicating our common goals in maintaining safe and secure transportation system.

Q. Have any VIPR surface transportation operations ever directly resulted in the arrest of any suspected attackers? If so, how many? Have VIPR surface transport operations ever discovered any explosives during searches of passenger baggage? If so, how many instances?

The mission of VIPR is deterrence and prevention of terrorism. Specific operational results are considered security sensitive information. Although the value of deterrence is difficult to measure directly the presence of law enforcement transportation security personnel VIPR assets increases the difficulty with which potential terrorists plan and conduct terrorist activity.

Q. The National Association of Railroad Passengers says TSA should be more mindful that train stations are not airports and they should be treated differently by security personnel. NARP says that for more than a century train stations have acted as more of a community hub than airports. The TSA, NARP says, should be more sensitive to the differences when it comes to these search operations. What is the TSA's or VIPR's response?

TSA's VIPR teams are tailored to meet the specific goals of any law enforcement or security operation in our Nation's transportation domain. VIPR teams can be composed of a variety of TSA, federal, state, and local law enforcement and security assets. TSA deploys VIPR teams to provide additional detection and response capabilities, and expand the unpredictability of security measures to deter and deter potential terrorist and/or organized criminal activity. They can also be deployed to augment existing law enforcement and security resources during public events that have the potential to draw large crowds into the transportation domain.

In many instances, VIPR teams consist of TSA law enforcement assets working with our law enforcement partners and are not deployed to conduct administrative searches. At the request of a stakeholder, TSA may deploy uniformed screeners to conduct administrative searches; however there are strict operational plans designed in coordination with the requesting stakeholder to ensure the teams are effective and efficient for the given environment.

Q. What happens if someone declines to be searched during a VIPR operation or exercise?

VIPR teams are deployed in coordination with local law enforcement to perform specific counter terrorism operations. All assets assigned to the VIPR team will conduct security and law enforcement operations in accordance with agreed upon plans.

Q. How many TSA personnel are working fulltime with VIPR? How has that changed over time?

The VIPR team program is designed to enable team size and composition to vary and be tailored to the specific mission. The teams generally can consist of local law enforcement officers, federal air marshals, canine teams, transportation security inspectors, transportation security officers and other local and/or TSA assets as deemed appropriate for the mission.

Since these teams are tailored to meet the needs of the requesting agency and the environment there is not a “normal” or “regular” size/composition.

Q. Do VIPR operations or exercises ever include plainclothes personnel? If so, are those plain clothes personnel ever VIPR/TSA officers?

Each operation is tailored based on the environment or at the specific request of our stakeholders. TSA VIPR operations can be composed of a variety of TSA, federal, state, and local law enforcement and security assets including: federal air marshals, TSA certified explosive detection canine teams, transportation security officers, behavior detection officers, TSA transportation security inspectors, local law enforcement officers, and security technology.

Q. How many of these teams will be dedicated to surface transportation? How many of these teams will be dedicated to aviation transportation?

TSA VIPR operations are conducted in partnership with law enforcement and security authorities in all modes of transportation, including:
Commercial Aviation, Air Cargo, General Aviation, Mass Transit, Maritime, Freight Rail, Highway infrastructure, and Pipeline. They are highly mobile teams and work with the stakeholders to ensure they are capable in providing security in all areas of transportation.

Q. What is TSA's authority to conduct searches of passengers and their baggage outside of the aviation domain and how is this not a violation of the 4th Amendment?

VIPR operations are tailored to meet the specific needs of each stakeholder request and the specific transportation environment. Based on the environment and needs of the stakeholders, VIPR operations can be composed of various TSA assets. These assets can include Federal Air Marshals who are the law enforcement arm of TSA, Transportation Security Officers who conduct passenger screening activities, and Transportation Safety Inspectors who have regulatory authority. In accordance with TSA's administrative search authority, and pursuant to an identifiable checkpoint, Transportation Security Officers can and do conduct random screening of passengers and baggage at surface transportation venues. Administrative searches are different from law enforcement searches in that the administrative search does not require probable cause, but must further an important government need, such as preventing would-be terrorists from bringing an explosive device onto a crowded commuter train. Importantly, the mission of the VIPR Program is to deter and detect acts of terrorism and many of TSA VIPR operations are visible presence operations. Thus, not all VIPR operations include checkpoint passenger screening.

Q. What criteria does TSA use to deploy VIPR teams at large events (i.e. DNC, RNC, NASCAR, NFL, etc.)

The mission of the Visible Intermodal Prevention and Response (VIPR) operations is to promote confidence in and protect our nation's transportation systems through targeted deployment of integrated TSA assets utilizing screening, inspections and law enforcement capabilities in coordinated activities to augment security of any mode of transportation.

In support of this mission, TSA has committed the VIPR program to provide terrorism risk mitigation support at transportation venues associated with National Security Special Events (NSSE) and events with Special Event Assessment Ratings (SEAR) of 1 or 2. There are approximately 8 to 12 of these events nationwide each year, including the State of the Union Address, the United Nations General Assembly, and the Super Bowl.

For events with regional or local prominence, TSA, through its VIPR field leaders, works with local stakeholders to identify risk-based opportunities for VIPR deployment personnel to augment state and local law enforcement and transportation security personnel and mitigate terrorism risk at transportation venues linked to those events.