



Transportation
Security
Administration

Office of Law Enforcement/Federal Air Marshal Service

Letter No. OLE 3421

Effective Date: 5/5/15

From: Roderick Allison 
Assistant Administrator/Director
Office of Law Enforcement/Federal Air Marshal Service

To: All Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) employees.

Subject: **Visible Intermodal Prevention and Response (VIPR) Planning Guidance**

1. **Revision:** This Policy Letter establishes OLE/FAMS guidance for compliance with [TSA MD 2800.13, Visible Intermodal Prevention and Response Program](#). The Letter also fully implements the guidelines outlined in TSA-OD-400-50-1-13B, *Visible Intermodal Prevention and Response Planning Guidance for the Office of Security Operations and the Office of Law Enforcement/Federal Air Marshal Service*, dated September 24, 2014. In addition, this revised Policy Letter supersedes FLD 7302, *Visible Intermodal Prevention and Response (VIPR) Planning Guidance for Federal Security Directors (FSD) and Office of Law Enforcement/Federal Air Marshal Service Special Agents in Charge (OLE/FAMS SAC)*, dated October 8, 2014.
2. **Explanation of Changes:** Changed the policy identifier to reflect the new Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) policy naming structure and updated organizational and personnel titles throughout.
3. **Attachment:**
 - A. TSA-OD-400-50-1-13B, *Visible Intermodal Prevention and Response Planning Guidance for the Office of Security Operations and the Office of Law Enforcement/Federal Air Marshal Service*.

File: 2000.1.4-b

OLE 3421

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

4. Responsibilities:

- A. Supervisors shall ensure that employees, under their supervision, understand and adhere to the Guidance in this Letter.
- B. OLE/FAMS Employees are responsible for following the Guidance contained in this Letter.

5. Guidance: OLE/FAMS personnel shall follow the provisions outlined in TSA MD 2800.13 and TSA-OD-400-50-1-13B.

File: 2000.1.4-b

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~



To enhance mission performance, TSA is committed to promoting a culture founded on its values of Integrity, Innovation and Team Spirit.

1. **PURPOSE:** This directive provides TSA policy and procedures for the full range of functions and activities for the Visible Intermodal Prevention and Response (VIPR) Program.
2. **SCOPE:** This directive applies to all TSA organizational elements.
3. **AUTHORITIES:**
 - A. 6 U.S.C. § 1112
 - B. 49 U.S.C. § 114
 - C. 49 U.S.C. § 44901
 - D. 49 U.S.C. § 44903
 - E. 49 U.S.C. § 44917
 - F. 49 C.F.R. Chapter XII
4. **DEFINITIONS:**
 - A. Concept of Operations (CONOPS): For purposes of this directive, a document that describes the process used by the Joint Coordination Center (JCC) to initiate, approve and monitor operations.
 - B. Deployment Operations Plan (DOP): For purposes of this directive, a document that describes specific VIPR operations.
 - C. Joint Coordination Center (JCC): Operations center, managed by Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) and comprised of representatives from OLE/FAMS, Office of Security Operations (OSO) and Transportation Sector Network Management (TSNM), is the single point of contact for VIPR deployments and for other incidents as directed by the Assistant Secretary.
 - D. Operations Coordinator: A TSA management official selected by Federal Security Directors (FSDs) or OLE/FAMS Field Office Special Agents in Charge (SACs) to oversee the VIPR operation.
 - E. Standard Operating Procedure (SOP): For purposes of this directive, a document that provides procedures for screening, inspection and law enforcement protocols.
 - F. Team Leader: A TSA employee selected by FSDs or OLE/FAMS SACs to serve as the on-site lead for the VIPR operation.

- G. Visible Intermodal Prevention and Response (VIPR) Program: TSA's deployment of personnel and equipment to augment the security of any mode of transportation at any location within the United States.

5. RESPONSIBILITIES:

- A. The Assistant Administrator for Law Enforcement/Director of the Federal Air Marshal Service is responsible for:
- (1) General oversight of Federal Air Marshals (FAMs), Explosive Security Specialists (ESSs), National Explosive Detection Canine Teams (NEDCTs), and Assistant FSDs for Law Enforcement.
 - (2) Drafting procedures for OLE/FAMS personnel that are consistent with this directive.
 - (3) Ensuring that OLE/FAMS personnel receive appropriate training to carry out this directive.
 - (4) Ensuring that all VIPR activities are carried out in accordance with applicable statutes, policies and directives and result in After-Action Reports and lessons learned.
 - (5) Establishing and managing the JCC.
 - (6) Ensuring the Transportation Security Operations Center (TSOC) provides assistance to VIPR operations and the JCC.
- B. The Assistant Administrator for Security Operations is responsible for:
- (1) General oversight of Behavior Detection Officers (BDOs), Bomb Appraisal Officers (BAOs), FSDs, Transportation Security Inspectors (TSIs) and Transportation Security Officers (TSOs).
 - (2) Drafting procedures for OSO personnel that are consistent with this directive.
 - (3) Ensuring that OSO personnel receive appropriate training to carry out this directive.
 - (4) Ensuring that all VIPR activities are carried out in accordance with applicable statutes, policies and directives and result in After-Action Reports and lessons learned.
 - (5) Management and oversight of the VIPR SOP and DOP when revisions are necessary.
- C. The Assistant Administrator for Operational Process and Technology/Chief Technology Officer is responsible for identifying, procuring and deploying security technology to support VIPR operations.

- D. The Assistant Administrator for Information Technology/Chief Information Officer is responsible for identifying, procuring and deploying information technology to support VIPR Operations.
- E. The Assistant Administrator for Intelligence is responsible for:
 - (1) Providing intelligence regarding threats and vulnerabilities.
 - (2) Providing risk analysis to assist in the planning of VIPR operations.
- F. The Assistant Administrator for Transportation Sector Network Management is responsible for:
 - (1) Supporting OSO and OLE/FAMS with VIPR operations.
 - (2) Working with transportation security partners and stakeholders on VIPR planning and implementation.
- G. The Chief Counsel is responsible for:
 - (1) Reviewing all operational documents and other policies to help ensure that VIPR operations are in compliance with legal requirements.
 - (2) Providing legal guidance on issues related to VIPR operations.
- H. The JCC is responsible for:
 - (1) Implementation, monitoring and oversight of the VIPR program and operations.
 - (2) Establishing guidelines for the coordination and deployment of VIPR operations.
 - (3) Ensuring that all VIPR activities are consistent with applicable statutes, policies and directives.
 - (4) Coordination and approval of DOPs for review.
 - (5) Ensuring that After-Action Reports are conducted and lessons learned are incorporated into future operational plans.
- I. The Operations Coordinator is responsible for:
 - (1) Ensuring that all VIPR activities are consistent with applicable statutes, policies, directives and procedures.
 - (2) Ensuring that all VIPR team members understand their responsibilities and authority during the VIPR operation, and have appropriate guidance to carry out VIPR operations.
 - (3) Consulting with local security, law enforcement and transportation officials to develop and deploy the VIPR operation.

- (4) Drafting the DOP and securing personnel and equipment resources to carry out the VIPR operation.
- (5) Working with the JCC on approval for the DOP.
- (6) Ensuring that all searches are conducted in accordance with [TSA MD 100.4](#), *Transportation Security Searches*.

J. The Team Leader is responsible for:

- (1) Providing on-site supervision of all VIPR operations.
- (2) Ensuring that all VIPR activities are consistent with applicable statutes, policies, directives and procedures.
- (3) Ensuring that all VIPR team members understand their responsibilities and authority during the VIPR operation, and have appropriate guidance to carry out VIPR operations.
- (4) Consulting with local security, law enforcement and transportation officials to develop and deploy the VIPR operation.
- (5) Ensuring that all searches are conducted in accordance with [TSA MD 100.4](#), *Transportation Security Searches*.

6. POLICY:

- A. TSA personnel shall use and implement this directive in carrying out their functions. Nothing in this directive is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter.
- B. VIPR teams may be developed to augment security in any mode of transportation. VIPR Teams may consist of one or any combination of the following TSA personnel: TSOs, BDOs, ESSs, BAOs, FAMs, TSIs, and NEDCTs. VIPR teams may use a variety of screening equipment and technologies.
- C. TSA will consult and coordinate with Federal, state, and local law enforcement officials, as well as affected transportation entities, as appropriate, when conducting these operations.
- D. VIPR Operations may be initiated by TSA Headquarters, including the JCC, or by local TSA officials or at the request of TSA stakeholders.
- E. TSA managers, as indicated in [TSA MD 100.4](#), in consultation with the Office of Chief Counsel, shall develop guidelines under which administrative or special needs searches will be conducted in various transportation venues.

7. **PROCEDURES:** VIPR operations shall be conducted in accordance with the VIPR DOP, VIPR SOP and VIPR CONOPS, and other relevant procedures. (These documents are available upon request if required for the performance of official duties by contacting the JCC at FC-JCC@dhs.gov).

8. EFFECTIVE DATE AND IMPLEMENTATION: This policy is effective immediately upon signature.

APPROVAL

Signed

9-12-08

Kip Hawley
Assistant Secretary

Date

Filing Instructions: File 200.1.1
Effective Date: 9-12-08
Review Date: 9-12-08
Distribution: Assistant Secretary/Administrator, Deputy Administrator, Associate Administrator, Assistant Administrators, Area Directors, Federal Security Directors, and OLE/FAMS HQ
Point of Contact: OLE/FAMS, Policy and Procedures Division,
OLE-FAMSPolicy@secureskies.net



Transportation Security Administration

Office of Security Operations
Office of Law Enforcement/Federal Air Marshal Service

September 24, 2014

Operations Directive

OD-400-50-1-13B: Visible Intermodal Prevention and Response Planning Guidance for the Office of Security Operations and the Office of Law Enforcement/Federal Air Marshal Service

Expiration: Indefinite

This Operations Directive (OD) is effective immediately upon signature. This OD supersedes **OD-400-50-1-13A**, *Visible Intermodal Prevention and Response Planning Guidance for Federal Security Directors and Office of Law Enforcement/Federal Air Marshal Service Special Agents in Charge, dated August 6, 2010*. **Changes to the previous version are indicated in bold.**

Summary

This OD provides guidance and procedures for Federal Security Directors (FSD) and Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) field office Supervisory Air Marshals in Charge (SAC) to jointly coordinate and execute Visible Intermodal Prevention and Response (VIPR) plans in their Area of Responsibility (AOR).

The VIPR mission is to promote confidence in and protect our nation's transportation systems through targeted deployment of integrated assets utilizing screening and law enforcement (LE) in coordinated activities to augment and enhance security.

The primary objective of VIPR operations is to prevent acts of terrorism **by** exercising security and **LE** capabilities in all modes of transportation. **The purpose of active screening in VIPR operations, outside of commercial aviation, is to detect the presence of explosives.** By consistently exercising and deploying **Transportation Security Administration (TSA)** assets in a preventative posture and conducting operations to deter **and disrupt** potential terrorist planning and **activities**, TSA will refine its capabilities to deploy assets when operational requirements are identified.

Definitions

A. Accessible Property Search - (b)(3):49 U.S.C. § 114(r)
(b)(3):49 U.S.C. § 114(r)

B. Activity Summary Report (ASR) – A mechanism used to report specific deployment information for each VIPR operation. An ASR must include a detailed summary for

each individual operation, state what assets will be utilized for the deployment, and address aspects that are unique to individual venues, capabilities, and deployments.

- C. After Action Report (AAR) – The mechanism for reporting a synopsis of observations, outcomes, and lessons learned from VIPR deployments related to a National Security Special Event (NSSE) or Special Event Assessment Ratings (SEAR) (b)(3):49
U.S.C. § event, or upon request.
- D. Deployment Operations Plan (DOP) – A comprehensive operational plan written after consultation with modal management, stakeholders, and LE partners. The DOP encompasses every authorized VIPR capability, deployable within transportation, in support of a particular mode, venue, series of venues or special event.
- E. Explosive Trace Detection (ETD) – A TSA-certified device designed to detect explosive particles on objects intended to be carried into any transportation mode, facility, or conveyance.
- F. Joint Coordination Center (JCC) – The nationwide coordination, approval, and logistics center for all VIPR deployments. The JCC comprises representatives from OLE/FAMS and the Office of Security Operations (OSO). It is the single point of contact (POC) for VIPR deployments.
- G. Operations Tracking Report (OTR) – A document submitted by the field to schedule future VIPR deployment dates, from which the JCC creates event logs in WEBEOC.
- H. Office of Security Policy and Industry Engagement (OSPIE) – the TSA office with responsibility for engaging with transportation sector stakeholders on a national level to develop and implement transportation security policies.
- I. Stakeholder – Any private or public entity responsible for the operation, maintenance, and/or security of a transportation mode, system, or venue.
- J. WebEOC – The document repository and program management system used by the JCC to track all VIPR deployments.
- K. VIPR Team – TSA personnel from the Offices of Security Operations and Law Enforcement who deploy specific law enforcement and transportation security capabilities with stakeholders in all modes of transportation nationwide.

Responsibilities

- A. FSDs, SACs, and/or their designees:
 - 1. Are responsible for the joint planning of VIPR operations in their AOR. **This planning must ensure stakeholders are fully engaged at the proper leadership level throughout the VIPR planning and execution process.**
 - 2. **Must maintain a high degree of situational awareness of specific VIPR operations within their AOR and the overall VIPR strategic plan.**

~~SENSITIVE SECURITY INFORMATION~~

3. May request additional support to deploy any TSA VIPR asset across the nation in coordination with the JCC to support VIPR activities in response to assessed risk and/or credible intelligence.
4. With responsibility for dedicating OSO personnel to VIPR teams, should assign the following: Surface Transportation Security Inspectors (TSI-S), Aviation Transportation Security Inspectors (TSI-A), Transportation Security Specialist - Explosives (TSS-E), Behavior Detection Officers (BDOs), and Transportation Security Officers (TSOs) where applicable. Additionally:
 - a. FSDs should provide the names of these dedicated assets to the VIPR program office.
 - b. FSDs have received additional FTEs to support this requirement.
 - c. FSDs should ensure that those personnel dedicated to VIPR teams are expending VIPR program funds.

Note: FSDs at airports without VIPR teams will not be impacted by this requirement.

5. Are responsible for collaborating closely among stakeholders, particularly the transportation system operator(s), within each AOR.
6. Are required to reassess the DOP on an annual basis or when threats, location vulnerabilities, or potential consequences of an attack change significantly.

Note: Risk information from OSPIE should be included as part of this reassessment.

7. Are required to apply a risk-based approach when identifying potential locations for VIPR deployment in all transportation modes associated with their AOR. Locations should be identified and prioritized based on the potential risk of terrorism. Input from OSPIE to inform the identification and prioritization process is highly encouraged.
8. Are responsible for identifying which VIPR capabilities and resources are best aligned with mitigating the risk of terrorism based on potential consequences and existing vulnerabilities.
9. Are responsible for developing a plan to schedule VIPR deployments in such a manner as to mitigate risk and maintain randomness and unpredictability. This may include scheduling VIPR operations on weekends, holidays, and non-business hours when appropriate.
10. Are responsible for developing an annual strategic plan prior to each fiscal year (FY) that delineates goals and objectives for deployment of TSA assets in support of VIPR operations.

Note: FSDs and OLE/FAMS SACs are encouraged to develop and coordinate this joint FSD/SAC FY strategic VIPR plan regionally and to utilize OSPIE resources for information and data in support of the planning process.

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 C.F.R. PARTS 15 AND 1520. NO PART OF THIS RECORD MAY BE DISCLOSED TO PERSONS WITHOUT A "NEED TO KNOW," AS DEFINED IN 49 C.F.R. PARTS 15 AND 1520, EXCEPT WITH THE WRITTEN PERMISSION OF THE ADMINISTRATOR OF THE TRANSPORTATION SECURITY ADMINISTRATION OR THE SECRETARY OF TRANSPORTATION. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 C.F.R. PARTS 15 AND 1520.~~

B. The JCC:

1. Provides operational guidance, oversight, and approval for all proposed VIPR operations.
2. Serves as the primary POC for coordinating VIPR deployments and is tasked with disseminating information to the field, including risk information from components of the Office of Security Policy and Industry Engagement (OSPIE)
3. Coordinates and supports all VIPR assets based on overall priority, senior leadership guidance, and/or intelligence-driven requirements.
4. Reviews all VIPR planning and operational documents from the field for compliance with the goals and objectives of the VIPR Program.
5. Coordinates support at transportation venues linked with National Special Security Event (NSSE) and Special Event Assessment Rating (SEAR) (b)(3):49 U.S.C. § 114(r) events. Direction and background information for participation in these events will be provided to relevant TSA field components.

Operational Requirements

- A. TSA's non-LE assets will be deployed in conjunction with a Federal, tribal, state, territorial, or municipal LE agency partner, or Federal Air Marshals (FAMs), when operating outside of commercial aviation. The LE partner must be dedicated as a VIPR resource and be physically present at the venue for the duration of the VIPR operation.
- B. Dedicated OSO assets assigned to VIPR teams shall be co-located with other VIPR personnel at the respective OLE/FAMS field office.
- C. Evidence of suspected violations of non-transportation-related criminal statutes discovered incidental to VIPR operations must be referred to the appropriate LE jurisdiction.
- D. The SAC and FSD should ensure that stakeholders have a comprehensive understanding of the capabilities and assets that TSA may employ during VIPR operations.
- E. Non-TSA assets deploying under the VIPR framework will do so under their own authorities. Unless otherwise formally directed by the TSA Assistant Administrator (AA) of OSO or the AA for OLE/FAMS, TSA VIPR assets will operate under TSA's authorities.
- F. Specific roles and responsibilities for all TSA VIPR personnel are addressed in the VIPR Standard Operating Procedures.
- G. All screening operations must be conducted in accordance with [TSA Management Directive 100.4. Transportation Security Searches](#).
- H. Primary Screening may be accomplished (b)(3):49 U.S.C. § 114(r)

(b)(3):49 U.S.C. § 114(r)

directed by the TSA Assistant Administrator (AA) of OSO or the AA for OLE/FAMS in consultation with Office of Chief Counsel (OCC). VIPR teams (b)(3):49 U.S.C. §

(b)(3):49 U.S.C. § 114(r)

(b)(3):49 U.S.C. § 114(r) unless otherwise directed by the AA for OSO or AA for OLE/FAMS.

Deployment Operations Planning

- A. A risk-based approach that considers threats to the specific transportation mode, vulnerabilities of the system, and consequences of an attack form the basis of deployment operations planning.

FSDs and SACs and/or their designees will provide deployment operations planning documentation which must include, but is not limited to, a description of the type of venue, potential threats to the system, the impact of a terrorist attack on the system, and what capabilities TSA can deploy to mitigate that risk and impact.

- B. All VIPR DOPs should be mutually agreed upon by both the FSD and the OLE/FAMS SAC and reviewed by a local OCC representative prior to submission to the JCC. As summarized in the DOP and ASR, all VIPR operations must have a connection to transportation security and must be designed to deter, detect, disrupt, and defeat acts of terrorism.
- C. VIPR operations at freight rail facilities require prior approval at the stakeholder's corporate level, including operations at shared rail facilities. The freight rail industry requires that the TSA Surface Regional Security Inspector (RSI) serve as liaison with the freight rail corporate stakeholder. Field personnel must contact the respective Surface RSI(s) who will facilitate communications between TSA and the respective corporate freight rail organization(s).
1. VIPR coordinators should ensure that their planning process provides sufficient time, at least two (2) additional weeks, for the corporate security stakeholders to review and concur with the operational schedule.
 2. After concurrence from the stakeholder, continue with the regular planning process including operational submission to the JCC with an OTR.
 3. The RSI map on JCC iShare provides contact information for the Surface RSIs aligned with OSO regions and their respective corporate freight rail responsibility.
- D. Each VIPR operation must have a single designated operational lead with responsibility for all TSA components. The selection of an operational lead requires FSD and SAC concurrence.

Reporting Requirements

Access to and instructions for the WebEOC database are coordinated through the JCC. Submit documents as follows:

- A. DOPs are due to the JCC via email no later than 7 business days prior to the deployment date. DOPs are approved by the FSD and OLE/FAMS SAC and must be

reviewed by local field counsel prior to submission to the JCC. The JCC will review DOPs for consistency with the VIPR Program mission, goals, and objectives. Headquarters' OCC will review further for legal sufficiency.

- B. An OTR must be submitted prior to the initiation of all VIPR operations.
- C. An ASR must be uploaded to the WebEOC event log prior to the execution of a VIPR operation to ensure that deployed capabilities are aligned with the requisite DOP and that staffing levels are accurately reflected.
- D. The JCC-processed ASR must be updated and uploaded to the WebEOC event log if a reportable event has occurred (for example, arrest, injury, equipment damage, etc.), if there are significant staffing changes, or to report observations, deficiencies, or lessons learned. An email notification must be sent to FC-JCC-TSA@dhs.gov to advise of the revised ASR.
- E. The AAR is due via email to the JCC at FC-JCC-TSA@dhs.gov, and uploaded to the WebEOC event log, no later than 10 business days after the conclusion of a VIPR operation related to NSSE or SEAR (b)(3):4
9
JCC events.

Point of Contact

Contact the JCC Surface, Aviation, and LE Subject Matter Experts at 703-563-3345 or 1-855-VIPRJCC or FC-JCC-TSA@dhs.gov Monday through Friday 6:00 a.m. to 8:00 p.m. Eastern time.



Kelly C. Hoggan
Assistant Administrator
Office of Security Operations



Roderick Allison
Assistant Administrator/Director
Office of Law Enforcement/Federal Air
Marshal Service

VISIBLE INTERMODAL PREVENTION AND RESPONSE

Visible Intermodal Prevention & Response (VIPR) Standard Operating Procedures



Transportation
Security
Administration

The Transportation Security Administration (TSA) personnel and contractors must use and implement these standard operating procedures in carrying out their functions related to security screening of passengers and property. Nothing in these procedures is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter by prospective or actual witnesses or parties. See *United States v. Caceres*, 440 U.S. 741 (1979).

Revision: 5
Date of Revision: May 1, 2015
Implementation Date: May 1, 2015

CONTROL PAGE

1. ADD	2. DELETE
Revision 3, July 18, 2014	Revision 2, June 09, 2008
Revision 4, April 8, 2015	Revision 3, July 18, 2014
Revision 5, May 1, 2015	Revision 4, April 8, 2015

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

Summary of Changes

Version	Date	Summary of Changes
4	04/08/15	The following change was made in this version: <ul style="list-style-type: none">• Page 1-8 - Section 1.8.3. – Added requirement for field offices to notify Joint Coordination Center of requests for additional TSA personnel and clarified information requirements
5	05/01/15	The following change was made in this version: <ul style="list-style-type: none">• Page 5-34 – Section 5.2.2 - Update Subject Matter Expertise for Transportation Security Specialists - Explosives

~~WARNING: This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

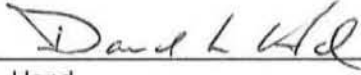
Revision: 5

Date of Revision: May 1, 2015

Implementation Date: May 1, 2015

VIPR SOP

EFFECTIVE DATE AND IMPLEMENTATION: These changes are effective immediately upon signature.



David L. Hand
Division Director
Field Operations Division
Office of Law Enforcement/Federal Air Marshal Service

Date 5/4/15

~~WARNING: This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

TABLE OF CONTENTS

- 1. PURPOSE AND GENERAL INFORMATION 1-1**
 - 1.1. PURPOSE 1-1**
 - 1.2. VIPR DOCUMENT HANDLING AND PROTECTION 1-1**
 - 1.3. JOINT COORDINATION CENTER (JCC)..... 1-2**
 - 1.4. OPERATIONAL PLANNING 1-2**
 - 1.5. DEPLOYMENT OPERATIONS PLAN (DOP) 1-3**
 - 1.6. VIPR RISK-BASED DEPLOYMENT METHODOLOGY 1-4**
 - 1.7. VIPR REPORTING 1-5**
 - 1.7.1. WEBEOC REPORTING 1-5
 - 1.7.2. OPERATIONS TRACKING REPORT (OTR) 1-6
 - 1.7.3. ACTIVITY SUMMARY REPORT (ASR) 1-6
 - 1.7.4. REPORTABLE EVENTS 1-6
 - 1.7.5. AFTER ACTION REPORT (AAR) 1-7
 - 1.7.6. CANCELLATIONS 1-7
 - 1.8. GENERAL INFORMATION 1-8**
 - 1.8.1. VISIBLE, UNIFORMED OPERATIONS..... 1-8
 - 1.8.2. LAW ENFORCEMENT SUPPORT..... 1-8
 - 1.8.3. REQUESTS FOR ADDITIONAL TSA PERSONNEL 1-8
 - 1.8.4. PRE-OPERATIONAL NOTIFICATIONS..... 1-9
 - 1.8.5. COMMUNICATIONS EQUIPMENT..... 1-9
 - 1.8.6. PRE-DEPLOYMENT BRIEFINGS..... 1-9
 - 1.8.7. APPLICABLE CASE LAW GOVERNING SEARCHES 1-9
 - 1.9. DEFINITIONS 1-10**
 - 1.10. ACRONYMS 1-14**
- 2. VIPR CAPABILITIES AND VENUES..... 2-17**
 - 2.1. CAPABILITIES 2-17**
 - 2.2. SCREENING CAPABILITIES..... 2-17**
 - 2.3. TRANSPORTATION VENUES 2-18**
 - 2.3.1. COMMERCIAL AIRPORT VENUES 2-18
 - 2.3.2. SURFACE AND OTHER TRANSPORTATION VENUES 2-18
 - 2.3.3. FREIGHT RAIL OPERATIONS 2-19
- 3. VIPR ACTIVE SCREENING CAPABILITIES..... 3-20**
 - 3.1. SCREENING INDIVIDUALS..... 3-20**

~~WARNING: This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

3.1.1. SCREENING INDIVIDUALS AT COMMERCIAL AIRPORT VENUES 3-20

3.1.2. INDIVIDUALS AT SURFACE AND OTHER TRANSPORTATION VENUES..... 3-20

3.2. SCREENING PROPERTY..... 3-20

3.2.1. SCREENING PROPERTY AT COMMERCIAL AIRPORT VENUES 3-20

3.2.2. SCREENING PROPERTY AT SURFACE AND OTHER TRANSPORTATION VENUES. 3-20

3.3. SCREENING VEHICLES..... 3-21

3.3.1. ETD SCREENING OF VEHICLES 3-21

3.3.2. SEARCH OF VEHICLES..... 3-22

3.4. VIPR ACTIVE SCREENING PROCEDURES 3-22

3.4.1. SCREENING EQUIPMENT 3-22

3.4.2. SIGNS AND NOTIFICATION 3-22

3.4.3. INITIATION AND WITHDRAWAL FROM SCREENING 3-23

3.4.4. SUPERVISOR/LEO NOTIFICATION 3-23

3.4.5. DISCOVERY OF SUSPECTED EXPLOSIVES OR EXPLOSIVE MATERIAL..... 3-24

4. VIPR PASSIVE SCREENING CAPABILITIES 4-25

4.1. GENERAL 4-25

4.2. VISUAL INSPECTIONS 4-25

4.3. PATROLS..... 4-25

4.3.1. PERIMETER..... 4-25

4.3.2. ON BOARD PUBLIC CONVEYANCE /VESSEL 4-25

4.3.3. CRITICAL INFRASTRUCTURE 4-25

4.3.4. MAN PORTABLE AIR DEFENSE SYSTEM (MANPADS) 4-26

4.3.5. SURVEILLANCE/COUNTER-SURVEILLANCE..... 4-26

4.3.6. BEHAVIOR RECOGNITION..... 4-26

4.4. EXPLOSIVES DETECTION CANINE TEAMS..... 4-27

4.5. AIRCRAFT SECURITY SWEEP 4-27

4.6. ID VERIFICATION 4-27

4.7. TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC)..... 4-27

4.8. PREVENTIVE RADIOLOGICAL NUCLEAR DETECTION (PRND)..... 4-28

4.8.1. RADIATION DETECTION EQUIPMENT 4-29

4.8.2. OPERATING PROCEDURES 4-29

4.8.3. PRE-DEPLOYMENT PROCEDURES..... 4-30

4.8.4. DEPLOYMENT PROCEDURES 4-30

4.8.5. SECONDARY SCREENING RESPONSE PROCEDURES..... 4-31

4.8.6. ADJUDICATION PROCEDURES..... 4-31

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

5. VIPR: OTHER CAPABILITIES 5-33

5.1. LAW ENFORCEMENT 5-33

5.2. SUBJECT MATTER EXPERTISE 5-33

5.2.1. GENERAL AVIATION OUTREACH 5-33

5.2.2. TRANSPORTATION SECURITY SPECIALIST-EXPLOSIVES (TSS-E) 5-33

5.2.3. TRANSPORTATION SECURITY INSPECTOR (TSI) 5-34

APPENDIX - VIPR CAPABILITIES A-1

~~WARNING: This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

**Chapter
1**

1. PURPOSE AND GENERAL INFORMATION

1.1. PURPOSE

- A. TSA's authority to develop Visible Intermodal Prevention and Response (VIPR) teams and conduct VIPR operations derives from the *Aviation and Transportation Security Act* (ATSA) (Public Law 107-71) and Section 1303 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (Public Law 110-53). 6 USC 1112 specifically authorizes the development of VIPR teams utilizing any asset of the Department of Homeland Security (DHS), including but not limited to federal air marshals, transportation security inspectors, canine detection teams, and advanced screening technology to augment the security of any mode of transportation at any location within the United States.
- B. These Standard Operating Procedures (SOP) establish uniform procedures and standards for the deployment of VIPR teams. VIPR teams shall:
 - Prior to the deployment, consult with local security, law enforcement, and transportation venue personnel to develop the VIPR Deployment Operations Plan (DOP) which describes the specific VIPR operation, including but not limited to deployment site, participants, security measures, screening operations, and any other pertinent protocol and procedures.
 - Prior to and during the deployment, consult with local security and law enforcement officials in the jurisdiction where the VIPR team is or will be deployed, to develop and agree upon the appropriate operational protocols and provide relevant information about the mission of the VIPR team, as appropriate.
 - Prior to and during the deployment, adhere to all directives, authorities, procedures, and protocol contained within the VIPR DOP, VIPR SOP, and all applicable TSA SOPs, Management Directives, and Operational Directives.

1.2. VIPR DOCUMENT HANDLING AND PROTECTION

- A. VIPR document templates can be found in the Templates section in WebEOC.
- B. TSA management must maintain at all FAM field offices and FSD offices:
 - A complete copy of this SOP and VIPR DOPs for all operations conducted; and
 - Any other SOP referenced in this document.
- C. The VIPR SOP and VIPR operational documents are Sensitive Security Information (SSI). If maintained electronically locally and in WebEOC, they must be password protected to prevent unauthorized access in accordance with 49 CFR part 1520.

WARNING: This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.

- D. TSA personnel must protect all SOPs from unauthorized access and ensure they are properly secured at all times in accordance with TSA SSI handling procedures. Refer to [Welcome to the Sensitive Security Information iShare Site](#).
- E. This SOP and any other applicable SOPs must be available to all TSA VIPR personnel for review.
- F. The VIPR DOP may be shared with the transportation stakeholder as a covered party with a need-to-know (49 CFR 1520). Prior to sharing the DOP with the transportation stakeholder, the stakeholder must be provided written instructions for handling SSI material. If the covered party is not familiar with handling SSI, a DHS Non-Disclosure Agreement should be signed. If the covered party is outside of DHS, they should be provided a copy of the SSI Best Practices Guide for Non-DHS Employees. Both documents are available in WebEOC VIPR Protocols section of WebEOC.

If transmitted via email, the DOP must be password protected. If the stakeholder is not a DHS agency, you must remove the TSA password and apply a different password to the document, following the TSA SSI password guidelines.
- G. All SOP questions should be directed to local field office VIPR management or VIPR program headquarters staff at FC-JCC-TSA@dhs.gov.

1.3. JOINT COORDINATION CENTER (JCC)

- A. TSA's Joint Coordination Center (JCC) is the nationwide coordination, approval, and logistics center for all VIPR deployments. The JCC comprises representatives from OLE and OSO. It is the single point of contact (POC) for VIPR deployments.
- B. The JCC:
 - 1. Provides approval, operational guidance, and oversight for all proposed VIPR operations.
 - 2. Serves as the primary POC for coordinating VIPR deployments and is tasked with disseminating information to the field, including risk information from components of the Office of Security Policy and Industry Engagement (OSPIE).
 - 3. Coordinates and supports all VIPR assets based on overall priority, senior leadership guidance, and/or intelligence-driven requirements.
 - 4. Reviews all VIPR planning and operational documents from the field for compliance with the goals and objectives of the VIPR Program.
 - 5. The JCC will coordinate support at transportation venues linked with National Special Security Events (NSSE) and Special Events Assessment Rating (SEAR) (b)(3) events. Direction and background information for participation in these events will be provided to relevant TSA field components.

1.4. OPERATIONAL PLANNING

- A. Apply a risk-based approach when identifying potential locations for VIPR deployment in all transportation modes associated with your AOR prioritized based on the potential risk of a terrorist attack.
- B. Identify the VIPR capabilities and resources that are best aligned with mitigating terrorism risks based on potential consequences and existing vulnerabilities.

WARNING: This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.

- C. Develop a plan to schedule VIPR deployments to mitigate risk and maintain randomness and unpredictability; this may include scheduling VIPR operations on weekends, holidays, and non-business hours when appropriate.
- D. VIPR operations are expected to encompass on-site operational in-briefings and out-briefings with the transportation and law enforcement stakeholders. When planning the operation and preparing the operational documents, the start time is the time that the on-site operation in-briefing with stakeholders is scheduled to start, and the end time is the time that the on-site operation out-briefing with stakeholders is concluded. If on-site in-briefing or out-briefing is not scheduled, then the operation should be scheduled to start when TSA and stakeholder VIPR personnel initiate the operation at the venue, and the operation should be scheduled to stop when TSA and stakeholder VIPR personnel cease the operation at the venue.
- E. Develop a joint Federal Security Director (FSD) and Federal Air Marshal (FAM) Supervisory Air Marshal in Charge (SAC) annual strategic plan prior to each fiscal year (FY) that delineates goals and objectives for deployment of TSA assets in support of VIPR operations. FSDs and SACs are encouraged to develop and coordinate this joint strategic plan regionally and to utilize OSPIE resources for information and data in support of the planning process.

1.5. DEPLOYMENT OPERATIONS PLAN (DOP)

- A. The Deployment Operations Plan (DOP) is a comprehensive plan written after consultation with modal management, stakeholders, and law enforcement partners. The DOP encompasses every authorized VIPR capability, deployable within transportation, in support of a particular mode, venue, series of venues or special event..
- B. When completing the DOP, apply a risk-based approach in identifying potential locations for VIPR deployment in all transportation modes associated with your AOR. Locations should be identified and prioritized based on the potential risk of a terrorist attack. Identify which VIPR capabilities and resources are best aligned with mitigating terrorism risks based on potential consequences and existing vulnerabilities.
- C. The DOP must include, but is not limited to, a description of the type of venue, potential threats to the system, the impact of a terrorist attack on the system, and what capabilities TSA can deploy to mitigate that risk and impact.
- D. All VIPR DOPs must be mutually agreed upon by both the FSD and the SAC and reviewed by the Office of Chief Counsel (OCC) field legal representative prior to submission to the JCC. All VIPR operations must have a connection to transportation security and must be designed to deter, detect, disrupt, and defeat acts of terrorism.
- E. Submit the draft DOP to FC-JCC-TSA@dhs.gov via email providing enough time for the review process to occur (b)(3):49 U.S.C. § 114(r) prior to the first deployment date. The JCC will review the DOP for consistency with the VIPR Program mission, goals, and objectives and will coordinate any changes with the DOP drafter. The JCC will coordinate with HQ OCC for further review for legal sufficiency. The final approved DOP will be transmitted to the SAC and FSD, and VIPR designees such as the VIPR SFAM(s), AFSD-LE, and DOP drafter.
- F. VIPR operations at freight rail facilities require prior approval at the stakeholder's corporate level, including operations at shared rail facilities. The freight rail industry requires the TSA Surface

WARNING: This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.

Regional Security Inspector (RSI) serve as liaison with the freight rail corporate stakeholder. Field personnel must contact the respective Surface RSI(s) who will facilitate communications between TSA and the respective corporate freight rail organization(s). See Section 2.3.3.

- G. SACs/FSDs and/or their designees must reassess the DOP on an annual basis or when threats, location vulnerabilities, or potential consequences of an attack change significantly. Risk information from the Office of Security Policy and Industry Engagement (OSPIE) provided by the JCC should be included as part of this reassessment.

1.6. VIPR RISK-BASED DEPLOYMENT METHODOLOGY

- A. The JCC is responsible for analyzing, updating, and providing information to the field concerning VIPR locations to which TSA personnel will deploy VIPR teams in an effort to detect, deter, and disrupt potential terrorist targeted actions against the nation's transportation systems.
- B. It is understood that prevention is a main staple of VIPR operations; however an additional purpose of VIPR operations is to prepare TSA personnel to respond to critical incidents through the deployment of its assets to augment or enhance existing security measures. By consistently exercising and deploying its assets in a preventative posture, and visibly deterring potential terrorist planning and actions, TSA will refine its capabilities to seamlessly deploy those assets during times of crisis.
- C. The following criteria may be considered when developing VIPR operations. Refer to JCC VIPR iShare for supporting documents: [Home - Joint Coordination Center \(JCC\)](#)

(b)(3):49 U.S.C. § 114(r)

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

(b)(3):49 U.S.C. § 114(r)

1.7. VIPR REPORTING

1.7.1. WEBEOC REPORTING

- A. The VIPR Team Leader or designee must use the WebEOC Event Log to report VIPR operations activity: VIPR operations start and stop times, periodic status updates over the course of operations, and any reportable events.
- B. The VIPR SFAM and/or Team Leader are responsible for reviewing and updating as appropriate the accuracy of information in the WebEOC Event Log, regardless of whether entries are generated by the airport Coordination Center or FAMS Field Office Operations Center.

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

1.7.2. OPERATIONS TRACKING REPORT (OTR)

- A. All reporting form templates can be found in the VIPR Templates section in WebEOC. Once date(s) have been determined for a VIPR operation, submit an Operations Tracking Report (OTR) to the JCC, normally several weeks prior to the operation, but no more than thirty days in advance. The OTR is the mechanism by which the JCC creates the WebEOC Event Logs for individual deployments.
- B. The OTR should identify each VIPR operation to be conducted. If multiple operations at the same venue on the same day are scheduled, one OTR entry should be made for each operation with operational times noted. If more than one transportation mode is being worked, a separate OTR must be submitted for that mode as OTRs are specific to the DOP. Multiple operations governed by the same DOP can be listed in one OTR, with a separate entry for each operation. Each OTR must display the title page of the appropriate DOP as the title of the OTR.

1.7.3. ACTIVITY SUMMARY REPORT (ASR)

- A. The Activity Summary Report (ASR) provides the specific operational details for each scheduled VIPR operation. The ASR must include the name and cell phone number of the Operational Team Leader for the VIPR Operation.
- B. The VIPR Team Leader or designee must upload the ASR to the WebEOC Event Log. An initial ASR should be submitted 48 to 72 hours prior to the execution of a VIPR operation to ensure that deployment staffing levels/types will be accurately reflected and to allow for JCC review. The JCC will process the ASR from WebEOC, upload the processed ASR to the Event Log as a new log entry, and return the ASR to the submitter via e-mail. The processed ASR, now called the AM ASR, will contain the assigned VIPR operation identification number and a new filename containing the operation date, operation number and FSD location.
- C. If there are changes in participants or capabilities deployed, or a reportable event occurs, the Team Leader must ensure the AM ASR with the assigned identification number is updated and submitted at the conclusion of the operation, renamed as a PM ASR. Make the necessary changes and complete the last section "Significant Incidents/Special Events". Upload the updated ASR to the WebEOC Event Log with the "Attach ASR" log type, noting that the ASR is a PM ASR and the reason for submission. Notify the JCC by email that a PM ASR has been uploaded. The PM ASR should be submitted prior to the end of duty.

1.7.4. REPORTABLE EVENTS

- A. The VIPR Team Leader must report significant events to TSA's Transportation Security Operations Center (TSOC) in accordance with Operations Directive (OD) 400-18-2 series: *Reporting Security Incidents to TSOC*, and notify the JCC by telephone. Refer to JCC VIPR iShare for the OD. The reportable event must be documented in the WebEOC Event Log with the "Significant Incident" log type. The JCC will review the event and may revise the log type to "Other Update" if it is deemed not significant for VIPR reporting. Prior to the end of duty, all follow up documentation must be sent via email to the JCC. This documentation includes the PM ASR with the "Significant Incidents/Special Events" section completed, the FAM Activity Report if applicable, the Suspicious Incident Report, and all other relevant agency documentation if applicable.

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

B. Reportable events may include

(b)(3):49 U.S.C. § 114(r)

(b)(3):49 U.S.C. § 114(r)

7. Result in media attention.

C. In cases of arrests, assistance to other agencies, or any law enforcement action taken, note the action in the Event Log and summarize in a PM ASR at the conclusion of the VIPR. Log entries should include but are not limited to the following:

1. Law enforcement agencies involved
2. Type of violation enforced or under investigation and whether or not the violation was initiated as a direct result of activities conducted during the VIPR operation
3. Time/location of arrest
4. Basic information of the subject (e.g. John Smith; M/W/35/5'11"/250)
5. Indices checks conducted and results (e.g. NCIC Warrant Check-Negative Results)
6. Injuries
7. Media attention
8. Other information deemed pertinent

1.7.5. AFTER ACTION REPORT (AAR)

The VIPR Team Leader or designee must upload to the Event Log an After Action Report (AAR) and submit to FC-JCC-TSA@dhs.gov within 10 business days after conclusion of a VIPR conducted in support of a National Special Security Event (NSSE) or Special Event Assessment Rating (SEAR) event, or as directed by management.

(b)(3):49 U.S.C. § 114(r)

1.7.6. CANCELLATIONS

To cancel an operation scheduled in WebEOC, the VIPR Team Leader or designee must make a log entry in the WebEOC Event Log using the "Cancellation" log type and indicate the reason for the cancellation, e.g. weather, staffing, stakeholder request. This log entry will alert the JCC to cancel the operation in the database.

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

1.8. GENERAL INFORMATION

1.8.1. VISIBLE, UNIFORMED OPERATIONS

The foundation that VIPR operates upon is high visibility uniformed operations. Uniformed operations have the greatest deterrent effect when all members of the team are uniformed and highly visible. VIPR Program policy requires that a majority of the FAMs on the VIPR be in uniform when conducting VIPR operations. Uniformed law enforcement team members, whether they be FAMs or federal, state, and local partners, complement the VIPR mission and only serve to increase its effectiveness.

1.8.2. LAW ENFORCEMENT SUPPORT

During all surface VIPRs, TSA non-law enforcement personnel must be deployed with a law enforcement officer or a FAM. This law enforcement partner must be a dedicated VIPR resource and physically present at the venue for the duration of the VIPR operation. The law enforcement entity must be identified in the DOP and in the ASR.

1.8.3. REQUESTS FOR ADDITIONAL TSA PERSONNEL

- A. All requests for additional TSA support, including dedicated VIPR teams from other AORs, must be made by the Field Office SAC to his or her Regional Director (RD) and to the JCC for review and approval. The RD will provide approval for the additional resources and the JCC will provide approval for the operational details, including a line of accounting for the resources. Once approved by both the RD and the JCC, the JCC has sole responsibility to coordinate **all** support, including determining availability of funds, assessing operational tempo and proximity of supporting offices, as well as considering additional guidance or input from TSA senior leadership.
- B. OLE/FAMS Field Offices coordinating VIPR support of NSSE and SEAR level events must provide the Joint Coordination Center (JCC) with the following information at the initiation of the planning process:
 - 1. Event Title, NSSE or SEAR Level (1-5), date(s), time(s) and duration,
 - 2. A brief background of the event, its purpose, the organizers, and relevant threat assessments or law enforcement bulletins (if any),
 - 3. Assessment of nexus of the event's terrorism threat to transportation venues
 - 4. Projected level of counter-terrorism support to be committed by other Federal, State, and Local agencies (outside of TSA)
 - 5. Anticipated level of support by the responsible field office, to include
 - a) number of operations and average duration,
 - b) number of VIPR assigned personnel,
 - c) number of GBA/Flight assigned personnel,
 - d) impact to flight operations (if any), and
 - e) projected additional VIPR team support requests (from outside of the local AOR), and travel cost estimate(if required), and
 - 6. Email string documenting SAC/RD/VIPR JCC concurrence.

WARNING: This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.

- C. Requests for additional OSO assets from outside of a given Area of Responsibility (AOR) such as Transportation Security Officers (TSO), Behavior Detection Officers (BDO), Transportation Security Specialists-Explosives (TSS-E) and other OSO personnel as part of the National Deployment Force (NDF) is coordinated by the National Deployment Office (NDO). Submission of an NDO Support Request Form from the requesting FSD requires Area Director level approval before being forwarded to the NDO for action. Additional information is available on the NDO Field Resources iShare site <https://team.ishare.tsa.dhs.gov/sites/SecurityOperations/OOP/NDO/support/default.aspx>

1.8.4. PRE-OPERATIONAL NOTIFICATIONS

- A. Deconfliction Protocols: TSA VIPR field components must develop local protocols in conjunction with stakeholders and partners that ensure proper notification to federal, state, and local law enforcement agencies prior to any VIPR operation. Deconfliction protocols:
 - Ensure officer safety by preventing blue on blue situations and;
 - Prevent one agency's law enforcement activities from compromising another agency's ongoing investigations.
- B. FSDs and SACs are encouraged to develop relationships with Fusion Centers, Office of Emergency Management Command Centers, and State Counter-Terrorism Offices within their AOR to effectively coordinate notification processes.

1.8.5. COMMUNICATIONS EQUIPMENT

Communications equipment must be available at all VIPR locations to provide direct communication between the VIPR team and other security partners. The equipment type must be specified in the VIPR DOP and must be tested and functional prior to each deployment.

1.8.6. PRE-DEPLOYMENT BRIEFINGS

Prior to conducting a VIPR operation, the Team Leader must ensure that the VIPR team has been briefed on the following venue specific information:

- A. TSA legal briefing and FAMS arrest authority
- B. Screening methodology
- C. Emergency response and evacuation plan
- D. Threat item resolution including:
 1. Explosives and explosive materials
 2. Firearms and prohibited items
 3. HAZMAT

1.8.7. APPLICABLE CASE LAW GOVERNING SEARCHES

Case law is available on the JCC VIPR iShare site.

- A. Consent Searches
 - Katz v. United States*

WARNING: This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.

Schneckloth v. Bustamonte

B. Administrative Searches/Airport Searches

United States v. Davis
United States v. Aukai
United States v. Hartwell

1.9. DEFINITIONS

Accessible Property – Property that is intended to be accessible to the individual in any secure area or while aboard any public conveyance.

Accessible Property Search (b)(3):49 U.S.C. § 114(r)
(b)(3):49 U.S.C. § 114(r)

Activity Summary Report (ASR) – A report of specific deployment information for each VIPR operation, providing a detailed summary of location(s), team assets, and capabilities.

Additional Screening – Secondary screening conducted to detect potential threats or risks or any particular substance, attribute, person, or undesirable material.

Administrative Search – A search conducted without a warrant as part of a regulatory plan in furtherance of a specified non-law enforcement government purpose, such as to determine compliance with TSA regulations or to prevent the carriage of threat items or entry of an unauthorized person into the sterile area, or to screen passengers entering any public conveyance.

After Action Report (AAR) - A mechanism for reporting a synopsis of observations, outcomes, and lessons learned from VIPR deployments related to a National Special Security Event (NSSE) or Special Event Assessment Rating (SEAR) (b)(3): event, or on request.

Aircraft Operations Area (AOA) – A portion of an airport, identified in the airport security program, in which security measures specified in 49 CFR Part 1542 are carried out. This area includes aircraft movement areas, aircraft parking areas, loading ramps, and safety areas for use by aircraft regulated under 49 CFR Part 1544 or 1546, as well as any adjacent areas (such as general aviation areas) that are not separated by adequate security systems, measures, or procedures. This area does not include the secured area.

Alarm Resolution – The process of determining that an individual or property is free of prohibited items following a screening system alarm by performing additional screening procedures.

Articulable Belief – A belief based on specific and articulable observations which indicate that an individual or item may pose a possible threat to transportation security.

Behavior Detection Officer (BDO) - Specially-trained TSA personnel and TSA contract personnel who execute TSA's Screening of Passengers by Observation Technique (SPOT) Program.

Checkpoint Screening - A search or appraisal of individuals and property for threats or threat items at a screening checkpoint.

Commercial Airport - A complex of runways and buildings for the takeoff, landing, and maintenance of civil aircraft, with facilities for passengers.

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

Consent Search – A search by an authorized individual of a person, property, location, or vehicle based on permission by a person who has actual or apparent authority over the thing to be searched.

Conveyance – A means of transporting cargo, such as a vehicle, truck, or railway car.

Deployment Operations Plan (DOP) – A comprehensive plan written after consultation with modal management, stakeholders, and law enforcement partners. The DOP encompasses every authorized VIPR capability, deployable within transportation, in support of a particular mode, venue, series of venues or special event..

Direct Access Point (DAP) – Any location or route providing access to a SIDA, AOA, secured, sterile area, or aircraft. In these locations individuals, accessible property, and vehicles are subject to search by TSA.

Explosives – Military, commercial, or improvised compounds characterized by their ability to rapidly convert from a solid or liquid state into a hot gaseous compound with a much greater volume than the substances from which they are generated.

Explosive Trace Detection (ETD) – A TSA-certified device designed to detect explosive particles on objects intended to be carried into any transportation mode, facility, or conveyance.

Federal Air Marshal (FAM) – A TSA law enforcement officer who derives his or her authority from 49 U.S.C. § 114(p), 49 U.S.C. § 44903(d), 49 U.S.C. § 44917, and the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53, 121 Stat. 266).

Federal Security Director (FSD) – The ranking TSA authority responsible for day-to-day operational leadership and coordination of federal security capabilities within an assigned area of responsibility.

General Aviation Airport - An airport used exclusively by private and business aircraft not providing air carrier commercial passenger service.

Hazardous Materials (HAZMAT) – Substances or materials that have been determined to be capable of posing an unreasonable risk to health, safety, and property when transported in commerce, and which have been so designated under the U.S. Department of Transportation (DOT) HAZMAT Regulations (HMR).

Improvised Explosive Device (IED) – A device that has been fabricated in an improvised manner and incorporates explosives or destructive, lethal, noxious, pyrotechnic, or incendiary chemicals in its design. Generally an IED will consist of an explosive, a power supply, a switch or timer, and a detonator or initiator.

Joint Coordination Center (JCC) – The TSA national coordination center for all TSA VIPR operations, responsible for the oversight of planned and on-going VIPR operations throughout the nation. It is the one source of information for the operational deployment of TSA assets for VIPR operations and non-routine, response, and recovery operations. The JCC is also responsible for TSA asset deployment during times of crisis or critical incidents.

Law Enforcement Officer (LEO) – A sworn employee of a government entity (Federal, to include U.S. Military Police and U.S. Capitol Police, state, tribal, territorial and local, to include Rail police officers), with full power of arrest, who is trained and commissioned to enforce the criminal laws of the jurisdiction(s) in which he or she is commissioned.

Lead Transportation Security Officer (LTSO) – A TSO who is designated by TSA management or an STSO to perform additional duties and responsibilities. An LTSO may be designated to perform the functions of an STSO. In this SOP, when the term STSO is used, it also refers to a LTSO who has been designated to perform STSO functions.

WARNING: This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.

Man Portable Air Defense Systems (MANPADS) – Shoulder-launched surface-to-air-missiles, typically guided weapons that are a threat to low flying aircraft.

Multi-Mode Threat Detector (MMTD) - A type of Explosive Trace Detection (ETD) equipment made by Smith Detection. This system has undergone technical evaluations and piloting to support TSA screening operations in surface modes of transportation. MMTD were purchased by the Office of Security Policy and Industry Engagement to support Mobile Screening VIPR operations in several mass transit locations across the US

National Special Security Event (NSSE) - National Special Security Events (NSSEs) designate major activities or observances that, under federal law, give the Secret Service the authority and responsibility for all security planning associated with such events. NSSEs usually include the presence of national political dignitaries, foreign heads of state, and/or large crowds; or have other major national or international significance. For events that do not rise to the NSSE level, there is an additional ranking protocol used at the federal level, the Special Events Program of the U.S. Department of Homeland Security (see SEAR).

Operations Tracking Report (OTR) – A document submitted by the field to schedule future VIPR deployment dates, from which the JCC creates event logs in WebEOC.

Preventive Radiological Nuclear Detection (PRND) – The use of radiation detection and isotope identification equipment during a VIPR operation.

Prohibited Items – Items that are not permitted to be carried by individuals through the screening checkpoint, in the sterile area, or onboard a mode of transportation.

Random Continuous Selection – A random selection protocol where persons, property, or vehicles at a screening location are selected based solely upon the availability of a screening station. When the screening station is not engaged in screening a person, property, or a vehicle, the next person, property or vehicle that approaches the screening station is selected for screening. Once the screening of that person, property, or vehicle is completed, the next approaching person, property, or vehicle is selected for screening.

Random Selection Protocol – A pre-determined protocol that uses a random number generator or other neutral system to select which persons, property, or vehicles will be screened during an administrative or special needs search. Random selection for screening helps to ensure that selection authority is not arbitrarily or discriminatorily exercised.

Regional Security Inspector (RSI) – A TSA employee who is the principal technical specialist within OSO at the national level for compliance oversight activities in aviation, cargo, or surface transportation. The Surface RSI serves as liaison between OSO and large freight rail corporations whose operations are multi-regional or national in scope.

Screening - A search or appraisal of a person, place, document or thing, with or without assisting technologies, to determine compliance with TSA standards, regulations and applicable laws in order to detect a threat.

Screening Checkpoint - A screening location at the entry to a secure or other area of a transportation facility or public conveyance.

Screening of Passengers by Observation Technique (SPOT) Program - SPOT is a behavior observation and analysis program that detects behaviors and activities that deviate from an established environmental baseline. Individuals whose behaviors meet or exceed predetermined thresholds are referred for additional screening or law enforcement intervention.

WARNING: This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation.

Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.

Search – An examination or inspection conducted in accordance with the Fourth Amendment of a person's body, property, conveyance, or other area where the person would have a reasonable expectation of privacy.

Secure Area – Any area of a transportation facility for which access is restricted and controlled in some manner, to include but not limited to: sterile, secured, and air operations areas of airports.

Security Identification Display Area (SIDA) – A portion of an airport, specified in the airport security program, in which security measures are carried out. This area includes the secured area and may include other areas of the airport.

Senior Leadership – For purposes of this SOP, Senior Leadership consists of the Administrator, Deputy Administrator, Chief of Staff, Chief Counsel, Assistant Administrators and their Deputies and designees.

Sensitive Security Information (SSI) – Information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would constitute an unwarranted invasion of privacy, reveal trade secrets, disclose privileged or confidential information obtained from any person, or be detrimental to the security of transportation.

Special Events Assessment Rating (SEAR) - DHS leads the overall Special Events Assessment Rating (SEAR) process for the federal government. Co-chairs of the Special Events Work Group, which represents 50+ other federal agencies, work through a risk assessment methodology of special events reported through an annual data evaluation that takes into consideration the numerous types of threats, vulnerabilities, and potentially adverse consequences associated with each event. The result is assigned a SEAR level 1 through 5 designation that is used to help determine the level of federal awareness of and support given to the event.

Special Needs Search - A search conducted without a warrant and in furtherance of a special governmental need, beyond the ordinary needs of law enforcement. In the context of transportation security, special needs searches are designed to mitigate the risk to the public posed by the introduction of threats into the transportation system.

Stakeholder - Any private or public entity responsible for the operation, maintenance, and/or security of a transportation mode, system, or venue.

Sterile Area – A portion of an airport, defined in the airport security program, that provides individuals access to boarding aircraft and to which the access generally is controlled by TSA or by an aircraft operator under 49 CFR part 1544 or a foreign air carrier under 49 CFR part 1546, through the screening of persons and property.

Supervisory Transportation Security Officer (STSO) – The individual who directly supervises TSOs and the screening process. It may also refer to an LTSO who has been designated to perform STSO functions.

Threat Items – Any potentially hazardous items that pose a risk to transportation security, such as explosives, incendiaries, and items that could be used as weapons or otherwise transformed into a threat.

Toxic Inhalation Hazard (TIH) - Under the Hazardous Materials Regulations (49 CFR 171-180), TIH materials are gases or liquids that are known or presumed on the basis of tests to be so toxic to humans as to pose a hazard to health in the event of a release during transportation. Movement of large quantities of TIH materials by rail in proximity to population centers warrants special consideration and attention. These materials have the potential of causing significant numbers of fatalities and injuries if intentionally released in an urban environment.

Transportation Access Area – In the DOP, the designated area to which access is controlled by TSA through the screening of individuals and/or property.

WARNING: This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation.

Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.

Transportation Security Inspector (TSI) - A specially-trained TSA employee who conducts security assessments of transportation systems, works with transit officials to enhance the security of their systems, provides technical assistance for security, and conducts regulatory inspections. TSIs provide domain expertise, assess vulnerabilities and make recommendations to improve aviation security.

Transportation Security Inspector - Cargo or Multimodal Canine Handler - A Transportation Security Inspector who is a handler for an explosives detection canine. The canine team can screen air cargo, and search aircraft, vehicles, air operations areas, transit stations, and other transportation facilities.

Transportation Security Officer (TSO) – An individual who is trained, qualified, and authorized in accordance with applicable TSA standards and directives to screen individuals, accessible property, identification documents, and/or checked baggage for the presence of explosives, incendiaries, weapons, or other threats or threat items.

Transportation Security Specialist - Explosives (TSS-E) – A TSA employee specifically trained to determine if property is, or contains an improvised explosive device (IED), explosive, or IED components.

Transportation Venue - A building, structure, or location that facilitates the movement of passengers or goods in the transportation system.

TSA Certified Canine - Canine teams that have been certified to TSA standards or canine programs that have been approved by TSA.

TSA Management - The Federal Security Director (FSD)/ Supervisory Air Marshal in Charge (SAC) or his or her designee, who has overall responsibility for the VIPR.

Visible Intermodal Prevention and Response (VIPR) - TSA's deployment of specialized teams to augment the security of any mode of transportation. VIPR teams may comprise any asset of the U.S. Department of Homeland Security (DHS), including, FAMs, TSIs, cargo or multimodal canine detection teams, and detection technology.

WebEOC - The document repository and program management system used by the JCC to track all VIPR deployments.

1.10. ACRONYMS

AAR	After Action Report
AD	Area Director
AFSD	Assistant Federal Security Director
AFSD-I	Assistant Federal Security Director-Inspections
AFSD-LE	Assistant Federal Security Director-Law Enforcement
AFSD-S	Assistant Federal Security Director-Screening
AOA	Air Operations Area
ASAC	Assistant Supervisory Air Marshal in Charge
ASR	Activity Summary Report
BDO	Behavior Detection Officer
CBRNE	Chemical Biological Radiological Nuclear Explosive
CCTV	Closed Circuit Television

WARNING: This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.

CFR	Code of Federal Regulations
DAP	Direct Access Point
DFSD	Deputy Federal Security Director
DHS	Department of Homeland Security
DOP	Deployment Operations Plan
DOT	Department of Transportation
ETD	Explosive Trace Detection
FAM	Federal Air Marshal
FSD	Federal Security Director
HAZMAT	Hazardous Materials
HHMD	Hand-Held Metal Detector or "hand-wand"
HMR	Hazardous Materials Regulations
ID	Identification
IED	Improvised Explosive Device
JCC	Joint Coordination Center
LEO	Law Enforcement Officer
LTSO	Lead Transportation Security Officer
MANPADS	Man Portable Air Defense Systems
MMTD	Multi-Mode Threat Detector
NDO	National Deployment Office
NDF	National Deployment Force
NEDCTP	National Explosives Detection Canine Training Program
NSSE	National Special Security Event
OCC	TSA Office of Chief Counsel
OD	Operations Directive
OSO	Office of Security Operations
OLE	Office of Law Enforcement
OSPIE	Office of Security Policy and Industry Engagement
OTR	Operations Tracking Report
PSC	Passenger Screening Canine
PRND	Preventive Radiological Nuclear Detection
RD	Regional Director
RSI	Regional Security Inspector
SAC	Supervisory Air Marshal in Charge

WARNING: This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.

Revision: 5

Date of Revision: May 1, 2015

Implementation Date: May 1, 2015

VIPR SOP

SEAR	Special Events Assessment Rating
SFAM	Supervisory Federal Air Marshal
SIDA	Security Identification Display Area
SOP	Standard Operating Procedures
SPOT	Screening of Passengers by Observation Techniques
SSI	Sensitive Security Information
STSO	Supervisory Transportation Security Officer
TIH	Toxic Inhalation Hazard
TSA	Transportation Security Administration
TSI	Transportation Security Inspector
TSI-A	Transportation Security Inspector - Aviation
TSI-C	Transportation Security Inspector - Cargo
TSI-S	Transportation Security Inspector - Surface
TSOC	Transportation Security Operations Center
TSO	Transportation Security Officer
TSS-E	Transportation Security Specialist-Explosives (formerly Bomb Appraisal Officer (BAO))
TWIC	Transportation Workers Identification Credential
VBIED	Vehicle Borne Improvised Explosive Device
VIPR	Visible Intermodal Prevention and Response
WebEOC	Web Emergency Operations Center

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

**Chapter
2**

2. VIPR CAPABILITIES AND VENUES

2.1. CAPABILITIES

- A. This section describes approved capabilities that can be conducted during a VIPR operation under TSA VIPR authorities within the transportation modes. VIPR capabilities are grouped into screening capabilities, either active or passive, as well as other capabilities.

- B. (b)(3):49 U.S.C. § 114(r)

2.2. SCREENING CAPABILITIES

(b)(3):49 U.S.C. § 114(r)

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

(b)(3):49 U.S.C. § 114(r)

2.3. TRANSPORTATION VENUES

2.3.1. COMMERCIAL AIRPORT VENUES

- A. A commercial airport provides scheduled commercial service, and the airport and the air carriers are governed by TSA security regulations. Commercial airport venues do not include stand-alone General Aviation (GA) airports which do not have scheduled commercial service. A commercial airport may have a GA facility (commonly referred to as a Fixed Base Operator (FBO)) or an area within the commercial airport's property where GA operators conduct business. The GA area is generally separate from the commercial area of the airport but it is subject to the airport's Security Program.
- B. Different VIPR capabilities may be deployed at a commercial airport with the agreement of the airport operator. Commercial airports are subject to Transportation Security Regulations that do not typically pertain to GA airports. See Chapter 5 VIPR Other Capabilities.

2.3.2. SURFACE AND OTHER TRANSPORTATION VENUES

- A. In this SOP, surface and other transportation venues include Mass Transit, Freight Rail, Highway/Critical Infrastructure, Maritime, Pipeline, and General Aviation (GA) airports. For purposes of applying VIPR screening capabilities, GA airports that are not located as part of a commercial airport are considered in this category. For VIPR deployments, stand-alone GA airports demonstrate greater operational similarities to deployments in the other transportation modes than to commercial aviation.
- B. General Aviation encompasses all civil aviation except for scheduled passenger and cargo service and military aviation. GA airports are not required to comply with the federal airport security rules in 49 CFR 1542 which govern the operations at a commercial airport. TSA has not required GA airports to implement security measures except for those facilities located within the Washington, D.C. Airspace Restricted Zone.

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

2.3.3. FREIGHT RAIL OPERATIONS

- A. Planning for a VIPR operation on any freight rail property requires prior approval at the freight rail operator's corporate level, including operations at shared rail facilities. The freight rail industry requires the TSA Surface Regional Security Inspector (RSI) serve as liaison with the freight rail corporate stakeholder. Field personnel must contact the respective Surface RSI(s) who will facilitate communications between TSA and the respective corporate freight rail organization(s).
- B. (b)(3):49 U.S.C. § 114(r)
- C. After concurrence from the stakeholder, continue with the regular planning process including operational submission of an OTR to the JCC.
- D. Refer to JCC iShare for contact information for the Surface RSIs aligned with OSO regions and their respective corporate freight rail responsibility.

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

**Chapter
3**

3. VIPR ACTIVE SCREENING CAPABILITIES

3.1. SCREENING INDIVIDUALS

3.1.1. SCREENING INDIVIDUALS AT COMMERCIAL AIRPORT VENUES

(b)(3):49 U.S.C. § 114(r)

3.1.2. INDIVIDUALS AT SURFACE AND OTHER TRANSPORTATION VENUES

(b)(3):49 U.S.C. § 114(r)

3.2. SCREENING PROPERTY

3.2.1. SCREENING PROPERTY AT COMMERCIAL AIRPORT VENUES

(b)(3):49 U.S.C. § 114(r)

3.2.2. SCREENING PROPERTY AT SURFACE AND OTHER TRANSPORTATION VENUES

(b)(3):49 U.S.C. § 114(r)

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

3.3. SCREENING VEHICLES

(b)(3):49 U.S.C. § 114(r)

3.3.1. ETD SCREENING OF VEHICLES

(b)(3):49 U.S.C. § 114(r)

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

3.3.2. SEARCH OF VEHICLES

(b)(3):49 U.S.C. § 114(r)

3.4. VIPR ACTIVE SCREENING PROCEDURES

(b)(3):49 U.S.C. § 114(r)

3.4.1. SCREENING EQUIPMENT

(b)(3):49 U.S.C. § 114(r)

3.4.2. SIGNS AND NOTIFICATION

- A. Whenever VIPR operations include active screening of individuals, property, or vehicles, the VIPR Team Leader must ensure approved signs are posted, clearly stating that individuals and property are subject to search.
- B. Signs and notification must be described in the VIPR DOP in compliance with the following:

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

- Signs must be prominently displayed to provide adequate notice to individuals before they enter the screening location. The notice should be provided in such a manner as to allow persons the opportunity to avoid the search by choosing not to enter the location.
- The notice should provide warning that once the screening process has begun, screening must be completed.
- Approximate dimensions and specific location of signs must be described in the VIPR DOP.
- When the VIPR DOP includes screening of persons and/or property, the signs must indicate "All persons and property are subject to search beyond this point".
- When the VIPR DOP includes screening of vehicles, signs must indicate "Vehicle inspection ahead. All vehicles are subject to search beyond this point".

3.4.3. INITIATION AND WITHDRAWAL FROM SCREENING

- A. A screening activity may be initiated once an individual has elected to attempt entry into a sterile or secure area of the transportation venue, or elected to attempt to board an aircraft, bus, train, or other public conveyance.

(b)(3):49 U.S.C. § 114(r)

3.4.4. SUPERVISOR/LEO NOTIFICATION

(b)(3):49 U.S.C. § 114(r)

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

Revision: 5

Date of Revision: May 1, 2015

Implementation Date: May 1, 2015

VIPR SOP

(b)(3):49 U.S.C. § 114(r)

3.4.5. DISCOVERY OF SUSPECTED EXPLOSIVES OR EXPLOSIVE MATERIAL

(b)(3):49 U.S.C. § 114(r)

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

**Chapter
4**

4. VIPR PASSIVE SCREENING CAPABILITIES

4.1. GENERAL

TSA assets can deploy capabilities to assess individuals, property, and vehicles for the presence of explosives and explosive materials before entering any transportation mode or conveyance without impeding the individuals. These inspection measures can be conducted at any transportation venue or on a conveyance.

4.2. VISUAL INSPECTIONS

(b)(3):49 U.S.C. § 114(r)

4.3. PATROLS

4.3.1. PERIMETER

(b)(3):49 U.S.C. § 114(r)

4.3.2. ON BOARD PUBLIC CONVEYANCE /VESSEL

(b)(3):49 U.S.C. § 114(r)

4.3.3. CRITICAL INFRASTRUCTURE

(b)(3):49 U.S.C. § 114(r)

WARNING: This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.

Revision: 5
Date of Revision: May 1, 2015
Implementation Date: May 1, 2015

VIPR SOP

4.3.4. MAN PORTABLE AIR DEFENSE SYSTEM (MANPADS)

(b)(3):49 U.S.C. § 114(r)

4.3.5. SURVEILLANCE/COUNTER-SURVEILLANCE

(b)(3):49 U.S.C. § 114(r)

4.3.6. BEHAVIOR RECOGNITION

(b)(3):49 U.S.C. § 114(r)

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

4.4. EXPLOSIVES DETECTION CANINE TEAMS

(b)(3):49 U.S.C. § 114(r)

4.5. AIRCRAFT SECURITY SWEEP

(b)(3):49 U.S.C. § 114(r)

4.6. ID VERIFICATION

(b)(3):49 U.S.C. § 114(r)

4.7. TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC)

(b)(3):49 U.S.C. § 114(r)

WARNING: This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.

Revision: 5

Date of Revision: May 1, 2015

Implementation Date: May 1, 2015

VIPR SOP

(b)(3):49 U.S.C. § 114(r)

B. Further information can be found at:

<https://ishare.tsa.dhs.gov/offices/intelligence/pages/vettingoperationsdivision.aspx>

TWIC verification will be conducted in accordance with 49 CFR 1570.1, 1570.3, 1570.5, 1570.7, 1570.9(a), 1570.11, 1572.19(c) and the Coast Guard Law Enforcement Informational Bulletin *Procedures for Handling Seized TWICs* of June 30, 2009. Refer to JCC VIPR iShare for supporting documents.

C. If TSA personnel are presented with a TWIC card by either a commercial vehicle operator or during the course of an investigation being conducted by a state, local or Federal Law Enforcement Officer, the following actions should be taken.

(b)(3):49 U.S.C. § 114(r)

4.8. PREVENTIVE RADIOLOGICAL NUCLEAR DETECTION (PRND)

(b)(3):49 U.S.C. § 114(r)

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

Revision: 5

Date of Revision: May 1, 2015

Implementation Date: May 1, 2015

VIPR SOP

(b)(3):49 U.S.C. § 114(r)

4.8.1. RADIATION DETECTION EQUIPMENT

(b)(3):49 U.S.C. § 114(r)

4.8.2. OPERATING PROCEDURES

(b)(3):49 U.S.C. § 114(r)

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

4.8.3. PRE-DEPLOYMENT PROCEDURES

(b)(3):49 U.S.C. § 114(r)

4.8.4. DEPLOYMENT PROCEDURES

(b)(3):49 U.S.C. § 114(r)

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

(b)(3):49 U.S.C. § 114(r)

4.8.5. SECONDARY SCREENING RESPONSE PROCEDURES

(b)(3):49 U.S.C. § 114(r)

4.8.6. ADJUDICATION PROCEDURES

(b)(3):49 U.S.C. § 114(r)

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

Revision: 5

Date of Revision: May 1, 2015

Implementation Date: May 1, 2015

VIPR SOP

(b)(3):49 U.S.C. § 114(r)

~~**WARNING:** This record contains sensitive security information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. government agencies, public disclosure governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

