



**Transportation  
Security  
Administration**

May 7, 2018

**3600.1**

Case Number: 2013-TSFO-01016

Edward Hasbrouck  
The Identity Project  
1736 Franklin St 9th Floor  
Oakland, CA 94612

Dear Mr. Hasbrouck:

On May 23, 2017, you appealed the TSA's response to Freedom of Information Act (FOIA) request 2013-TSFO-01016 for "copies of all records pertaining to any 'TSOC ID Verification Report' or similar log, record, report, or e-mail message indicating the numbers of ID checks, numbers of ID checks resulting in a 'not verified' outcome, or numbers of checks resulting in a 'denied' outcome, including but not limited to any aggregated reports for these quantities over any time periods, any guidelines or instructions for the preparation of such reports or the categorization of events or outcomes for reporting purposes, and any e-mail messages mentioning such reports or reporting protocols." Specifically, you appealed, 1) the "no records" response to any email messages or other records pertaining to the responsive reports; 2) the format of the records provided, and 3) the "no records" response to file and file system data and metadata. In our October 20, 2017, response to your appeal, you were notified that the TSA was affirming the format of the records provided and the "no records" response for file and file system data and metadata, but we were remanding your initial request back to the FOIA Branch to conduct a search for any of the email messages or other records pertaining to the responsive records.

An additional search was conducted within TSA and the Standard Operating Procedure in-place at the time the reports were created is being released to you in part. Portions not released are being withheld pursuant to the Freedom of Information Act, 5 U.S.C. § 552(b)(3). Please refer to the Applicable Exemptions list at the end of this letter that identifies the authority for withholding the exempt material, which is indicated by a mark appearing in the block next to the exemption. An additional enclosure with this letter explains these exemptions in more detail. No email messages pertaining to the responsive records were located. The email account utilized to prepare and distribute the TSOC reports was centralized into the National Transportation Vetting Center email account, and all emails created during that time associated with the TSOC reports already released to you have been deleted.

The rules and regulations of the Transportation Security Administration applicable to Freedom of Information Act requests are contained in the Code of Federal Regulations, Title 6, Part 5. They are published in the Federal Register and are available for inspection by the public.

Fees

There are no fees associated with processing this request because the fees incurred do not exceed the minimum threshold necessary for charge.

### Administrative Appeal

In the event that you wish to appeal our remanded response, an administrative appeal may be made in writing to Kimberly Walton, Assistant Administrator, Office of Civil Rights & Liberties, Ombudsman and Traveler Engagement (CRL/OTE), Transportation Security Administration, 701 South 12<sup>th</sup> Street, West Building, W3-110S, Arlington, VA 20598-6033. Your appeal **must be submitted within 90 days** from the date of this determination. It should contain your FOIA request number and, to the extent possible, the reasons why you believe the initial determination should be reversed. In addition, the envelope in which the appeal is mailed should be prominently marked "FOIA Appeal." Please note that the Assistant Administrator's determination of the appeal will be administratively final.

Additionally, you have the right to seek dispute resolution services from the Office of Government Information Services (OGIS) which mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. If you are requesting access to your own records (which is considered a Privacy Act request), you should know that OGIS does not have the authority to handle requests made under the Privacy Act of 1974. You may contact OGIS as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001; e-mail at [ogis@nara.gov](mailto:ogis@nara.gov); telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5796.

If you have any questions pertaining to your request, please feel free to contact the FOIA Branch at 1-866-364-2872 or 1-571-227-2300.

Sincerely,



Deborah O. Moore  
Acting FOIA Officer

Summary:

Number of Pages Released in Part or in Full: **40**

Number of Pages Withheld in Full: **0**

Number of Pages Referred: **0**

### **APPLICABLE EXEMPTIONS FREEDOM OF INFORMATION ACT AND/OR PRIVACY ACT**

#### **Freedom of Information Act (5 U.S.C. 552)**

☐ (b)(1) ☐ (b)(2) ☒ (b)(3) ☐ (b)(4) ☐ (b)(5) ☐ (b)(6)

☐ (b)(7)(A) ☐ (b)(7)(B) ☐ (b)(7)(C) ☐ (b)(7)(D) ☐ (b)(7)(E) ☐ (b)(7)(F)

Enclosures

FREEDOM OF INFORMATION ACT  
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

Transportation Security Administration (TSA) FOIA Branch applies FOIA exemptions to protect:

Exemptions

**Exemption (b)(1):** Records that contain information that is classified for national security purposes.

**Exemption (b)(2):** Records that are related solely to the internal personnel rules and practices of an agency.

**Exemption (b)(3):** Records specifically exempted from disclosure by Title 49 U.S.C. Section 114(r), which exempts from disclosure Sensitive Security Information (SSI) that “would be detrimental to the security of transportation” if disclosed.

**Exemption (b)(4):** Records that contain trade secrets and commercial or financial information obtained from a person that is privileged or confidential.

**Exemption (b)(5):** Inter- or intra-agency records that are normally privileged in the civil discovery context. The three most frequently invoked privileges are the deliberative process privilege, the attorney work-product privilege, and the attorney-client privilege:

- Deliberative process privilege – Under the deliberative process privilege, disclosure of these records would injure the quality of future agency decisions by discouraging the open and frank policy discussions between subordinates and superiors.
- Attorney work-product privilege – Records prepared by or at the direction of a TSA attorney.
- Attorney-client privilege – Records of communications between an attorney and his/her client relating to a matter for which the client has sought legal advice, as well as facts divulged by client to attorney and any opinions given by attorney based on these.

**Exemption (b)(6):** Records that contain identifying information that applies to a particular individual when the disclosure of such information “would constitute a clearly unwarranted invasion of personal privacy.” This requires the balancing of the public’s right to disclosure against the individual’s right to privacy.

**Exemption (b)(7)(A):** Records or information compiled for law enforcement purposes, but only to the extent that production of such law enforcement records or information...could reasonably be expected to interfere with law enforcement proceedings.

**Exemption (b)(7)(C):** Records containing law enforcement information when disclosure “could reasonably be expected to constitute an unwarranted invasion of personal privacy” based upon the traditional recognition of strong privacy interests ordinarily appropriated in law enforcement records.

**Exemption (b)(7)(E):** Records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

**Exemption (b)(7)(F):** Records containing law enforcement information about a person, in that disclosure of information about him or her could reasonably be expected to endanger his or her life or physical safety.

**U.S. Department of Homeland Security  
Transportation Security Administration**



**Transportation  
Security  
Administration**

**Office of Intelligence and Analysis (OIA)**

**Vetting Operations Division (VOD)**

**Identity Verification Call Center Branch  
(IVCCB)**

**Standard Operating Procedure (SOP)**

**Version 2.1**

October 7, 2013

~~The Transportation Security Administration (TSA) intends that TSA Management and contractors use and implement these standard operating procedures in carrying out their functions as it is related to the various program business processes. 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).~~

~~**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.~~

~~SENSITIVE SECURITY INFORMATION~~**REVISION HISTORY**

Revision Date	Version	Modified By	Comments
06/30/2008	1.0	Ron Juhl	Original IVCC SOP
05/01/2012	2.0	T. Cossairt, M. Ratchford, K. Flanagan, T. Holloman	Added call handling, special circumstances, process assistance, and Known or Suspected Terrorist procedures following reorganization and move from OSO to OIA.
10/07/2013	2.1	T. Cossairt, M. Ratchford, T. Holloman, B. Sapp, C. Guin, A. Acker	See SOP v2.1 Summary of Revisions spreadsheet

As Defined by IVCC	
Revision schedule:	As needed
Vital Record:	Yes
Key Program Document:	Yes

~~SENSITIVE SECURITY INFORMATION~~**TABLE OF CONTENTS**

<b>1</b>	<b>IVCC SOP OVERVIEW .....</b>	<b>1</b>
1.1	Purpose.....	1
1.2	Prerequisites.....	1
1.3	Definitions .....	2
1.4	Scope.....	3
1.5	Process Flow Diagram.....	4
1.6	Roles and Responsibilities .....	4
1.7	Tools .....	5
1.8	Policy .....	5
1.9	Related Topics .....	6
<b>2</b>	<b>IDENTITY VERIFICATION PROCEDURE .....</b>	<b>7</b>
2.1	Call Opening.....	7
2.2	Conducting the Database Search .....	9
2.2.1	Additional Search Option to Locate Young Adults.....	10
2.3	Verification Procedure for Foreign Nationals .....	11
2.3.1	ATS-P or TECS Record Indicates Need for Escalation.....	11
2.3.1.1	Non-Actionable Derogatory Information .....	11
2.3.1.2	Actionable Derogatory Information.....	12
2.4	Verified/Unverified Determinations .....	13
2.4.1	Verified .....	13
2.4.2	Unverified .....	13
2.4.3	WebEOC Data Entry.....	15
2.4.3.1	Verified Passengers.....	15
2.4.3.2	Unverified Passengers.....	15
2.4.4	Call Backs .....	17
2.4.5	Narratives.....	18
2.5	Special Circumstances .....	19
2.5.1	Passengers under 18 Years Old.....	19
2.5.2	Passengers (b)(3) 49 U.S.C. § .....	19
2.5.3	Third Party Verification .....	19
2.5.4	Passenger Requires a Translator .....	20
2.5.5	Passengers Escorted by Law Enforcement (Bounty Hunter Scenario).....	21
2.5.6	Passengers under U.S. Marshals Service (USMS) Protection .....	21
2.5.7	Repeat Offenders .....	22
2.5.8	Suspicion of Fraud .....	22
2.5.9	COI Form in Circulation.....	23
2.5.10	Suspected Process Integrity Violations.....	23
2.5.11	Intoxicated Passengers .....	23
2.5.12	Uncooperative Passengers .....	24
2.5.13	Voluntary Withdrawals.....	24

~~**SENSITIVE SECURITY INFORMATION**~~

2.5.14	Gate Passes.....	25
2.5.15	Information Gathering Calls .....	25
2.5.16	TSA Airport Employees .....	26
2.5.17	Other Airport Employees.....	26
2.5.18	Declaration of Nationality (DON) .....	26
2.5.19	Large Groups of Foreign Nationals and School Groups.....	26
2.5.20	Military Orders.....	26
2.5.21	Re-Entry.....	27
2.6	Process Assistance Calls (formerly “SOP” calls).....	27
2.7	Watch List Checks .....	29
2.7.1	Requests for Watch List Checks in the Case of a Substantial Mismatch .....	29
2.7.2	Requests for Watch List Checks in the Case of a Complete Mismatch.....	30
2.7.3	No-Fly and Selectee Watch List Matches.....	30
2.8	Events.....	31
2.9	Known or Suspected Terrorist (KST) Report .....	32
<b>APPENDIX A</b>	<b>Acronyms .....</b>	<b>A-1</b>
<b>APPENDIX B</b>	<b>Database Search Rules .....</b>	<b>B-3</b>

**LIST OF TABLES**

Table 1-1: Definitions .....	2
Table 1-2: Roles and Responsibilities.....	4

**LIST OF FIGURES**

Figure 2-1: WebEOC Screen to Create IVRN .....	7
Figure 2-2: (b)(3) 49 U.S.C. § 114(n) .....	9
Figure 2-3: Sample Cisco Agent Desktop with Duration of Call and Wait Time .....	13
Figure 2-4: WebEOC Call Data Section.....	15
Figure 2-5: WebEOC PAX Info Provided on Form Section .....	16
Figure 2-6: WebEOC PAX Response Section.....	17
Figure 2-7: WebEOC Case Disposition Section.....	17
Figure 2-8: Process Assistance Checkbox .....	28
Figure 2-9: SF KST Log .....	33

## 1 IVCC SOP OVERVIEW

### 1.1 Purpose

Existing Transportation Security Administration (TSA) screening procedures and airline security programs require Travel Document Checker (TDC) qualified Transportation Security Officers (TSO) and air carriers to verify the identity of passengers over the age of 18 before allowing the passengers to enter the sterile area of an airport. Under these procedures, passengers are required to produce acceptable identification to a TSA Screening Representative (TSR) before proceeding to the screening checkpoint. Passengers who do not produce acceptable identification and who fail to assist TSA personnel in adequately verifying their identity will be denied entry.

The purpose of this procedure is to prevent known or suspected terrorists from entering the sterile area of an airport and boarding an aircraft or to prevent them from accessing the sterile area in order to collect information that may assist in conducting terrorist activities.

The TSA Identity Verification Call Center (IVCC) provides assistance to passengers and other individuals at U.S. airports who fail to present acceptable identity verification documentation to a TSR but are willing to cooperate by providing personal identity information and answering a series of questions. This SOP establishes procedures for use by the IVCC to:

- Verify the identity of individuals attempting to gain access to an airport sterile area or board an aircraft through a TSA screening checkpoint when that individual does not present acceptable identification documentation.
- Confirm that in the case of a significant mismatch between the name on the boarding pass and the name on the acceptable ID, that the passenger is not a match to the Selectee or No Fly Watch List.

### 1.2 Prerequisites

The following list of training and documents should be completed prior to reviewing this SOP.

- N/A



## 1.3 Definitions

Table 1-1: Definitions

Term	Definition
Acceptable Forms of ID	Forms of identity documentation that allow a passenger/gate pass holder to proceed to the screening checkpoint. These are listed in the TDC SOP section entitled <i>Acceptable Forms of Photo ID</i> .
(b)(3) 49 U.S.C. § 114(r)	
Certification of Identity (COI)	A form provided to the passenger by the TSR granting permission for TSA to review personally identifiable information (PII) in order to assist in verifying the individual's identity.
Consistent	The information provided by the passenger is an exact match or reasonably close to the information in various databases.
Event	A situation in which the IVCC has determined that an individual is unverified, and a TSA employee other than the Federal Security Director (FSD) or designee has allowed the individual to enter the screening checkpoint or the sterile area of an airport without a LEO interview or without receiving acceptable, previously undisclosed identity documentation.
Identification Documentation	Documents that passengers and gate pass holders may present to the TSR in order to prove identity and proceed to the screening checkpoint. This includes acceptable and other forms of ID.
Identity Verification	The process of confirming information supplied by an individual (b)(3) 49 U.S.C. § 114(r)
Inconsistent	The information provided by the passenger is significantly different from the information in various databases.
Law Enforcement Officer (LEO)	A sworn employee of a government entity (Federal, to include U.S. military police and U.S. Capitol police, State, territorial, tribal, and local, to include rail police officers), with full power of arrest, who is trained and commissioned to enforce the public criminal laws of the jurisdiction(s) in which he/she is commissioned.
Sterile Area	A portion of an airport, defined in the airport security program, that provides passengers access to board aircraft and to which the access is generally controlled by TSA through the screening of persons and property.

Term	Definition
TSA Screening Representative (TSR)	The TSA employee at an airport filling the TDC role who has been designated to: 1) review identification documentation, determine if IVCC assistance is needed to assist in verifying identity when individuals fail to produce acceptable identification documentation; and 2) determine if a mismatch between the name on a boarding pass and the name on acceptable identification documentation is significant enough to contact the IVCC for a Watch List check. Employees filling the role may include any qualified Lead Transportation Security Officer (LTSO), Supervisory Transportation Security Officer (STSO), Transportation Security Officer (TSO), Behavior Detection Officer (BDO), Screening Passengers by Observation Technique (SPOT) Transportation Security Manager (STSM), Transportation Security Manager (TSM), or Coordination Center Officer (CCO).
Watch List	The No-Fly and Selectee List components of the Terrorist Screening Database maintained by the Terrorist Screening Center.
WebEOC	System used to 1) generate a unique Identity Verification Reference Number (IVRN) for verified and unverified passengers 2) log unverified passengers and 3) view the Known or Suspected Terrorist (KST) web board.

#### 1.4 Scope

The procedures in this IVCC SOP are designed to guide the Security Assistants (SA), Supervisory Security Assistants (SSA), and Section Chief within the Office of Intelligence and Analysis, Vetting Operations Division, in verifying identities, coordinating watch list matching, and handling events. SSAs should use their professional judgment, experience, and training to handle any situations not covered in the SOP.

Revisions to and enforcement of SOPs for the following groups are out of scope of this SOP:

- FSDs and their designees
- Transportation Security Officers
- Law Enforcement Officers
- Secure Flight Analysts

In all cases, the final decision to allow/deny the passenger access to the screening checkpoint belongs to the FSD. The FSD or FSD-appointed designee may allow a passenger unverified by the IVCC to proceed to the screening checkpoint.

## 1.5 Process Flow Diagram

The current IVCC process flows are located in the Supervisor folder on iShare [here](#).

## 1.6 Roles and Responsibilities

The IVCC includes three roles filled by government full-time equivalents (FTE). The following table describes the responsibilities associated with each role.

**Table 1-2: Roles and Responsibilities**

Role	Responsibilities
Branch Manager	<ul style="list-style-type: none"> <li>▪ Maintain overall supervisory and reporting responsibility for the IVCC</li> <li>▪ Provide strategic guidance and finalize policy and procedural revisions</li> <li>▪ Attend OIA leadership briefings</li> <li>▪ Finalize all staffing decisions</li> </ul>
Section Chief (formerly Transportation Security Specialist or TSS)	<ul style="list-style-type: none"> <li>▪ Maintain supervisory and reporting responsibility for the IVCC</li> <li>▪ Review and approve policy and procedural revisions</li> <li>▪ Attend OIA leadership briefings</li> <li>▪ Conduct or supervise all staffing activities and make staffing decisions</li> </ul>
Supervisory Security Assistant (SSA)	<ul style="list-style-type: none"> <li>▪ Supervise and coach SAs</li> <li>▪ Handle call escalations</li> <li>▪ Provide final verified/unverified determination</li> <li>▪ Answer callback line and document final disposition</li> <li>▪ Escalate events to Transportation Security Operations Center (TSOC) and OIA leadership</li> <li>▪ Compile and distribute reports</li> <li>▪ Monitor quality of SA documentation and customer service</li> <li>▪ Create and maintain schedules</li> </ul>
Security Assistant (SA)	<ul style="list-style-type: none"> <li>▪ Answer incoming calls from TSRs seeking assistance with identity verification and watch list matching</li> <li>▪ Search databases</li> <li>▪ Complete Call Data Sheets</li> <li>▪ Enter information into WebEOC</li> <li>▪ Generate IVRN</li> <li>▪ Answer callback line (as needed)</li> <li>▪ Compile reports (as needed)</li> </ul>

## 1.7 Tools

IVCC personnel currently use the following tools:



## 1.8 Policy

The IVCC SOP complies with the following policies:

- Secure Flight Final Rule – Section 1560.105
- Privacy Impact Assessment (PIA) for the TSA Operations Center Incident Management System
- CPB requirements for user permissions and electronic privacy acknowledgments for ATS-P and TECS databases

In addition, the IVCC has a “no information out” policy in order to maintain the integrity of the IVCC process. The IVCC prohibits sharing passengers’ personal information, procedures or technology associated with the verification process with anyone outside of VOD.

SAs may not disclose the following information to TSRs:

- The procedures, technology, or third party resources used to assist the IVCC in establishing the identity of passengers
- The results of a search other than the verbiage in the call script
- Whether or not the SA was able to locate a record
- The accuracy or inaccuracy of a passenger’s responses, or
- Any other information that may jeopardize the integrity of the IVCC process, provide passengers with increased opportunity to gain understanding of processes, methods and techniques, unnecessarily increase passengers’ ability to interpret the purposes behind questions being asked or other information gathering and dissemination practices that may go beyond a person’s “need to know.”

Additionally SAs may not elaborate on a passenger’s information provided in the database.

SSAs may determine that an FSD or designee, airport coordination center, or other TSA management representative has a need to know and provide additional details on passengers on a case-by-case basis.

## 1.9 Related Topics

The following SOPs help provide a comprehensive view of identity verification policies and procedures:

- Travel Document Check SOP
- Screening Management SOP

## 2 IDENTITY VERIFICATION PROCEDURE

This procedure describes the primary function of the IVCC, to perform identity verification for passengers who arrive at the screening checkpoint without acceptable identification documentation.

*Note: If a standard call (one that does not involve a third party) reaches 10 minutes, notify the SSA who may assist in the search.*

In all cases, if the SA has any questions or concerns, the SA should put the caller on hold and seek guidance from an SSA.

### Audience:

- SA
- SSA

### Steps:

#### 2.1 Call Opening

1. Answer the incoming call and state, "Hello, this is the Identity Verification Line – my name is (First Name, First Initial of Last Name). May I have your name, title and airport code?"
2. Create a record in WebEOC for every call. In the WebEOC Create New Record Display, click Create New Record and click OK.

ID	Date Reported	Recorder
725555	03/14/2012 13:30:13	





**Figure 2-1: WebEOC Screen to Create IVRN**

- If WebEOC is down:
    - a. Close and re-open WebEOC
    - b. If WebEOC is still not working for the SA, another SA may assist and generate the IVRN
    - c. If WebEOC is down for everyone, proceed with the identity verification, and call the airport with the IVRN when it is back up
3. Complete the Call Data section of the Call Data Sheet including:
    - Date
    - Time (start of call)
    - Operator (SA)
    - Airport POC
    - Title (e.g., Lead Transportation Security Officer (LTSO), Supervisory Transportation Security Officer (STSO), Behavior Detection Officer (BDO))
    - Airport Code
    - Contact #
  4. Ask the TSR to confirm that the passenger has completed the COI.
    - a. Typically, the passenger has completed the COI, and the call proceeds.
    - b. If the passenger has not signed the COI, you may wait for the COI to be signed if the passenger is available and able to sign quickly; otherwise, end the call, advise the airport POC to call back once the COI form is completed, and discard the incomplete Call Data Sheet in the SSI bin.
  5. Ask the TSR to confirm if the passenger has any documentation with his/her name on it. If necessary, suggest the TSR not make any assumptions regarding whether or not the information is valuable and allow you the opportunity to determine if the document is helpful in establishing the person's identity.
    - If the passenger does not have any acceptable documentation, ask the TSR to ask the reason and record in the Reason for no ID field.
    - If the TSR replies that any identity documentation is available for the individual:
      - Note the documentation under ID Presented.
      - If the documentation is actually sufficient per the TDC SOP, follow section 2.6 Process Assistance Calls.
  6. Ask the TSR for information to complete the PAX Info section:
    - M/F
    - Last, First and Middle Name
    - Alias (if needed)
    - Date of Birth (DOB)
    - (b)(3) 49 U.S.C. § 1114(e) - check if yes
    - Social Security Number (SSN) – Last four digits only
  7. Complete the Current Address section with the information on the COI provided by the TSR.



~~SENSITIVE SECURITY INFORMATION~~

## 2.2 Conducting the Database Search

1. Search  (b)(3):49 U.S.C. § 114(r)  (b)(3):49 U.S.C. § 114(r). If the database contains  (b)(3):49 U.S.C. § 114(r)  (b)(3):49 U.S.C. § 114(r) the individual, one or more records will be returned on the Results Page.
2. If the search returns no results, choose from among the following search options, and enter the information on the Call Data Sheet:

 (b)(3):49 U.S.C. § 114(r)

3. If the passenger is located, check the Base box on the Call Data Sheet next to whatever information helped locate the record.
4. If the passenger is still not located, proceed to the section Additional Search Option to Locate Young Adults, Foreign Nationals, or Unverified U.S. Citizens.

 (b)(3):49 U.S.C. § 114(r)



~~SENSITIVE SECURITY INFORMATION~~

5. A minimum amount of information is required to open the record:

(b)(3):49 U.S.C. § 114(r)

6. If the minimum matching information is met, click Comprehensive Report.
7. On the next screen, Reports Selection, click "Custom Comprehensive Report."
- 8.

(b)(3):49 U.S.C. § 114(r)

### 2.2.1 Additional Search Option to Locate Young Adults

The following procedure is intended to help locate a young adult's record in Accurint (or Clear). In this case you may use parent, guardian, or other relative in order to (b)(3):49 U.S.C. § 114(r). Do not ask the young adult any questions about the relative's record. The purpose of this procedure is to locate the young adult's record, not to generate challenge questions from a relative's record.

(b)(3):49  
U.S.C. §

1. Attempt to locate the young adult by a standard database search.
2. If the young adult cannot be found in Accurint by a standard search, (b)(3):49 U.S.C. § 114(r). If the relative's record is found (b)(3):49 U.S.C. § 114(r), you may open the relative's comprehensive report.
3. Hit Control F to search. Type the name of the young adult and hit Enter.
  - a. If the name is not found in the record:
    - i. You will receive a "no text" message.
    - ii. Close the record.
  - b. If the name is found in the record:
    - i. The search will direct you to the name and highlight it.
    - ii. By hitting next you may find the name multiple times with the Lexis ID or DOB attached. This can help you confirm if the passenger is the person listed.
    - iii. Use the name link to bring you to the passenger's record where you can ask questions from the passenger's comprehensive report, but only if you can verify an additional identifier in the record such as DOB or SSN to confirm you are in the correct record.

## 2.3 Verification Procedure for Foreign Nationals

The following procedure applies to foreign nationals who cannot be verified through an Accurant/Clear search.

(b)(3)-49 U.S.C. § 114(r)



### 2.3.1 ATS-P or TECS Record Indicates Need for Escalation

#### 2.3.1.1 Non-Actionable Derogatory Information

(b)(3)-49 U.S.C. § 114(r)



(b)(3);49 U.S.C. § 114(r)

### 2.3.1.2 Actionable Derogatory Information

IVCC defines actionable derogatory information as information identified in the passenger's ATS-P or TECS database record that may require law enforcement notification or involvement when the passenger is encountered at the airport (e.g., open wants and warrants, silent hits, etc.).

One particular type of actionable derogatory information is a "silent hit." ATS-P and TECS indicate the precise language "silent hit" to identify a passenger who is presumed to be unaware that he/she is a person of interest to law enforcement. The database remarks generally provide law enforcement contacts and direction for those who encounter the silent hit.

The SA/SSA must presume any passenger with actionable derogatory information is unaware that he/she is a person of interest to law enforcement and use extreme caution not to alert the passenger or TSR that there is derogatory information located in the record, or indicate anything out of the ordinary.



(b)(3);49 U.S.C. § 114(r)

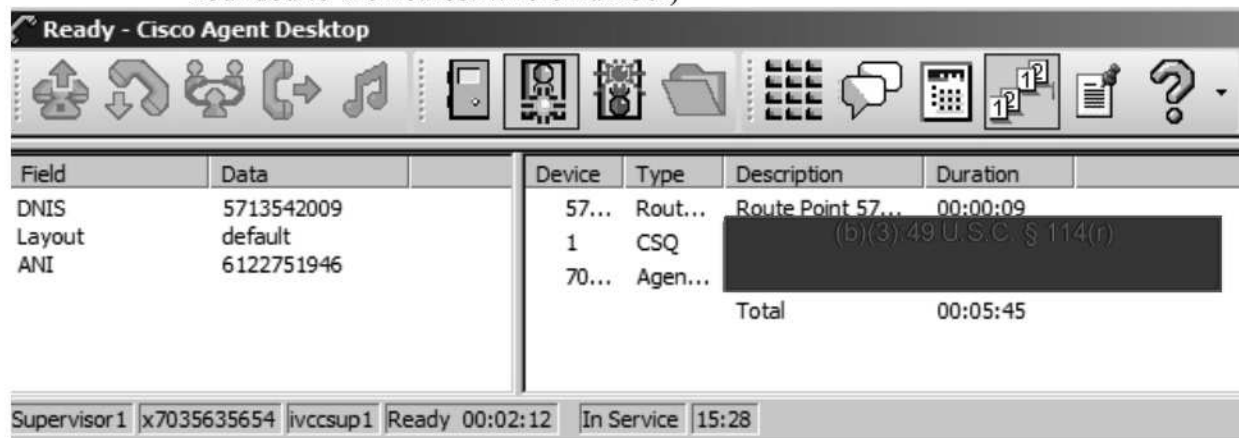
(b)(3) 49 U.S.C. § 114(r)

## 2.4 Verified/Unverified Determinations

Identity verification results in a verified or unverified determination.

### 2.4.1 Verified

1. 
2. 
3. Conclude the call.
4. Complete the following sections of the Call Data Sheet:
  - Circle Verified
  - Ref # (IVRN)
  - Duration of Call (this can be found on the Cisco Agent Desktop “Agent” line and rounded to nearest whole number due to WebEOC system constraints)
  - Wait Time (this can be found on the Cisco Agent Desktop “CSQ” line and rounded to the nearest whole number)



The screenshot shows the Cisco Agent Desktop interface. At the top, it says "Ready - Cisco Agent Desktop". Below this is a toolbar with various icons. The main area displays a table with call data:

Field	Data	Device	Type	Description	Duration
DNIS	5713542009	57...	Rout...	Route Point 57...	00:00:09
Layout	default	1	CSQ	(b)(3) 49 U.S.C. § 114(r)	
ANI	6122751946	70...	Agen...		
Total					00:05:45

At the bottom, there is a status bar showing: Supervisor 1, x7035635654, ivccsup1, Ready 00:02:12, In Service 15:28.

**Figure 2-3: Sample Cisco Agent Desktop with Duration of Call and Wait Time**

5. Proceed to WebEOC Data Entry section.

### 2.4.2 Unverified

15. Consult an SSA to ensure that all means of identification have been exhausted before issuing a final determination of unverified.

~~SENSITIVE SECURITY INFORMATION~~

16. If the passenger is unverified, ask the TSR for the following information to complete the Flight Information section of the Call Data Sheet before informing the TSR that the passenger is unverified:

- Airline
- Flight #
- From (Departure)
- To (Arrival)

17. Provide the unverified determination and callback instructions to the TSR using the appropriate "Inconsistent" script.

18. For unverified Foreign Nationals.

(b)(3)-49 U.S.C. § 114(r)

19. Complete the following sections of the Call Data Sheet:

- Circle Unverified
- Ref # (IVRN)
- Duration of Call (read from Cisco Agent Desktop and rounded to the nearest whole number due to system constraints)
- Wait Time (read from Cisco Agent Desktop and rounded to the nearest whole number)

6. Write under Alternate Questions/Answers section one of the following:

- No record found
- Record Found with Inconsistent Responses
- Record Found Lacking Identifying Information

7. Proceed to WebEOC Data Entry section.

### 2.4.3 WebEOC Data Entry

**Call Data**

\* Required Fields

\* Date/Time: 02/08/2013 15:28:24

\* Recorder:

\* Airport Contact:

\* Contact Title:

\* Contact #:

\* Airport Code:

\* Call Queue Wait Time: (minutes)

\* Duration of Call: (minutes)

Referred to TSOC: ☐ Check if call was referred to TSOC.

Foreign National: ☐ Check if passenger is a foreign national.

Referred to OI: ☐ Check if passenger was referred to OI.

Process Assistance: ☐

Watch List Check: ☐ Check if Watch List check conducted.

Explanation:

Delete: ☐ Check to remove entry from log.

**Figure 2-4: WebEOC Call Data Section**

#### 2.4.3.1 Verified Passengers

In WebEOC complete the following fields in the Call Data section:

- Date/Time
- Airport Contact
- Contact #
- Recorder
- Contact Title
- Airport Code
- Call Queue Wait Time (rounded to nearest whole number)
- Duration of Call (rounded to nearest whole number)

#### 2.4.3.2 Unverified Passengers

1. Complete the same Call Data fields for a verified passenger.
2. Check Foreign National box if applicable.
3. 

(b)(3):49 U.S.C. § 114(r)
4. Enter one of the following choices in the Explanation field:
  - a. PAX with ID: [Type of ID]
  - b. PAX without ID
  - c. F/N with ID: [Type of ID]
  - d. F/N without ID
6. Under the PAX Info Provided on Form section, complete the following fields:
  - a. Last Name
  - b. First Name

~~SENSITIVE SECURITY INFORMATION~~

c. Middle Name (if applicable)  
d. Current Address

**PAX Info Provided on Form**

PAX Record Not Found: ☐ Check if record not found.

Last Name:  First:  Middle:   
Alias:

---

Current Address

Street:   
City:  State:  Zip:

**Figure 2-5: WebEOC PAX Info Provided on Form Section**

7. Under the PAX Response section, complete the following fields:

(b)(3):49 U.S.C. § 114(r)

(b)(3):49 U.S.C. § 114(r)

~~SENSITIVE SECURITY INFORMATION~~**Figure 2-6: WebEOC PAX Response Section**

8. Under the Case Disposition section:
  - a. Check the PAX Not Verified box
  - b. Leave PAX Access as Unknown until after the callback
9. Click Save.
10. Give the Call Data Sheet to the SSA to await the callback.

The screenshot shows the 'Case Disposition' section of a web form. It includes the following fields and options:

- PAX Not Verified:** A checkbox that is checked, with the label 'Check if passenger was not verified.'
- PAX Access:** Three radio buttons: 'Allowed', 'Denied', and 'Unknown'. The 'Unknown' option is selected.
- Send to Incident Monitor:** A checkbox that is unchecked, with the label 'Click to send report to TSOC Incident Monitor'.
- Incident Monitor Title Text:** A text box containing '(ID: 900988) Passenger Unverified/Unknown at ()'.
- Incident Monitor Report Text:** A large text area for additional reporting.

**Figure 2-7: WebEOC Case Disposition Section**

#### 2.4.4 Call Backs

TSRs or airport coordination centers must call the IVCC to report the final decision on all unverified passengers, whether the passenger was allowed or denied access to the screening checkpoint. (b)(3) 49 U.S.C. § 114(r)

(b)(3) 49 U.S.C. § 114(r)

1. Answer the callback line and record the following information on the Call Back Information sheet (on the back of the Call Data Sheet):
  - a. IVCC operator (who takes the callback)
  - b. Time of callback
  - c. Name and title of caller
  - d. Caller's contact number
  - e. Disposition of the passenger (allowed/denied)
  - f. Was a LEO involved (Yes/No)
  - g. Agency (b)(3) 49 U.S.C. § 114(r)



- h. Was a database check conducted (Yes/No)
- i. What database (National Crime Information Center) (b)(3):49 U.S.C. § 114(r)
- j. Database check results (Record found with wants or warrants, Record found lacking identifying information, No record found, Other)
- k. What information used to conduct the database check
- l. Under whose authority was the passenger allowed or denied access (TSA Title and Name). If allowed by someone other than an FSD or designee without LEO involvement or further identifying documentation, proceed to Event section
- m. Notes (e.g., previously undisclosed documents, details that might not belong in a narrative but would help with administration)

## 2.4.5 Narratives

After answering the callback, the SSA creates a narrative.

1. Open the Narrative Templates folder and select the appropriate template.
2. Delete the sections that do not apply.
3. Overwrite the placeholders in bold.
4. Save the file using the format: [IVRN] Passenger's Last Name [narrative template].
5. After proofreading the narrative, copy it into WebEOC in the Incident Monitor Report text box under Case Disposition (see figure 2-7).
6. Change Unknown to Allowed or Denied (see figure 2-7).
7. Check the box to send the report to TSOC Incident Monitor.
8. Click Save.
9. Copy the narrative into the Daily Summary.
10. If denied, enter the information into the Denied Summary spreadsheet.

## 2.5 Special Circumstances

The IVCC follows the guidance below for special identity verification scenarios.

### Audience:

- SA
- SSA
- Section Chief

### 2.5.1 Passengers under 18 Years Old

Passengers under the age of 18 are not required to provide identification documentation. TSRs may be unsure if an individual is under 18 and call the IVCC.

#### Steps:

1. If the TSR doubts a passenger's claim to be under 18, (b)(3) 49 U.S.C. § 114(r).
2. If a LEO resolves any possible deception and there is new credible information that the passenger is 18 or older, the SSA may choose to allow identity verification to proceed.

### 2.5.2 Passengers (b)(3) 49 U.S.C. §

The following procedure guides identity verification in cases where (b)(3) 49 U.S.C. § 114(r) SA has difficulty verifying identity due to the lack of history of residences, vehicles, etc.

#### Steps:

1. Perform standard identity verification.

2.

3.

### 2.5.3 Third Party Verification

The following third party verification procedure guides SAs and SSAs when passengers are unable to communicate (e.g., escorted by a caregiver, cognitively impaired, etc.).

#### Steps:

(b)(3):49 U.S.C. § 114(r)

#### 2.5.4 Passenger Requires a Translator

The following procedure guides SAs and SSAs when passengers require a translator.

1. The IVCC allows objective translators who do not have a vested interest in allowing the passenger to travel (i.e., not traveling companions, family members, or nearby passengers who volunteer). Ask if an acceptable translator is available to assist, for example,

translators employed by TSA at the airport or IVCC, airlines, or law enforcement. It is preferred that SAs speak directly to TSA translators.

2. The TSR may call back if it will take time to locate an acceptable translator.
3. If an acceptable translator cannot be found, the IVCC will be unable to perform identity verification. Treat the call as a Process Assistance Call.

### 2.5.5 Passengers Escorted by Law Enforcement (Bounty Hunter Scenario)

The following procedure guides SAs and SSAs when passengers (prisoners or self-deporting passengers) are being escorted by a "LEO," do not possess acceptable identification documentation and cannot establish their own identities.

#### Steps:

1. Confirm with the TSR that the escort transporting the prisoner is in possession of 1) valid law enforcement credentials and 2) a second form of government photo ID. The escort must also present paperwork that indicates the authority to transport the prisoner, and the document must identify the passenger by the same name as that on the boarding pass. Escorts may not use other forms of identification (e.g., business cards, employment IDs) as a substitute for credentials and transport paperwork.
2. The IVCC requires that a LEO or AFSD-LEO (preferred), TSA management or their designee (as a last resort, if a LEO is unavailable) verify the authenticity of the escort's ID and transport paperwork. If the escort provides acceptable documentation and a LEO/AFSD-LEO/TSA management confirms that the documentation and identification are authentic, they may allow the passenger to proceed to the screening process. If they determine it is not, they may deny the passenger.
3. If the escort then provides acceptable documentation, but the TSR does not involve a LEO/AFSD-LEO/TSA manager to verify the documentation, determine that the passenger is unverified.
4. If the escort does not provide acceptable documentation:
  - a. Determine that the passenger is unverified
  - b. Refer the TSR to airport law enforcement

### 2.5.6 Passengers under U.S. Marshals Service (USMS) Protection

The USMS maintains a program that protects the identity of individuals providing assistance to the federal government. The following procedure guides SAs and SSAs when a passenger may be in witness protection and does not possess acceptable identification documentation. *Note: Do not ask for the actual identity of the protected individual.*

#### Steps:

1. If a LEO is escorting the person, refer the TSR to the U.S. Marshals Service section of the TDC SOP.

2. If a LEO is not escorting the person, determine that the passenger is unverified and refer the TSR to an airport LEO. Suggest that the TSR also notify his/her supervisor.

### 2.5.7 Repeat Offenders

The following procedure guides SAs and SSAs when passengers are possibly attempting to test the system by using alternative means or routes to access the screening checkpoint. Examples include, but are not limited to: a passenger or gate pass holder previously unverified and/or denied makes multiple attempts to access the screening checkpoint 1) (b)(3):49 U.S.C. § 114(r)

(b)(3):49 U.S.C. § 114(r)

#### Steps:

1. If there is suspicion of fraud, follow Suspicion of Fraud section 2.5.7 below.
2. If there is no suspicion of fraud, follow identity verification procedures as usual.

3.

(b)(3):49 U.S.C. § 114(r)

### 2.5.8 Suspicion of Fraud

The following procedure guides SAs and SSAs when they observe suspicious activity. Examples include but are not limited to the following: SA overhears passenger being advised to be deceptive about the reason for not having acceptable documentation, TSR mentions suspicion that identification documentation is fraudulent, etc.

#### Steps:

1. If fraud is suspected before identity verification begins:

a.

(b)(3):49 U.S.C. § 114(r)

- b. Refer the TSR to the TDC SOP and advise the TSR to call a LEO.

(b)(3):49 U.S.C. § 114(r)

2. If fraud is suspected during identity verification, determine that the passenger is unverified.

### 2.5.9 COI Form in Circulation

The following procedure applies to situations in which the SA finds that the passenger is in possession of a COI form that was used for previous identity verification.

#### Steps:

1. Advise the TSR to have the passenger surrender the COI form and provide it to TSA management. The COI form is SSI and is not to be circulated to the public.
2. Request any information from the TSR that may assist in determining how the form was released.
3. Notify the SSA.
4. Handle the call as a Process Assistance call.

### 2.5.10 Suspected Process Integrity Violations

(b)(3):49 U.S.C. § 114(r)

#### Steps:

(b)(3):49 U.S.C. § 114(r)

### 2.5.11 Intoxicated Passengers

Per Federal Aviation Administration (FAA) regulations, intoxicated passengers are not allowed to board an aircraft if the airline is aware of the situation. The following procedure applies if a TSR discloses that the passenger appears intoxicated.

#### Steps:

1. If the TSR discloses that the passenger appears to be intoxicated before identity verification begins:
  - a. Notify the SSA, who will consult with the TSR and confirm that the airport is requesting verification for a seemingly intoxicated passenger.
  - b. Ask the TSR to confer with TSA management and the airline, to determine if the process should continue.
  - c. If after TSA management is notified, they determine that the IVCC may perform identity verification, proceed to research the passenger.

2. If the TSR discloses that the passenger appears to be intoxicated after identity verification begins, determine that the passenger is unverified.

### 2.5.12 Uncooperative Passengers

The following procedure applies to passengers who are rude, belligerent, or refuse to answer questions.

#### Steps:

1. Ask the TSR to advise the passenger that if he/she does not cooperate, this may lead to denial to board the flight.
2. If the passenger remains uncooperative, proceed with the unverified procedure.
3. If the passenger becomes verbally or physically abusive, advise the TSR to call law enforcement and TSA management.

### 2.5.13 Voluntary Withdrawals

Voluntary withdrawals or “walk-aways” refer to passengers who approach the TDC but decide not to complete the screening process.

*Once passengers enter the screening checkpoint, they are not able to walk away. Per revised Office of Chief Counsel (OCC) policy pending publication, the TDC is part of the screening checkpoint, and passengers may not voluntarily withdraw from the process at this point.*

#### Steps to take until OCC Walk-Away Policy Takes Effect:

1. Proceed through the identity verification process as usual.
2. If the passenger withdraws before the identity verification process is complete, determine that the passenger is unverified.
3. Consider the final determination to be denied and complete the Call Back Information sheet immediately.
4. Enter “Voluntarily Withdrew from the Identity Verification Process” in a custom narrative.

#### Steps to take after OCC Walk-Away Policy Takes Effect:

If the passenger attempts to withdraw from the TDC/Identity Verification process, The TSR will refer to the TDC SOP for steps taken when a passenger leaves the screening area. The TDC SOP procedures for passengers who voluntarily withdraw from the process are outside the scope of IVCC operations.



### 2.5.14 Gate Passes

The following procedure applies to non-traveling individuals seeking access to the sterile area of an airport who do not have acceptable identification documentation. Examples include but are not limited to parents/guardians escorting minors, non-travelers wanting to visit the airport shops/restaurants, non-travelers wanting to visit friends or airport employees, passengers who have left an item behind in the sterile area and want to retrieve it, etc.

(b)(3);49 U.S.C. § 114(r)

#### Steps:

1. If the TSR mentions that the call is regarding a gate pass, ask the TSR the reason for the gate pass.

(b)(3);49 U.S.C. § 114(r)

2. As with traveling passengers, if the TSR or SA has concerns that the gate pass is for a suspicious activity:

(b)(3);49 U.S.C. § 114(r)

3. Traveling passengers receive priority over gate pass holders. If the SSA determines time-sensitive or critical operations are jeopardized, the IVCC may not be able to assist gate pass holders at that time.

### 2.5.15 Information Gathering Calls

The following procedure applies to information-gathering calls or “social engineering” calls to collect information about IVCC policies and procedures.

(b)(3);49 U.S.C. § 114(r)

(b)(3);49 U.S.C. § 114(r)

#### Steps:

- 1.

(b)(3);49 U.S.C. § 114(r)

- 2.



~~SENSITIVE SECURITY INFORMATION~~

3.

(b)(3):49 U.S.C. § 114(r)

4.

### 2.5.16 TSA Airport Employees

(b)(3):49 U.S.C. § 114(r)

### 2.5.17 Other Airport Employees

(b)(3):49 U.S.C. § 114(r)

### 2.5.18 Declaration of Nationality (DON)

Section 2.5.18 17 is pending leadership review and will be added in a future version.

### 2.5.19 Large Groups of Foreign Nationals and School Groups

The IVCC is not staffed to handle lengthy calls to process large groups of foreign nationals or students/teams. Refer (b)(3):49 U.S.C. § 114(r) for a LEO.

### 2.5.20 Military Orders

(b)(3):49 U.S.C. § 114(r)

### 2.5.21 Re-Entry

The following procedure applies to passengers who have entered the sterile area, left, and would like to re-enter the sterile area.

1. Boarding Passes:

(b)(3):49 U.S.C. § 114(r)

2. Gate Passes:

(b)(3):49 U.S.C. § 114(r)

### 2.6 Process Assistance Calls (formerly "SOP" calls)

The following procedure applies to calls that provide process assistance to TSRs regarding accepting other forms of identification allowed by the TDC SOP. These calls may or may not require identity verification. Some process assistance calls will require an update. "Process Assistance Calls Requiring Update" If the TSR is required to contact the IVCC for a process assistance call in order to update the passenger's allowed or denied status, the SA must provide a reference number to the TSR for the call back.

**Audience:**

- SA
- SSA
- Section Chief

**Steps:**

1. If the TSR is unaware of TDC SOP procedures and did not need to call the IVCC:
  - a. Request that the TSR follow established TDC SOP procedures for checking the identification documentation.
  - b. End the call.
2. If the TSR is aware of TDC SOP regarding other forms of ID but prefers IVCC involvement (e.g., the TSR is allowed to accept a BJ's Wholesale Club card and library card but prefers identity verification):
  - a. Ask the TSR if he/she would like to consult the STSO or manager regarding using the disclosed documentation, because if the IVCC proceeds with identity verification and provides an unverified determination, the previously disclosed

~~**SENSITIVE SECURITY INFORMATION**~~

documents will no longer be acceptable, and the IVCC will recommend LEO involvement.

- b. If the TSR wishes to proceed, perform identity verification as usual.
  - c. If the determination is unverified and the TSR then utilizes the previously disclosed documentation, an SSA should inform the STSO that without FSD (or designee) approval to re-use the previously disclosed documents, the situation will be tracked and escalated on an incident report as a violation of the IVCC procedure.
    - The SSA collects all information (e.g., names of those involved, airport, date/time, summary, etc.) and submits to the Section Chief for escalation to the FSD.
3. If the process assistance call did not result in an identity verification check, mark the Process Assistance box in the Call Data section of WebEOC.

Process Assistance: ☐ Check if no check was conducted.

**Figure 2-8: Process Assistance Checkbox**

4. Write "Process Assistance Call" or PAC on the Call Data Sheet under Alternate Questions/Answers.
5. Include the following additional information on the Call Data Sheet only:
  - a. Passenger/gate pass holder's full name.
  - b. Brief synopsis of the reason for the call and what was stated to caller.

## 2.7 Watch List Checks

The IVCC acknowledges the definition of a substantial mismatch as outlined in Chapter 4 of the TDC SOP unless otherwise directed by Secure Flight Operations.

The IVCC has determined a substantial mismatch is fundamentally different from a complete mismatch. The IVCC defines a substantial mismatch as one where the name on the boarding pass implies a recognizable association to the name on the acceptable identification. The IVCC defines acceptable identification *for the purpose of Watch List matching* as government-issued ID. Examples include married vs. maiden name, or name change with accompanying documentation.

The IVCC defines a complete mismatch as one where the name on the boarding pass has no recognizable association to the name on the identifying documents or the name presented on the COI form. If the IVCC determines the name on the boarding pass is completely different from the name on the identification, the IVCC will be unable to verify the identity of the passenger. In the case of a complete mismatch, the IVCC recognizes the FSD or the FSD designee as the only authority who can determine if the passenger will proceed through the security checkpoint. The IVCC will have Secure Flight conduct a Watch List check for the complete mismatch if the FSD/designee determines the passenger will be allowed to proceed through screening.

### Audience:

- SA
- SSA

### 2.7.1 Requests for Watch List Checks in the Case of a Substantial Mismatch

Steps for a substantial mismatch (married/maiden name, legal name change, etc.) if the passenger has acceptable (government-issued) identification:

- 1.
- 2.

(b)(3) 49 U.S.C. § 114(r)

~~SENSITIVE SECURITY INFORMATION~~

3.

(b)(3):49 U.S.C. § 114(r)

**Steps for a substantial mismatch if the passenger has other identification or no identification:**

1.

(b)(3):49 U.S.C. § 114(r)

2.

## 2.7.2 Requests for Watch List Checks in the Case of a Complete Mismatch

**Steps:**

1.

(b)(3):49 U.S.C. § 114(r)

2.

## 2.7.3 No-Fly and Selectee Watch List Matches

(b)(3):49 U.S.C. § 114(r)

**Steps:**

1.

(b)(3):49 U.S.C. § 114(r)

2.

3.  
4.  
5.  
6.  
7.  
8.  
9.

(b)(3), 49 U.S.C. § 114(r)

## 2.8 Events

The following procedure applies to time-sensitive situations in which the IVCC has provided a determination of unverified, and a TSA employee other than the FSD or designee has allowed the passenger to enter the screening checkpoint or the sterile area of an airport without LEO involvement or without receiving acceptable, previously undisclosed identity documentation. An event may be low-risk or potentially high-risk.

### Audience:

- SSA

### Steps:

1. During the callback, complete all fields on the Call Back Information sheet. Gather as many additional details as possible.
2. Call airport coordination center, ask who on the FSD staff is available to assist, contact person, and see if he/she agrees with the decision to allow the passenger.
  - a. If the FSD staff POC agrees, this is not an event. Enter the POC's name in the narrative as the final authority who allowed the passenger.
  - b. If the FSD staff POC does not agree.

(b)(3), 49 U.S.C. § 114(r)

(b)(3), 49 U.S.C. § 114(r)

~~SENSITIVE SECURITY INFORMATION~~

- 3.
- 4.
- 5.
- 6.
- 7.

(b)(3) 49 U.S.C. § 114(r)

**Audience:**

SA

If an SA discovers a procedural error that may result in an event, the SA should report the incident to the SSA. The SSA will identify the chain of command and communicate with the appropriate TSA officials at the airport. The SA should only participate in communication of an event or potential event when requested to do so by an SSA.

**2.9 Known or Suspected Terrorist (KST) Report**

(b)(3) 49 U.S.C. § 114(r)

**Audience:**

- SA
- SSA

**Steps:**

- 1.

(b)(3) 49 U.S.C. § 114(r)

~~SENSITIVE SECURITY INFORMATION~~

---

(b)(3) 49 U.S.C. § 114(r)



~~**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.~~



~~**SENSITIVE SECURITY INFORMATION**~~**APPENDIX A ACRONYMS**

Acronym	Description
ACD	Automated Call Distribution
ATS-P	Automated Targeting System - Passenger
BDO	Behavior Detection Officer
CBP	Customs and Border Protection
CCO	Coordination Center Officer
CDO	Command Duty Officer
COI	Certification of Identity
CSA	Customer Support Agent
DMV	Department of Motor Vehicles
DOB	Date of Birth
FAA	Federal Aviation Administration
FAMS	Federal Air Marshal Service
F/N	Foreign National
FSD	Federal Security Director
FTE	Full-time Equivalent or Employee
ICE	Immigration and Customs Enforcement
ID	Identification
IVCC	Identity Verification Call Center
IVCCB	Identity Verification Call Center Branch
IVRN	Identity Verification Reference Number
KST	Known or Suspected Terrorist
LEO	Law Enforcement Officer
LTSO	Lead Transportation Security Officer
NCIC	National Crime Information Center
NFNR	No Fly Notification Report
OCC	Office of Chief Counsel
OIA	Office of Intelligence and Analysis
OSO	Office of Security Operations
PAX	Passenger
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PNR	Passenger Name Record
POC	Point of Contact
SA	Security Assistant
SFA	Secure Flight Analyst
SFUI	Secure Flight User Interface
SIDA	Secure Identification Display Area
SNR	Selectee Notification Report
SOC	Secure Flight Operations Center

~~**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.~~

~~SENSITIVE SECURITY INFORMATION~~

Acronym	Description
SOP	Standard Operating Procedure
SPOT	Screening Passengers by Observation Technique
SSA	Supervisory Security Assistant
SSI	Sensitive Security Information
SSN	Social Security Number
STSO	Supervisory Transportation Security Officer
TDC	Travel Document Checker
TPB	Trends and Patterns Branch
TSA	Transportation Security Administration
TSM	Transportation Security Manager
TSO	Transportation Security Officer
TSOC	Transportation Security Operations Center
TSS	Transportation Security Specialist
USMS	U.S. Marshals Service
VEA	Vetting and Encounter Analyst
VOD	Vetting Operations Division

~~**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.~~

~~**SENSITIVE SECURITY INFORMATION**~~**APPENDIX B DATABASE SEARCH RULES**

The IVCC [REDACTED]

(b)(3) 49 U.S.C. § 114(r)

confirm information

provided by a passenger. The following rules guide SSAs and SAs:

1. IVCC personnel are authorized to access the databases only when requested by a TSA representative at an airport or by TSA management to assist in verifying the identity of an individual seeking access to the screening checkpoint. IVCC personnel must not access information or use the database for personal inquiries or any other purpose. Unauthorized use of the databases may lead to discipline, criminal penalties, and/or dismissal of the IVCC employee. IVCC personnel may not print, record, or otherwise retain any information accessed on an individual other than that called for by call data sheets and WebEOC.
2. Identity verification using the databases [REDACTED]  
(b)(3) 49 U.S.C. § 114(r) [REDACTED] SSAs may supply details to the FSD staff.
3. The SA must confirm [REDACTED] (b)(3) 49 U.S.C. § 114(r) [REDACTED] the information in the database. Identities are considered verified when [REDACTED] (b)(3) 49 U.S.C. § 114(r) [REDACTED] (b)(3) 49 U.S.C. § 114(r) [REDACTED]
4. [REDACTED] (b)(3) 49 U.S.C. § 114(r) [REDACTED]
5. SAs may not ask questions related to the individual's political party affiliation, charitable contributions, sexual orientation, religion, race, ethnicity, finances, possible criminal record, or other personally sensitive areas.
6. The information in the databases [REDACTED] (b)(3) 49 U.S.C. § 114(r) [REDACTED] Information in the database should be considered a tool to help identify an individual without other forms of identification.