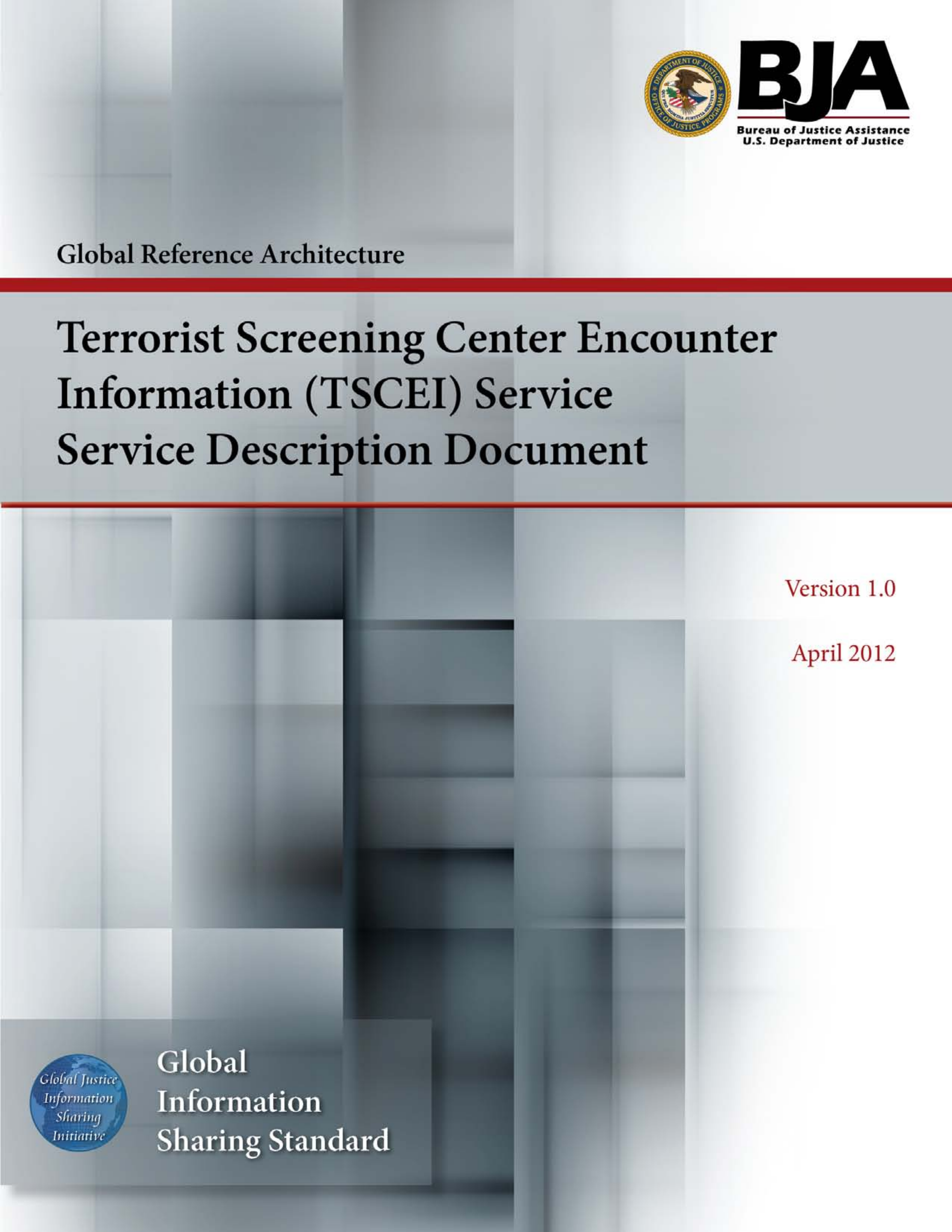


BJA
Bureau of Justice Assistance
U.S. Department of Justice

Global Reference Architecture

Terrorist Screening Center Encounter Information (TSCEI) Service Service Description Document

Version 1.0

April 2012

Global Justice Information Sharing Initiative

Global
Information
Sharing Standard

Global Standards

Global's collection of normative standards has been versioned independently and assembled into a package of composable, interoperable solutions specifically supporting an information exchange. The package is known as the Global Standards Package (GSP). GSP solutions are generally technically focused but also may include associated guidelines and operating documents. GSP deliverables include artifacts associated with many of the Global product areas, including but not limited to:

- **Global Reference Architecture (GRA):** Offers guidance on the design, specification, and implementation of services (and related infrastructure) as part of a justice Service-Oriented Architecture (SOA).
- **Global Service Specification Packages (SSPs):** Reference services that serve as the means by which the information needs of a consumer are connected with the information capabilities of an information provider.
- **Global Federated Identity and Privilege Management (GFIPM):** Guidelines and standards for establishing, implementing, and governing federated identity management approaches.
- **Global Privacy Technology Framework:** A framework for automating access control (in particular, privacy) policy as part of information exchange.

For More Information

For more information on the GSP and the Global Standards Council (GSC)—the Global group responsible for developing, maintaining, and sustaining the same—please visit http://www.it.ojp.gov/gsc.

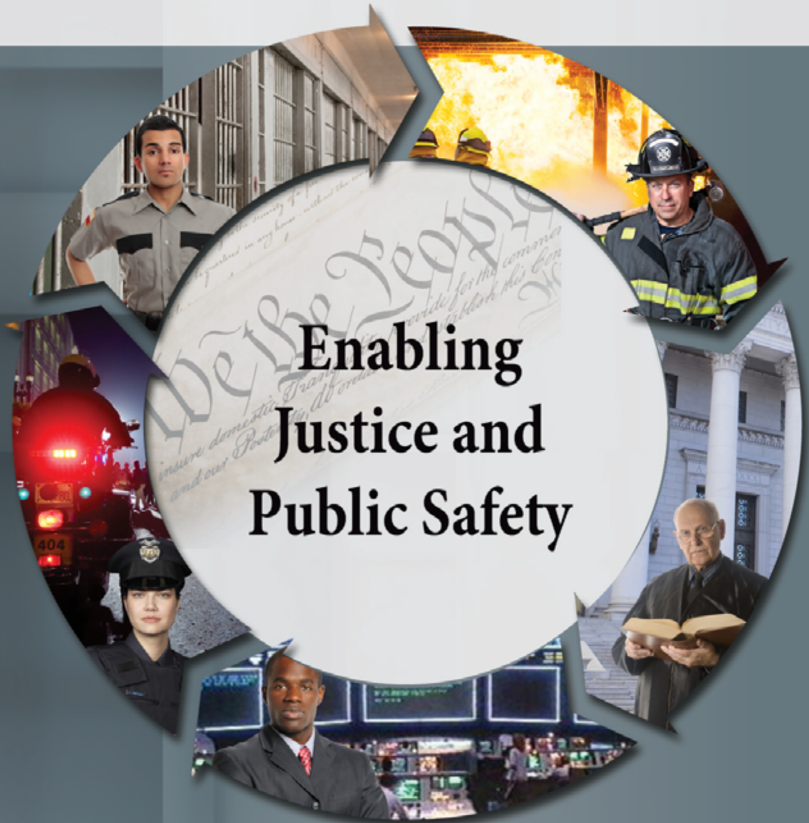


Table of Contents

1. Document Introduction

In the context of the GRA and Service-Oriented Architecture **[SOA]** in general, a service is the means by which one partner gains access to one or more capabilities offered by another partner. Capabilities generate real-world effects that can be as simple as sharing information or can involve performing a function as part of a complex process or changing the state of other related processes. Government organizations have numerous capabilities and a multitude of partner organizations, both inside and outside of their traditional communities. There are significant benefits for these organizations to share information and have access to each other's capabilities. Achieving interoperability among these organizations requires alignment of business and technical requirements and capabilities. In addition, it is critical to have a consistent way of specifying these requirements and capabilities and sharing them across organizational boundaries. The GRA was developed to facilitate interoperability and to assist in meeting other key requirements common in a complex government information sharing environment. In order to achieve interoperability, a consistent approach must be defined to identify, describe, and package services and their interactions in many different technical environments, across multiple government lines of business, at all levels of government, and with partner organizations.

The GRA defines a service interface as “the means for interacting with a service.” It includes specific protocols, commands, and information exchange by which actions are initiated on the service. A service interface is what a system designer or implementer (programmer) uses to design or build executable software that interacts with the service. That is, the service interface represents the “how” of the interaction. Since the service interface is the physical manifestation of the service, best practices call for service interfaces which can be described in an open-standard, machine-referenceable format (that is, a format which could be automatically processed by a computer).

A Service Specification is a formal document describing the capabilities made available through the service; the service model that defines the semantics of the service by representing its behavioral model, information model, and interactions; the policies that constrain the use of the service; and the service interfaces which provide a means to interacting with the service. A Service Specification is analogous to the software documentation of an Application Programming Interface **[API]**. It provides stakeholders with an understanding of the structure of the service and the rules applicable to its implementation. It gives service consumers the information necessary for consuming a particular service and service providers the information necessary for implementing the service in a consistent and interoperable way.

The main components of a Service Specification are the Service Description, one or more Service Interface Descriptions, and the schemas and the samples used to implement and test the service.

A Service Description contains information about all aspects of the service which are not directly tied to the physical implementation of the service; in other words, the service interface. A Service Interface Description is a description of the physical implementation; specifically, the service interface used in a specific implementation of the service.

This document is a Service Description of the TSC Encounter Information Service.

2. Service Overview

2.1 Purpose

Provide Positive Encounter information and updates to state or U.S. government territory designated fusion centers.

2.2 Scope

The scope includes law enforcement agencies' encounter information that is sent to the state or U.S. government territory designated fusion center based on the location of the encounter.

Note: The scope includes only encounters resulting from law enforcement agencies and does not include encounters resulting from other screening agencies.

2.3 Capabilities

1. Provide Positive Encounter information to state or U.S. government territory designated fusion centers.

2. Provide Positive Encounter updates to state or U.S. government territory designated fusion centers.

3. Provide Encounter change of status information to state or U.S. government territory designated fusion centers.

2.4 Real-World Effects

1. The Positive Encounter information can be used tactically by a fusion center to further investigate a specific case in collaboration with the respective law enforcement agency or agencies.

2. The Positive Encounter information can be used tactically to inform the Joint Terrorism Task Force (JTTF) of encounters within its area of responsibility.

3. The encounter information (and any supplemental derogatory[1] information that may be provided) can be used for analytical purposes to provide information about Known or Suspected Terrorists (KST) traversing the jurisdiction of a fusion center and to assist in determining patterns. This will facilitate situational awareness.

2.5 Summary

This service provides two interface descriptions. The first will be used by fusion centers to receive information regarding Positive Encounters from TSC. The second will be used by TSC to receive acknowledgement messages asynchronously from the receiving fusion center.

2.6 Description

This service will be used by state or U.S. government territory designated fusion centers to receive information regarding positive encounters from TSC. The encounter information received by state or U.S. government territory designated fusion centers will be limited to Positive Encounters resulting from the hits by local law enforcement agencies on an extract of the Terrorist Watchlist. The extract of the Terrorist Watchlist used to identify law enforcement hits is the Known or Suspected Terrorist File (KST) maintained by the National Crime Information Center (NCIC). The service will also be used by TSC to send any changes of status or updates related to Positive Encounter Information to the state or U.S. government designated fusion centers.

2.6.1 Security Classification

The information exchanged by this service is considered Sensitive But Unclassified (SBU). As a result, the service can be assigned a security classification of SBU.

2.6.2 Service Specification Package Version

This service specification is built based on version 1.0.0 of the Service Specification Package.

3. Business Scenarios

3.1 Business Scenario

State and U.S. government territory designated fusion centers will use this service to receive Positive Encounter information. A Positive Encounter results from a hit by local law

---

[1] Derogatory information is classified information that supports an individual's nomination as a KST to the TSDB. Source: ISE-EAF v2.0.

enforcement against an extract of the Terrorist Watchlist. This information will be used for tactical and analytical purposes.

3.1.1 Primary Flow

- Local law enforcement conducts name-based search queries against an extract of the Terrorist Watchlist based on an encounter.

- If a match occurs, the Terrorist Screening Center (TSC) receives the query information and the response of the search as an XML message closely resembling a log file format.

- If a match occurs, local law enforcement is notified and requested to contact the TSC via a phone call.

- Upon receiving a phone call, the TSC researches, gathers, verifies, documents, and analyzes available information to determine whether the individual encounter matches an identity in the Terrorist Screening Database (TSDB). This results in a preliminary determination.

- The information is passed to the TSC watch commander. The watch commander vets the preliminary determination. A notification is sent electronically to the Terrorist Screening Operations Unit (TSOU). TSOU performs secondary determination.

- In the case of a positive preliminary determination, information about the Positive Encounter is sent electronically to the state or U.S. government territory designated fusion center.* The exact timing of this notification will be dependent on TSC business processes and any MOUs in place between TSC and applicable state or U.S. government territory designated fusion centers.

- In case of negative secondary determination, TSC and TSOU work on establishing concurrence regarding the encounter. That results in final determination. The final determination is subject to export review process.

- Upon completion of the export review process, TSC sends the encounter information, including the final determination, to the state or U.S. government territory designated fusion center. The encounter information contains the encounter status allowing notification of any status changes to be sent to the state or U.S. government territory designated fusion center.

- The state or U.S. government territory designated fusion center receives the encounter information message.

- The encounter information is captured by the state or U.S. government territory designated fusion center. The specific processes for capturing and using the information will be determined based on the state or U.S. government territory designated fusion center's business processes and the policies and procedures contained in an MOU between the TSC and the state or U.S. government territory designated fusion center.

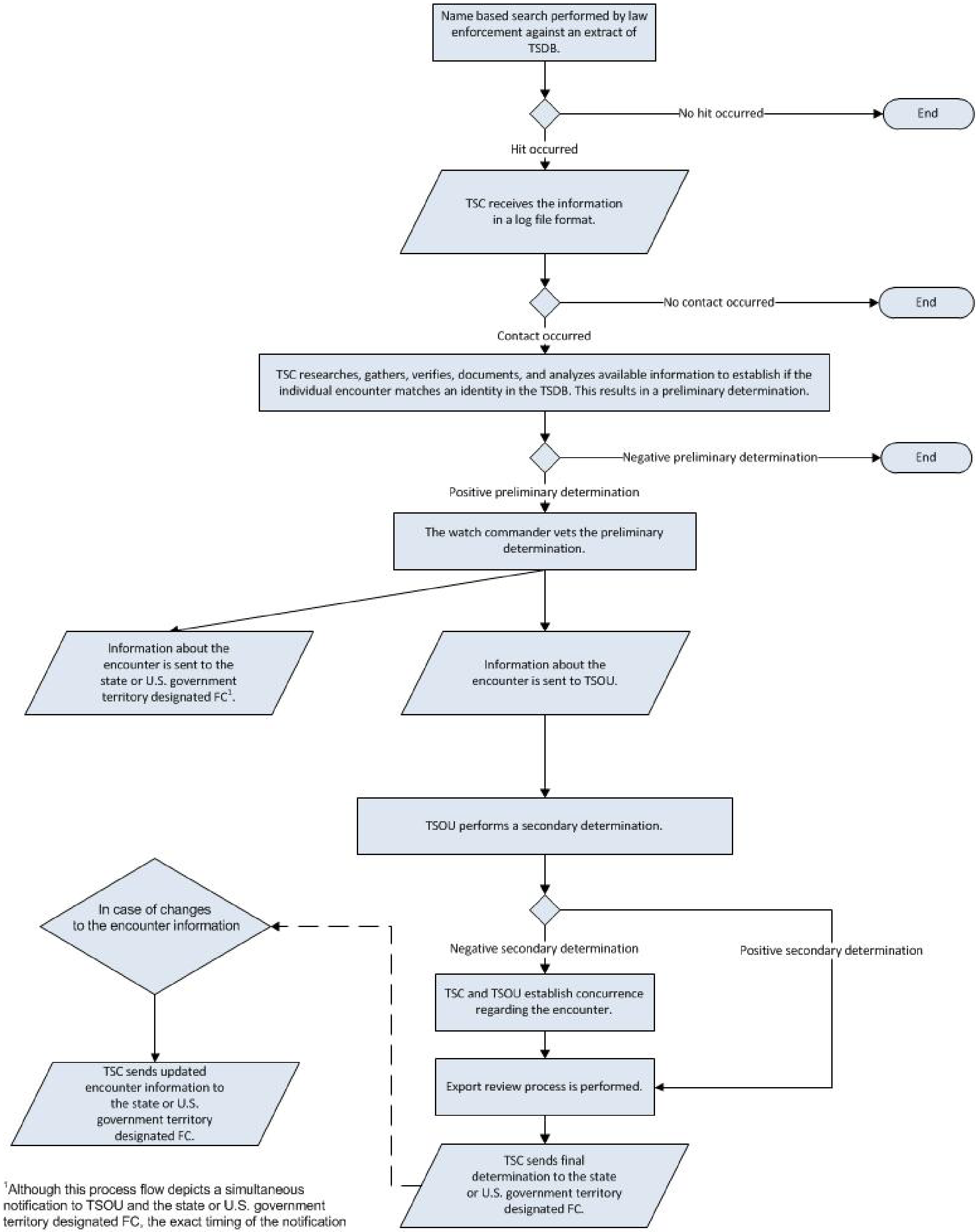
- Upon receipt of the encounter information, the state or U.S. government territory designated fusion center sends an asynchronous acknowledgement message to the TSC. This message indicates successful receipt and processing of the encounter message and includes information necessary to correlate the acknowledgement with the original encounter information message.

- The fusion center analyst follows up and/or performs further analysis, researching the encounter information to facilitate risk assessment and situational awareness.

- In case of any changes to the encounter information, including status changes, TSC sends the updated encounter information to the state or U.S. government territory designated fusion center.

*In the current process, this communication is achieved via a phone call.

The process flow, use case, and sequence flow diagrams provided below depict the business process flow in more detail.


Name based search performed by law enforcement against an extract of TSDB.
No hit occurred
End
Hit occurred
TSC receives the information in a log file format.
No contact occurred
End
Contact occurred
TSC researches, gathers, verifies, documents, and analyzes available information to establish if the individual encounter matches an identity in the TSDB. This results in a preliminary determination.
Negative preliminary determination
End
Positive preliminary determination
The watch commander vets the preliminary determination.
Information about the encounter is sent to the state or U.S. government territory designated FC1.
Information about the encounter is sent to TSOU.
TSOU performs a secondary determination.
In case of changes to the encounter information
Negative secondary determination
Positive secondary determination
TSC and TSOU establish concurrence regarding the encounter.
Export review process is performed.
TSC sends updated encounter information to the state or U.S. government territory designated FC.
TSC sends final determination to the state or U.S. government territory designated FC.

[1] Although this process flow depicts a simultaneous notification to TSOU and the state or U.S. government territory designated FC, the exact timing of the notification to the FC will be dependent on TSC business processes and any MOUs in place between TSC and the applicable FC.

Figure 1: Encounter Business Process Flow Diagram

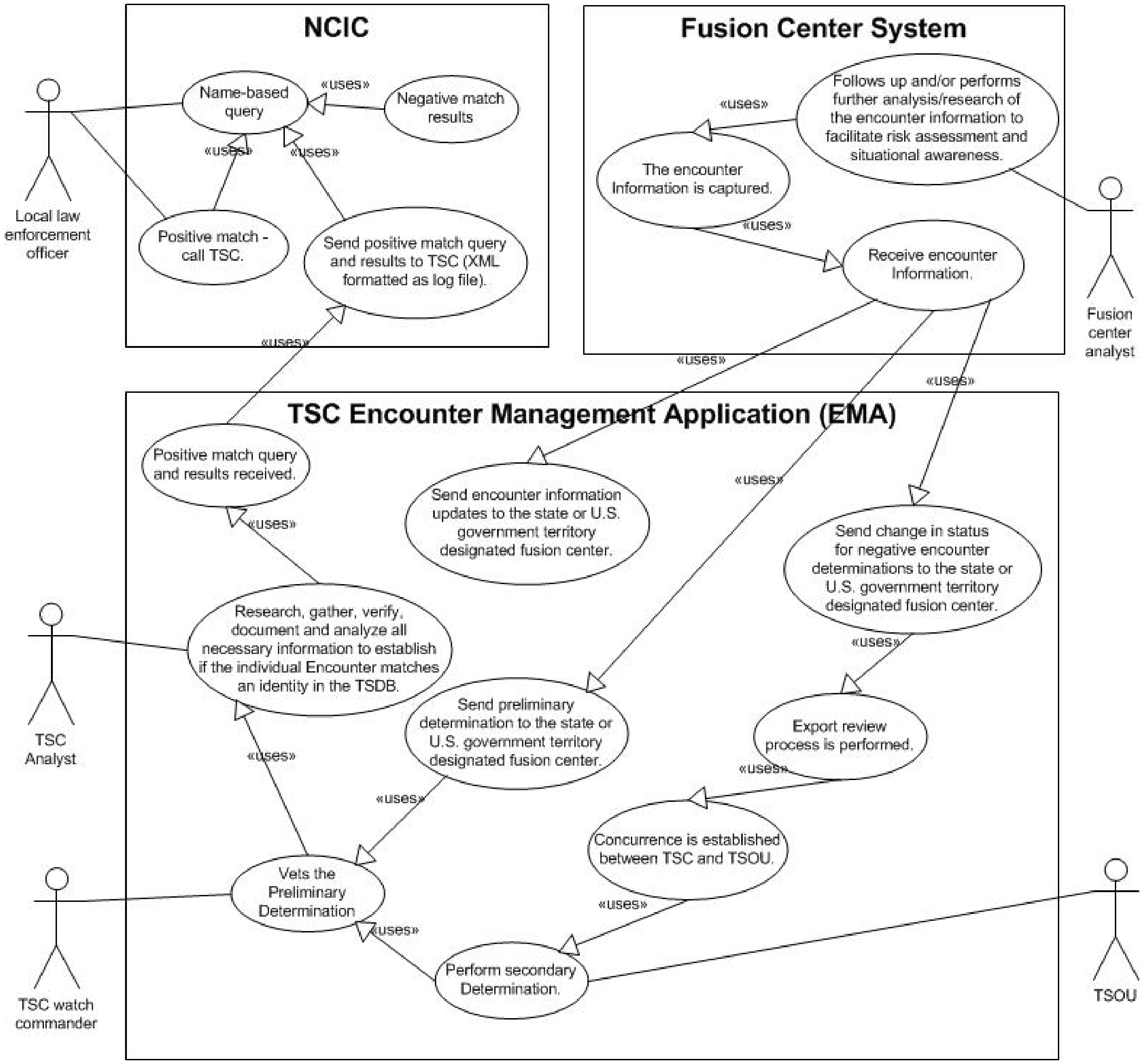

NCIC
Name-based query
«uses»
Negative match results
«uses»
«uses»
Positive match - call TSC.
Send positive match query and results to TSC (XML formatted as log file).
Local law enforcement officer
Fusion Center System
«uses»
Follows up and/or performs further analysis/research of the encounter information to facilitate risk assessment and situational awareness.
The encounter Information is captured.
«uses»
Receive encounter Information.
Fusion center analyst
«uses»
«uses»
«uses»
TSC Encounter Management Application (EMA)
Positive match query and results received.
Send encounter information updates to the state or U.S. government territory designated fusion center.
«uses»
Send change in status for negative encounter determinations to the state or U.S. government territory designated fusion center.
«uses»
Research, gather, verify, document and analyze all necessary information to establish if the individual Encounter matches an identity in the TSDB.
TSC Analyst
«uses»
Send preliminary determination to the state or U.S. government territory designated fusion center.
«uses»
Export review process is performed.
«uses»
«uses»
Concurrence is established between TSC and TSOU.
Vets the Preliminary Determination
«uses»
«uses»
TSC watch commander
Perform secondary Determination.
TSOU

Figure 2: Use Case Diagram

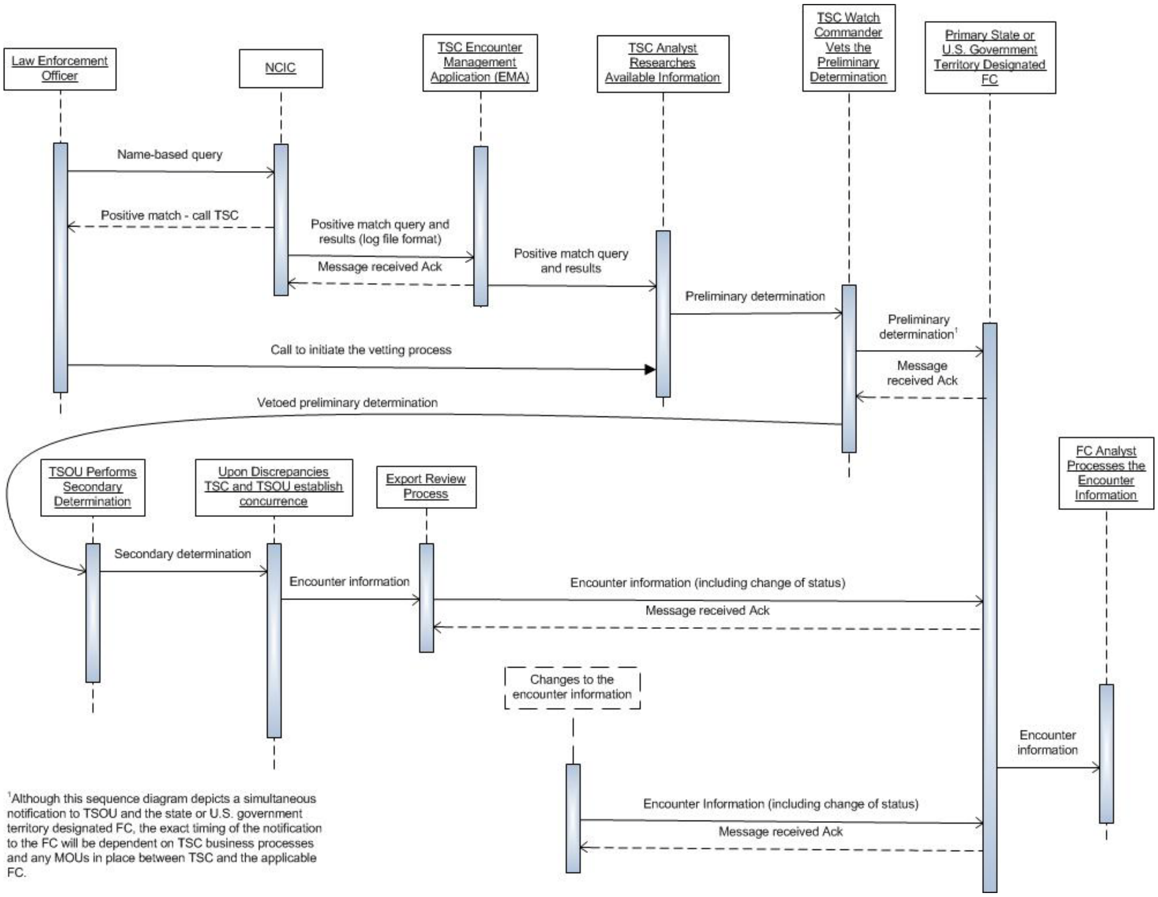

Law Enforcement Officer
NCIC
TSC Encounter Management Application (EMA)
TSC Analyst Researches Available Information
TSC Watch Commander Vets the Preliminary Determination
Primary State or U.S. Government Territory Designated FC
Name-based query
Positive match - call TSC
Positive match query and results (log file format)
Message received Ack
Positive match query and results
Preliminary determination
Preliminary determination¹
Message received Ack
Call to initiate the vetting process
Vetoed preliminary determination
TSOU Performs Secondary Determination
Upon Discrepancies TSC and TSOU establish concurrence
Export Review Process
FC Analyst Processes the Encounter Information
Secondary determination
Encounter information
Encounter information (including change of status)
Message received Ack
Changes to the encounter information
Encounter information
Encounter Information (including change of status)
Message received Ack
¹Although this sequence diagram depicts a simultaneous notification to TSOU and the state or U.S. government territory designated FC, the exact timing of the notification to the FC will be dependent on TSC business processes and any MOUs in place between TSC and the applicable FC.

Figure 3: Encounter Sequence Diagram

3.1.2 Alternative Flows

No alternative flows have been identified at this time.

3.2 Service Interoperability Requirements

3.2.1 Service Assumptions

- All messages exchanged between TSC and the fusion centers are stored in a log for auditing purposes.

- All messages exchanged between TSC and the fusion centers require an acknowledgement of receipt.

- The acknowledgement of receipt is sent asynchronously and will contain WS-ReliableMessaging and WS-Addressing metadata about the encounter message. The metadata will include a correlation identifier of the message being acknowledged.

- An MOU will be in place between TSC and the state or U.S. government territory designated fusion centers.

- TSC will have information about the state or U.S. government territory designated fusion center for a specific location and send the encounter information to the fusion center responsible for the location where the encounter occurred. The state or U.S. government territory fusion center responsible for the location where the encounter occurred will be determined based on the ZIP code of the location. In case there is no ZIP code available, the Originating Agency Identifier (ORI) of the law enforcement agency could be used to determine the state or U.S. government territory fusion center to which the encounter should be sent.

- The state or U.S. government territory designated fusion center will ultimately pass the information to any other fusion centers within its jurisdiction or to any other fusion center which would benefit from the information.

3.2.2 Service Dependencies

No dependencies have been identified at this time.

3.2.3 Execution Context

This service will leverage the TSC Encounter Management Application (EMA) Service Layer. The service will also adhere to the transaction infrastructure defined by the Terrorist Watchlist Person Data Exchange Standard (TWPDES).

High-level information from the TWPDES regarding the transaction infrastructure implementation is provided below:

- TWPDES leverages existing commercial standards:
  - Organization for the Advancement of Structured Information Standards (OASIS) ebXML Messaging Service (ebMS)
  - World Wide Web Consortium (W3C) Simple Object Access
  - Protocol (SOAP)
- TWPDES supports multiple transportation standards and products:
  - Message Oriented Middleware (e.g., IBM Websphere MQ)

  - WS-Security, WSReliableMessaging, and other W3C Web service standards
  - Supports request, reply semantics, and error handling

3.2.4 Policies and Contracts

- Applicable policies will be regulated under the MOU between TSC and the state or U.S. government territory designated fusion centers.
- TSC will notify only one fusion center regarding a hit. This will be the state or U.S. government territory designated fusion center for the location of the hit based on the ZIP code of the location. The state or U.S. government territory designated fusion centers which received the encounter will distribute the information to fusion centers within its jurisdictions and any fusion centers which might be owners or interested in the case.
- A periodic reconciliation of the encounter information is required by TSC. Additional information about the current technical implementation of the reconciliation process is available under the Additional Information section of this document. state or U.S. government territory designated fusion centers are required to implement the same level of reconciliation for any further distribution of the information to fusion centers within their jurisdictions.
- A periodic audit process will be in place to verify that the information available to state or U.S. government territory designated fusion centers is accurate. state or U.S. government territory designated fusion centers are required to implement an audit process for any further distribution of the information to fusion centers within their jurisdictions.
- The current process is documented for encounters related to the KST file and related to law enforcement queries of this file. Other screening agencies are not included in the process.

3.2.5 Security

The service will adhere to the security rules required and documented by TSC.

- The service will adhere to the *Fusion Center Guidelines*[2] and, more specifically, "Guideline 9: Security."

---

[2] For more information, please refer to the *Fusion Center Guidelines* document. http://www.it.ojp.gov/documents/fusion_center_guidelines.pdf.

- The service can be implemented to exchange information which has different security classifications (e.g., unclassified or classified).* The required security policies and constraints will be implemented for each level of information classification.

- An MOU between TSC and the state or U.S. government territory designated fusion centers will regulate security requirements.

**The specifications could be further enhanced to handle information of a higher security level by specific fusion centers and the TSC based on MOUs between the agencies.*

3.2.6 Privacy

The service will adhere to the *Fusion Center Guidelines*[3] and, more specifically, "Guideline 8: Privacy and Civil Liberties."

The MOU between TSC and the state or U.S. government territory designated fusion centers will regulate privacy requirements.

3.2.7 Additional Information

Provided below is additional information discovered during the process of creating the service specification.

- Every record in the TSDB is manually reviewed and categorized by the various exports based on type and quality of data. The criteria are based not only on the record, but also on the derogatory information on which the record is based. The derogatory information related to a record in TSDB resides with its respective nominating agency. One example of an export of TSDB is the Known or Suspected Terrorist File (KST).

- Law enforcement and other screening agencies conduct a search against their respective extracts of the Terrorist Watchlist.

- Fusion centers will benefit from getting the encounter information not only related to law enforcement queries but also from other screening agencies. This is especially true for border control information. Currently, this is done through a manual process via tab reports. A determination will need to be made if this is possible and within the scope of this project. The process from a technical perspective would be similar.

---

[3] For more information, please refer to the *Fusion Center Guidelines* document *http://www.it.ojp.gov/documents/fusion_center_guidelines.pdf*.

- The preliminary determination conducted by TSC is achieved in a limited time frame (5–15 minutes).

- Silent hits will not fall under this process, since they are not verifiable. Only the case agent is notified of the hit in the case of a silent hit.

- The notification of the query and response from NCIC to TSC is designed for a matrix line printer. It has been modified to an electronic log file, but the format is the same as for the matrix line printer. This file is analyzed on a weekly basis.

- A change of status related to encounter or individual information should be sent to the fusion center which has already received the encounter information. This fusion center will be responsible for passing this change of status information to fusion centers within its jurisdiction that previously received the original information.

- KST has limitations in handling international names. The algorithm is not optimized for the names prevalent on the list. Length and specific international names (Arabic, Chinese, etc.) are the main issues. These issues are being addressed through the CJIS Advisory Policy Board (APB) process.

- Reconciliation is a two-step process designed to ensure that downstream systems are in synch with the Encounter Management Application (EMA). The first level (Tier I) employs a system-level message digest created from the Encounter SR number and version number. If the systems do not agree on the message digest, the process calls for a second, more detailed report (Tier II) of each encounter and a message digest of all the data associated with it.

  To minimize data transmissions, the reconciliation process utilizes a message digest, a hash value of all relevant data. Given identical data, the digest values will also be identical. Any difference and the digest values will not agree.

  The digest values are created by hashing all relevant data fields utilizing the SHA-1 algorithm (SHA-1, NIST FIPS 180-1). Implementations of this algorithm are widely available, and it is not considered necessary to require the additional security or complexity of an SHA-2 algorithm.

  The reconciliation process would be a transactional process between the two systems. Since changes to data during the reconciliation process could alter the outcome of the digest process, systems must follow strict procedures to ensure that the process is run against the same data set. The reconciliation digest process needs to run in a consistent manner to ensure that both systems compute the same digest for the same data set. To ensure this, the order of data fields in the digest will be determined by the XML grammar (the schema), since this will be common to any implementation of the digest.

The table below outlines the fusion center drivers and objectives, documented during the project, which this service addresses.

Drivers and Objectives	Means of Achieving
"Information Underload" The appropriate interface capabilities do not exist among state, local law enforcement, and the fusion centers.	This service would allow fusion centers to receive information regarding persons, places, events, or objects from partnering fusion centers.

This service supports the following capabilities identified during the fusion center Capability and Service Interaction Modeling efforts.

Function:	Information Collection
Subfunction:	Receive Information (active)
Capability:	Receive information from TSC.

The following table outlines the fusion center (IAC) baseline capabilities this service supports. The baseline capabilities are selected from the document published by Global and named *Baseline Capabilities for State and Major Urban Area Fusion Centers.*[4]

---

[4] For more information, please refer to the *Fusion Center Baseline Capabilities* document at http://www.it.ojp.gov/documents/baselinecapabilitiesa.pdf.

A. Planning and Requirements Development	6. Situational Awareness Reporting—Fusion centers shall develop processes to manage the reporting to key officials and the public of information regarding significant events (local, regional, national, and international) that may influence state or local security conditions.
B. Information Gathering, Collection and Recognition of Indicators and Warnings	1. Information-Gathering and -Reporting Strategy—Fusion centers shall develop, implement, and maintain an information-gathering and -reporting strategy that leverages existing capabilities and shall identify methods for communicating information requirements and the overall information-gathering strategy to partners, to include any applicable fusion liaison officers. b. Leverage and/or coordinate with the JTTF and other federal, state, local, tribal and private sector information sharing and counterterrorism efforts
C. Processing and Collation of Information	1. Information Collation—Fusion center analysts shall use the necessary and available tools to process and collate information and intelligence to assist with accurate and timely analysis.
D. Intelligence Analysis and Production	1. Analytic Products—Fusion centers shall develop, implement, and maintain a production plan that describes the types of analysis and products they intend to provide for their customers and partners (which, at a minimum, include Risk Assessments; Suspicious Activity Reporting; Alerts, Warnings, and Notifications; and Situational Awareness Reporting [see Sections I.A.2, 4, 5, and 6 for further details on these product types]), how often or in what circumstances the product will be produced, and how each product type will be disseminated.

3.2.8 Encounter Verification Process

The Encounter Verification (EV) process provides the Terrorist Screening Center Possible Missed Encounter Information and updates to state or U.S. government territory fusion centers. Although the Encounter Information Service Specification does not explicitly include encounter verification, a summary of the EV process is provided here as a reference for future service development.

The EV process would be used by state or U.S. government territory designated fusion centers to receive Possible Missed Encounter information resulting from hits by local law enforcement against an extract of the Terrorist Watchlist contained in the NCIC Known or Suspected Terrorist File (KST). The Possible Missed Encounters represent the hits to the extract of the Terrorist Watchlist which did not result in a communication between local law enforcement and TSC. This information may be used for tactical and analytical purposes.

The Possible Missed Encounters contain hit information composed of the law enforcement query initiated during the encounter and its respective response generated from the National Crime Information Center (NCIC). State or U.S. government territory designated fusion centers would receive this information at the same time as the Joint Terrorism Task Force (JTTF) via a joint notification process.

An encounter verification process would provide the following real-world effects:

1. The Possible Missed Encounter Information can be used tactically by a fusion center to further investigate a specific case in collaboration with the Joint Terrorism Task Force (JTTF) and the respective law enforcement agency.

2. The Possible Missed Encounter can be used for analytical purposes to provide information about Known or Suspected Terrorists (KST) traversing the jurisdiction of the fusion center and determining patterns. This facilitates situational awareness.

Additional information describing the Encounter Verification Process, including process flows and use case diagrams, is included in Appendix D of this document.

3.3 Service Model

3.3.1 Information Model

The Encounter Information Service will use the Terrorist Watchlist Person Data Exchange Standard (TWPDES) Encounter IEPD. The current version of the standard is 3.0.

Provided below is the summary information regarding the Encounter Information IEPD found in the TWPDES.

3.3.2 Overview

- **Biographic and Situational Information**—this information describes the encounter, including the identity presented, activity, location, and time.

- **Biometric Information**—this information may support "the automated recognition of individuals based on their biological and behavioral characteristics" (ISO, IEC JTC1 SC37 Working Group 1). For example, a person's fingerprints, iris scan, facial image, voice print, DNA, etc.

- **Analysis Information**—this information describes the relationship between one or more encounters and associated identities, including location and time proximity.

3.3.3 Encounter Nomination

An encounter request is created to describe an encounter and transmit it to an encounter management system.

The basic data required includes information describing who, when, where, and why:

- **Who:** Contains the identity information of the screenee, along with any associated individuals, tangibles, and references to any existing SARs.

- **When:** Date and time of the encounter.

- **Where:** Location of the encounter.

- **Why:** Watchlist, screening database searches which result in a "hit" as a possible match.

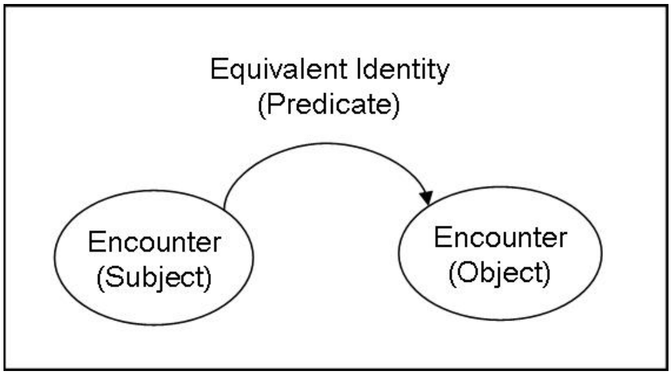
3.3.4 Encounter Disposition

An encounter disposition response conveys a high-level summary of the analysis of an encounter. This analysis includes a comparison of the information gathered through the encounter against identity information residing in one or more systems of record (SOR). The primary information conveyed in this message is an encounter disposition (e.g., "negative," or "inconclusive").

3.3.5 Encounter Analysis

An encounter analysis message describes the relationships between one or more encounters and their associated identities, thereby providing a strong chance that these relationships will result in enhanced situational awareness.

The example below represents encounter relationship based on equivalent identity.



For additional information, please reference: TSCEI SSP v.1.0.0/artifacts/service model/information model.

3.3.6 IEPD Reference

The information model of the service is based on the TWPDES 3.0 IEPD. The IEPD is available under the following folder of this Service Specification Package TSCEI SSP v.1.0.0/artifacts/service model/information model. For further information and new versions of the IEPD, please visit http://www.niem.gov/TWPDES.php.

3.3.7 Data Inputs

The data inputs for this service are a subset of the elements found in the TWPDES 3.0 Encounter Disposition Message. The list of elements is defined by the current MOU between TSC and the state or U.S. government territory designated fusion centers. Further information regarding the data inputs can be obtained by contacting the service specification owner organization.

3.3.8 Data Outputs

The data output of the service will be an acknowledgement message containing encounter identifier and metadata information (note that the acknowledgement is returned to TSC asynchronously).

3.3.9 Data Provenance

The data exchanged by this service would originate at the TSC. The TSC will send encounter information to the state or U.S. government territory fusion center responsible for the jurisdiction of the encounter location.

3.4 Behavior Model

3.4.1 Action Model

The information flow diagram below depicts, at a high level, the action model of the Encounter Information Service.

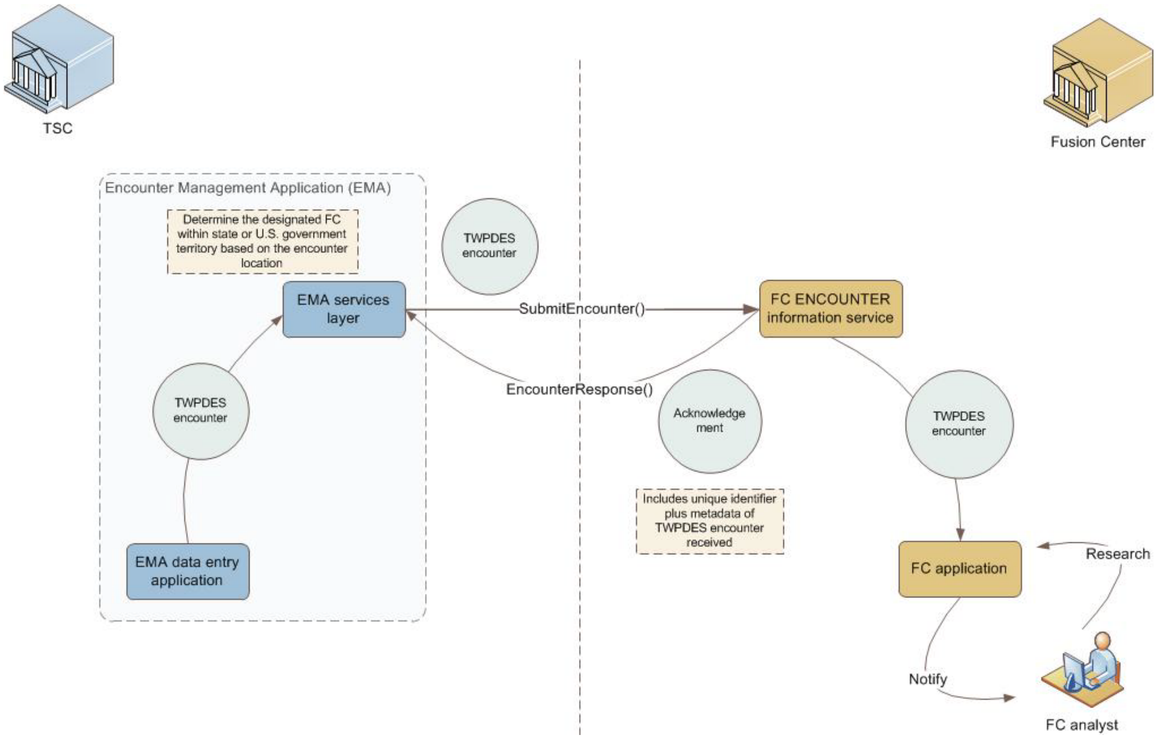

TSC
Fusion Center
Encounter Management Application (EMA)
Determine the designated FC within state or U.S. government territory based on the encounter location
TWPDES encounter
EMA services layer
SubmitEncounter()
FC ENCOUNTER information service
EncounterResponse()
TWPDES encounter
Acknowledge ment
TWPDES encounter
Includes unique identifier plus metadata of TWPDES encounter received
EMA data entry application
FC application
Research
Notify
FC analyst

Figure 4: Encounter Service Information Flow Diagram

The table below contains information about each individual service action.

Action Name	**SubmitEncounter**
Action Purpose	
This action will be used by the Encounter Management Application (EMA) Services Layer to send encounter information to the TSC Encounter Information Service implemented at the receiver (e.g., fusion center). The same action would be used to send updates of status information or updated encounter information.	
Action Inputs	**Action Outputs**
SubmitEncounterMessage	None
Action Provenance	
The provenance of this action is the same as the provenance of the service.	

Action Name	**EncounterResponse**
Action Purpose	
This action will be used by the receiver (e.g., fusion center) to send an acknowledgement message to the sender's (e.g. TSC) Encounter Information Service. The acknowledgement message leverages the WS-ReliableMessaging and WS-Addressing standards to provide status and correlation information.	
Action Inputs	**Action Outputs**
EncounterResponseMessage	None
Action Provenance	
The provenance of this action is the same as the provenance of the service.	

3.4.2 Process Model

The use case, sequence, and BPMN diagrams provided below describe in more detail the interaction between the service actions.

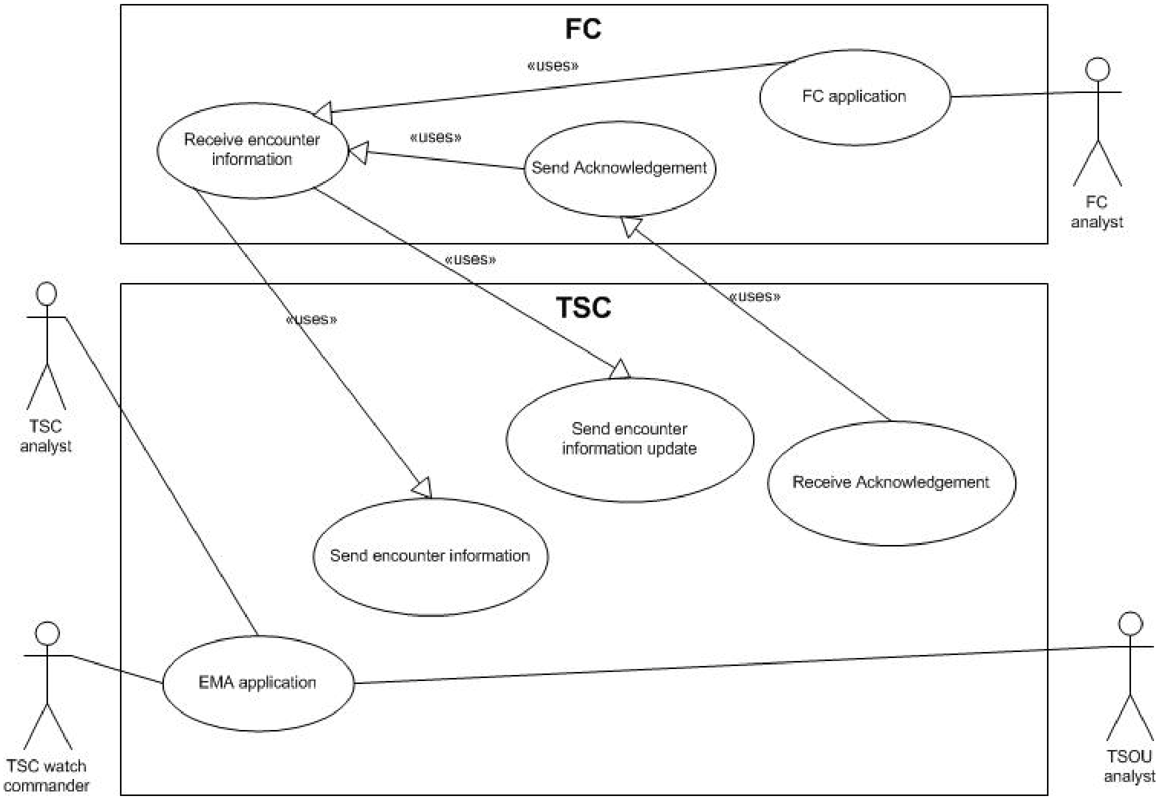


Figure 5: Encounter Information Service Behavior Model Use Case Diagram

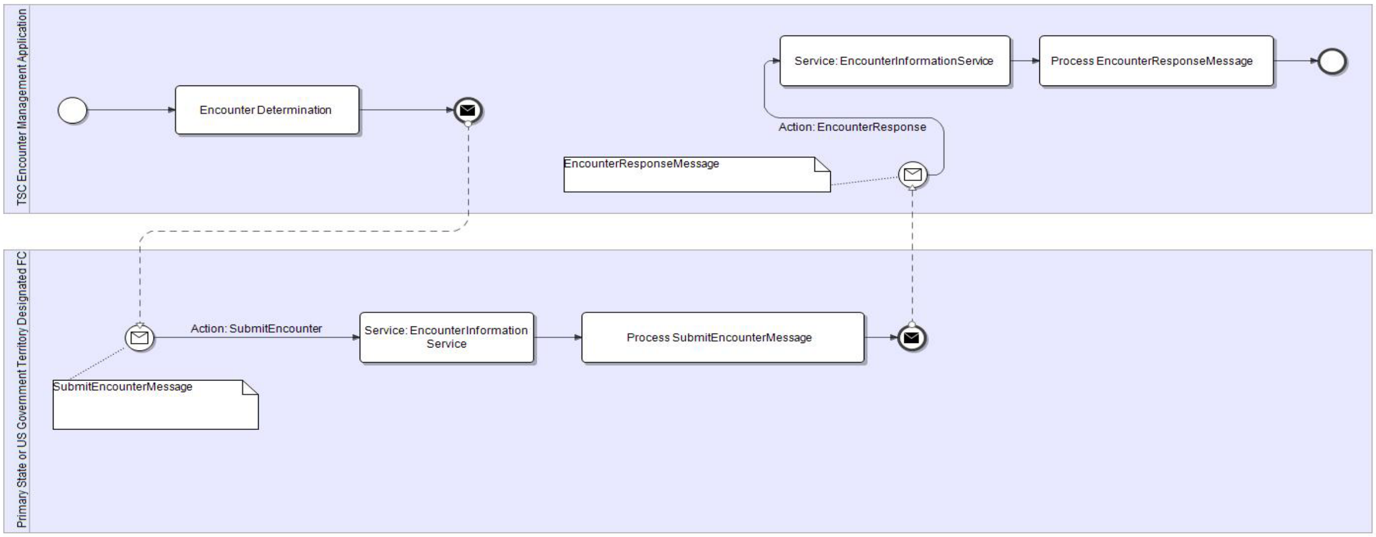

TSC Encounter Management Application
Encounter Determination
Service: EncounterInformationService
Process EncounterResponseMessage
Action: EncounterResponse
EncounterResponseMessage
Primary State or US Government Territory Designated FC
Action: SubmitEncounter
Service: EncounterInformation Service
Process SubmitEncounterMessage
SubmitEncounterMessage

Figure 6: Encounter Information Service Behavior Model BPMN Diagram

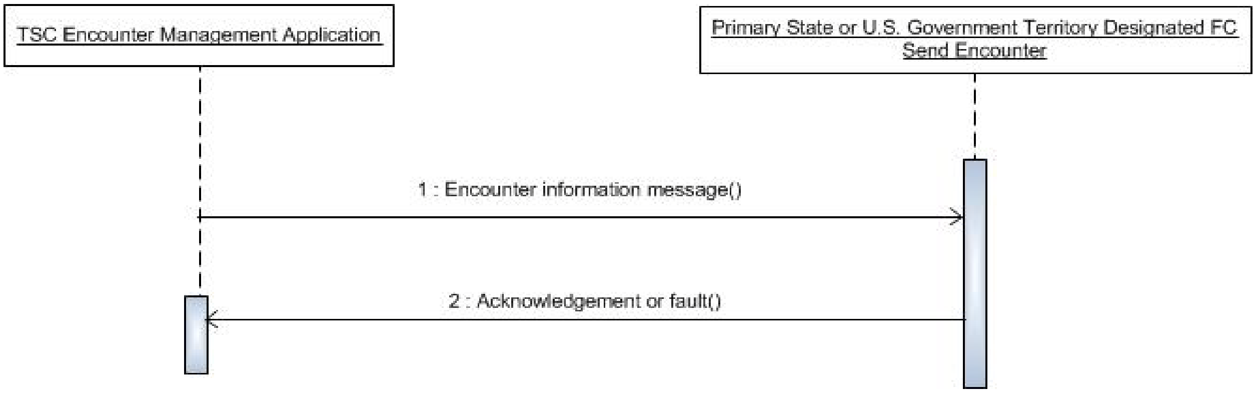

TSC Encounter Management Application
Primary State or U.S. Government Territory Designated FC Send Encounter
1 : Encounter information message()
2 : Acknowledgement or fault()

Figure 7: Encounter Information Service Behavior Model Sequence Diagram

For additional information, please reference TSCEI SSP v.1.0.0/artifacts/service model/behavior model.

Appendix A—References

Fusion Center Baseline Capabilities	http:// www.it.ojp.gov, documents, baselinecapabilitiesa.pdf
Fusion Center Guidelines	http:// www.it.ojp.gov, documents, fusion_center_guidelines.pdf
Terrorist Watchlist Person Data Exchange Standard (included in this package)	http://www.niem.gov/TWPDES.php
CJIS Security Policy	The CJIS Security Policy is considered to be Sensitive But Unclassified (SBU) material. This policy may not be posted to a public Web site, and discretion must be exercised in sharing the contents of the policy with individuals and entities who are not engaged in law enforcement or the administration of criminal justice. A copy may be obtained by contacting the state's CJIS Systems Officer (CSO).

Appendix B—Glossary

IAC	Information Analysis Center
FC	Fusion Center
TSC	Terrorist Screening Center
EMA	Encounter Management Application
Encounter	An Encounter is an interaction between a person of interest (POI) and law enforcement or screening agencies. A person of interest is one who possesses an identity that is associated with derogatory information residing in one or more systems of record (SOR) containing known and suspected terrorists (KST).
NCIC	National Crime Information Center
JTTF	Joint Terrorism Task Force
TSOU	Terrorist Screening Operations Unit
TSDB	Terrorist Screening Database
KST	Known or Suspected Terrorist File
NCIC	National Crime Information Center
ORI	Originating Agency Identifier
TWPDES	Terrorist Watchlist Person Data Exchange Standard
WS-Addressing	Web Services Addressing
WS-RM	Web Services Reliable Messaging

Appendix C—Document History

Date	Version	Editor	Change
02/21/2009	0.01.01	Iveta Topalova, Don Dinulos, Charles Carlton	Initial version
03/12/2009	0.01.05	Iveta Topalova	Updates to Service Specification
03/16/2009	0.01.05	Jim Douglas, Sam Ali	Review
03/18/2009	0.01.06	Iveta Topalova	Updates to Service Specification based on review
03/24/2009	0.01.06	Stan Larmee, Mark Korkolis	Review
03/25/2009	0.01.06	Jim Douglas	Review
03/26/2009	0.01.07	Iveta Topalova	Updates to Service Specification based on review
03/27/2009	0.01.08	IJIS Institute	Technical editing and formatting
03/27/2009	0.01.09	Iveta Topalova	Next revision
12/31/2009	0.05.01	Iveta Topalova, Collin Evans	Updates based on information from TSC
01/11/2010	0.9.2	Iveta Topalova	Updates based on review by TSC
01/18/2010	0.9.3	Iveta, Topalova, Collin Evans.	Final updates based on feedback from TSC
08/30/2010	0.9.4	Collin Evans	Separation of FC service interface and TSC service interface to accommodate asynchronous acknowledgements
07/05/2011	1.0.0	Collin Evans	Changed JRA references to GRA
04/11/2012	1.0.0	David Gillespie	Global Advisory Committee approved

Appendix D—Encounter Verification Process

Overview

Although the Encounter Information Service Specification does not explicitly include encounter verification, a summary of the EV process is provided here as a reference for future service development.

Encounter Verification Process Primary Flow

- In case a match occurs when law enforcement queries the KST, but a contact is not established between local law enforcement and TSC via a phone call, a batch process is run on the log files which represent the queries and responses for matches during KST queries. This process analyzes the hits and compares them with the Encounter Management Application (EMA) database. This process identifies a preliminary list of Possible Missed Encounters.

- The preliminary list of Possible Missed Encounters is turned over to a TSC Analyst to determine whether a call should have occurred.

- Upon an analyst's assessment that a call should have occurred, a joint notification* will be sent to the state or U.S. government territory designated fusion center and the JTTF. In the case of joint notification, fusion centers and JTTFs will be aware of the other agency working on the same case.**

**In the current process, if it is identified that a call should have occurred, the result is a discretional case lead sent to the field, which, in most cases, is sent to the Joint Terrorism Task Force (JTTF) or as a follow-up contact to the law enforcement agency that initiated the query.*

***Memoranda of understanding (MOUs) will be in place for regulating policies and procedures regarding the above joint notification.*

The process flow, use case, and sequence diagrams provided below depict the business process flow in more detail.

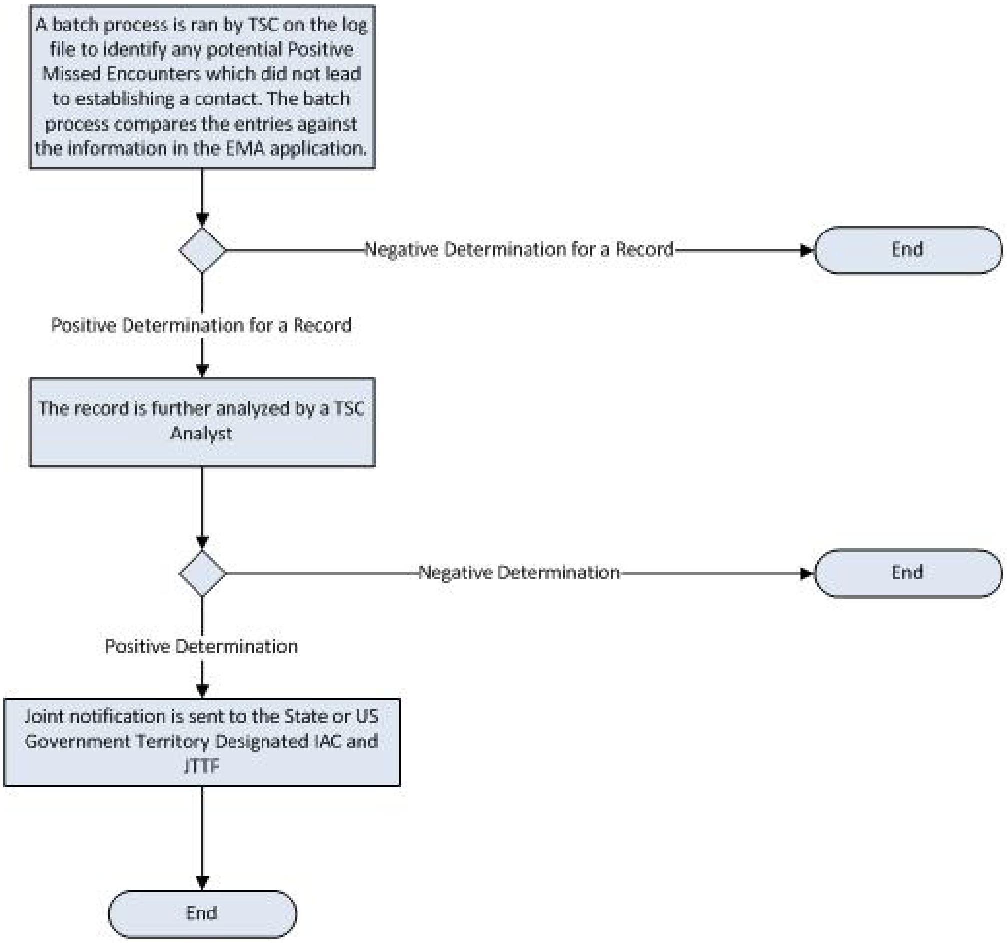

A batch process is ran by TSC on the log file to identify any potential Positive Missed Encounters which did not lead to establishing a contact. The batch process compares the entries against the information in the EMA application.
Negative Determination for a Record
End
Positive Determination for a Record
The record is further analyzed by a TSC Analyst
Negative Determination
End
Positive Determination
Joint notification is sent to the State or US Government Territory Designated IAC and JTTF
End

Figure 6: Encounter Verification Business Process Flow Diagram

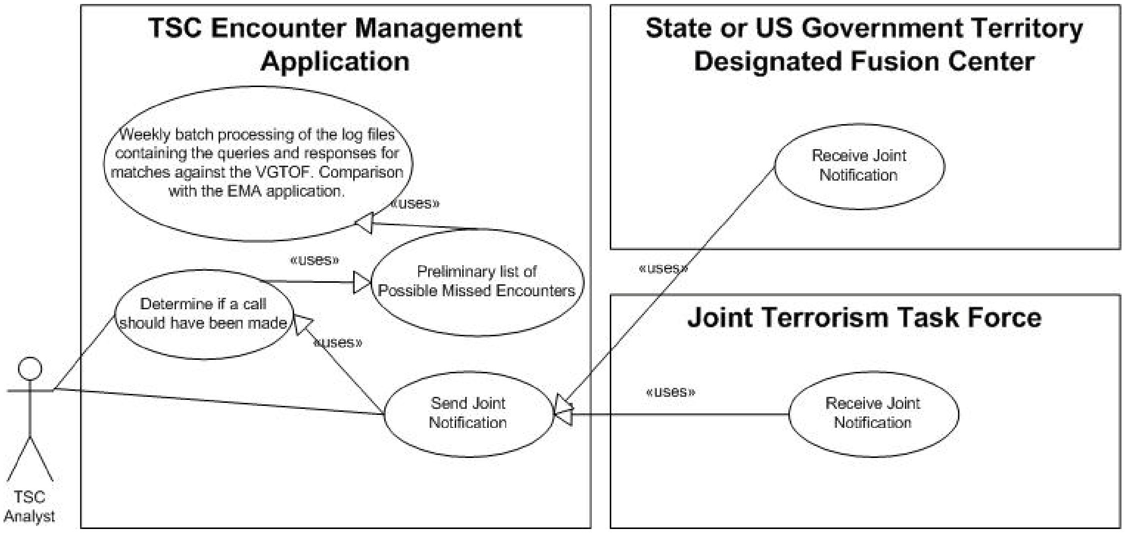

TSC Encounter Management Application
Weekly batch processing of the log files containing the queries and responses for matches against the VGTOF. Comparison with the EMA application.
«uses»
«uses»
Preliminary list of Possible Missed Encounters
Determine if a call should have been made
«uses»
Send Joint Notification
TSC Analyst
State or US Government Territory Designated Fusion Center
Receive Joint Notification
«uses»
Joint Terrorism Task Force
«uses»
Receive Joint Notification

Figure 7: Encounter Verification Use Case Diagram

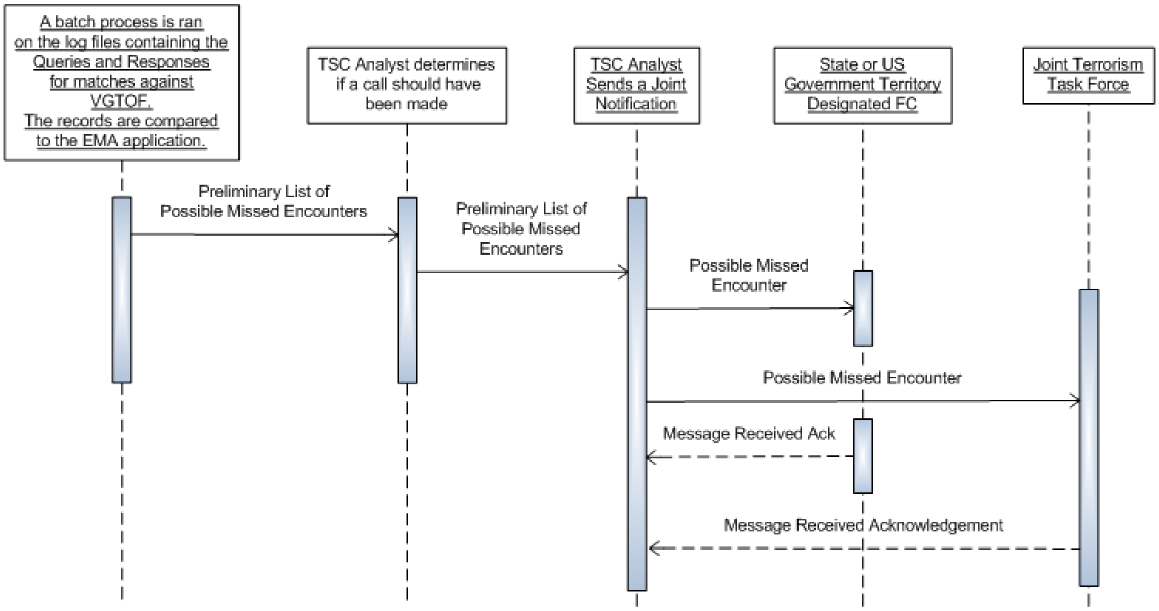

A batch process is ran on the log files containing the Queries and Responses for matches against VGTOF. The records are compared to the EMA application.
TSC Analyst determines if a call should have been made
TSC Analyst Sends a Joint Notification
State or US Government Territory Designated FC
Joint Terrorism Task Force
Preliminary List of Possible Missed Encounters
Preliminary List of Possible Missed Encounters
Possible Missed Encounter
Possible Missed Encounter
Message Received Ack
Message Received Acknowledgement

Figure 8: Encounter Verification Sequence Diagram

About Global

www.it.ojp.gov/global

The Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

For more information on Global and its products, including those referenced in this document, call (850) 385-0600 or visit http://www.it.ojp.gov/GIST.

About GSC

www.it.ojp.gov/gsc

In accordance with the founding principle of Global, the Global Standards Council (GSC) directly supports the broadscale exchange of pertinent justice and public safety information by promoting standards-based electronic information exchanges for the justice community as a whole. Specifically, the GSC develops, maintains, and sustains the standards—including this particular standard—associated with these aforementioned information exchanges. To further foster community participation and reuse, the GSC also receives, evaluates, and recommends to Global for adoption proposed standards submitted by Global consumers and stakeholders. In turn, the GSC employs an enterprise architecture approach for developing and maintaining the cohesive body of Global standards as one Global Standards Package (GSP), which can be accessed at http://www.it.ojp.gov/gsp.

http://www.it.ojp.gov/gsp

This project was supported by Grant No. 2009-DB-BX-K105 awarded by the Bureau of Justice Assistance, Office of Justice Programs, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.