Terrorist Watchlist Person Data Exchange Standard (TWPDES)
Version 3.0

Master Document

December 2009

Table of Contents

List of Figures

Document Revision History

Revision	Revised By	Date	Summary of Change
3.0 R0C0	C. J. Lee	12/4/2009	• Removed “Sensitive But Unclassified // For Official Use Only” markings in the document. • Removed references to “Controlled Unclassified Information”. • Updated Version 1.2b to Version 3.0 to mark the changes.

1 Introduction

1.1 Purpose

This document provides an overview of the Terrorist Watchlist Person Data Exchange Standard (TWPDES), version 3.0, including a brief description of its subordinate specifications.

1.2 Architectural Principles

TWPDES 3.0 leverages layered schema architectural principles, as shown in Figure 1 which enables the scope of TWPDES to expand, allowing additional mission domains to be accommodated without polluting the pure person and identity abstractions defined in the 1.0+ versions of TWPDES. Example mission domains include *encounter management*, *watchlisting* and future domains, such as *redress management*. As shown below, these additional mission domains are supported through layered abstractions and schemas, which are described as *subordinate component specifications* within TWPDES 3.0. The components are described in Information Exchange Package Documentation (IEPD), which comprises the TWPDES 3.0 package. These documents, along with associated schema definitions and sample messages, are listed in the *TWPDES3.0-Package-Description* document, which resides in the root of the TWPDES 3.0 delivery package archive file.

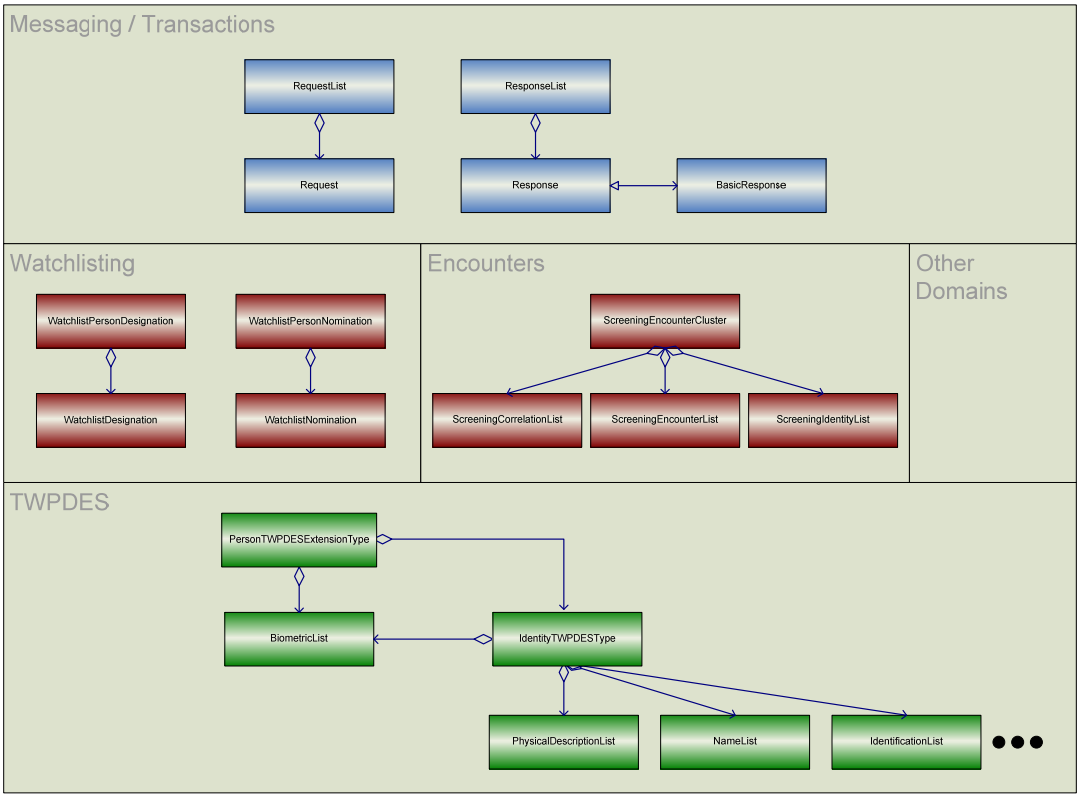

Figure 1: TWPDES Layered Schema Architecture

2 Subordinate Component Specifications

TWPDES 3.0, acts as a comprehensive standard for exchanging and sharing known or suspected terrorist (KST)-related information across the intelligence and law enforcement communities; both in the United States

and abroad. Though vast, this guide is necessary to successfully support all of the KST watchlisting requirements and KST encounter scenarios in the communities. These standards however are flexible and can be tailored to meet specific domain mission(s) without the necessity of extensive workarounds.

In addition, to allow for development beyond the scope of this guide, each component specification has built-in extension mechanisms to support on-going community efforts in the development of an inter-agency KST-data exchange model.

2.1 Biometric Data and Minor TWPDES Core Changes

One of the goals of TWPDES 3.0 is to provide not only biographic but also biometric data for the communication of known and suspected terrorist (KST) information across the law enforcement and intelligence communities in a single unified message. Using biometric and biographic data together can substantially improve the performance of identification and verification of known and suspected terrorists.

The primary design objective of the biometric data format in TWPDES is to allow biometric information to be exchanged between agencies, while leveraging existing standards and anticipating future standards and new biometric modalities as much as possible. Consequently, TWPDES 3.0 utilizes existing American National Standards Institute (ANSI)/National Institute of Standards and Technology (NIST)-Information Technology Laboratory (ITL) Biometric Standards Part 2, National Information Exchange Model (NIEM) and TWPDES.

Since the original TWPDES 1.2, several bugs in the TWPDES core schema were reported or identified during implementation of data exchanges using the standard. These defects are corrected in the TWPDES 3.0.

2.2 Message Transaction Specification (MTS)

The TWPDES 3.0 MTS component provides a flexible standard for the electronic exchange of TWPDES messages and related content between agencies and transactional systems deployed across the law enforcement and intelligence communities. Watchlist nominations, designations, encounters, and encounter dispositions are examples of content that can be conveyed via the MTS.

In developing the MTS, the primary goal was to satisfy the TWPDES conveyance requirements, while leveraging existing standards as much as possible. As such, the TWPDES MTS introduces a new standard, along with a prescription for leveraging three standards; two are established, commercial information technology standards: the Simple Object Access protocol (SOAP), which is maintained by the World Wide Web Consortium (W3C); and the e-business XML (ebXML) Messaging Service (ebMS), which is maintained by the Organization for the Advancement of Structured Information Standards (OASIS). Additional message exchange frameworks, such as the Emergency Data Exchange Language (EDXL) and Logical Entity eXchange Specifications (LEXS) standards; can be used to convey a TWPDES message.

2.3 Watchlisting Specification (WLS)

The TWPDES 3.0 WLS component provides a flexible standard for the communication of KST watchlisting information between agencies and transactional systems deployed across the intelligence and law enforcement communities. This includes both nominations to add entities to a terrorist watchlist and the subsequent dissemination of this watchlist to downstream agencies.

In developing the WLS, the primary goal was to allow a screening (or law enforcement) view of KST information to be exchanged between agencies, while leveraging existing standards as much as possible. As such, the TWPDES WLS introduces a new standard that utilizes existing TWPDES and National Information Exchange Model (NIEM) standards. When an element was created to support watchlisting, NIEM 2.0 data types were used whenever possible. If there was not an appropriate NIEM 2.0 type, TWPDES 3.0 types were used if available. If no types were found in either standard to support the requirements, new types were created. TWPDES 3.0 WLS IEPD is NIEM 2.0 compliant.

2.4 Encounter Specification

The Encounter Specification TWPDES3.0 component provides a comprehensive standard for the exchange of encounter information between agencies and transactional systems deployed across the law enforcement and intelligence communities. Each encounter describes an interaction with a *person-of-interest (POI).* A *POI* is one who possesses an identity that is associated with derogatory information residing in a *system-of-record (SOR)* containing watchlisted individuals. The Encounter specification is designed to convey encounter activity (e.g., *who*, *what*, *when*, *where*), any watchlist searches performed, and any encounter analysis results.

In developing the Encounter Specification, the primary goal was to allow intelligence, law enforcement and screening agencies to exchange information about encounters, while leveraging existing standards as much as possible. As such, the TWPDES 3.0 introduces a new standard that utilizes existing TWPDES and NIEM standards. When an element was created to support encounter information exchange, NIEM 2.0 data types were used whenever possible. If there was not an appropriate NIEM 2.0 type, TWPDES types were used if available. If no types were found in either standard to support the requirements, new types were created. TWPDES 3.0 Encounter Specification IEPD is NIEM 2.0 compliant.

2.5 Future Specifications

TWPDES 3.0 can accommodate additional business domains, as illustrated in Figure 1. Examples of such domains, include redress management, culturally-specific searching, workflow management, rich metadata and support for advanced analytics.

3 Glossary

Acronym	Definition
ebMS	ebXML Messaging Service
ebXML	e-business XML
EDXL	Emergency Data Exchange Language
IEPD	Information Exchange Package Documentation
KST	Known or Suspected Terrorist
LEISP	Law Enforcement Information Sharing Program
LEXS	LEISP Exchange Specification (old); Logical Entity eXchange Specifications (new)
MTS	Message Transaction Specification
NIEM	National Information Exchange Model
OASIS	Organization for the Advancement of Structured Information Standards
POI	Person of Interest
SOAP	Simple Object Access Protocol
SOR	System-of-Record
TWPDES	Terrorist Watchlist Person Data Exchange Standard
W3C	World Wide Web Consortium
WLS	Watchlisting Specification
XML	eXtensible Markup Language