APPENDIX 2

DHS Watchlist Service Concept of Operations
Version 1.0, September 10, 2009

DHS WATCHLIST SERVICE

CONCEPT OF OPERATIONS DOCUMENT

Document Version 1.0

Department of Homeland Security (DHS)

Office of the Chief Information Officer (OCIO) and the

Screening Coordination Office (SCO)

September 9, 2009

Revision Chart

Version	Primary Author(s)	Description of Version	Date Completed

Stakeholders Review Sheet

Reviewed by:

Justin C. Matthes
Director, Transborder Screening Initiatives
Screening Coordination Office
Office of Policy
Department of Homeland Security

September 10, 2009
Date

Robin C. Burke
Chief of Staff
Terrorist Screening Center

September 10, 2009
Date

TABLE OF CONTENTS

1. INTRODUCTION

Homeland Security Presidential Directive 6 (HSPD-6), *Integration and Use of Screening Information to Protect Against Terrorism,* issued September 16, 2003, directed the Attorney General to establish an organization to consolidate the Government's approach to terrorism screening. Concurrent with the signing of HSPD-6, several cabinet officials[1] and the then Director of Central Intelligence executed a Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism (TSC MOU) and established the Terrorist Screening Center (TSC) to consolidate the Government's approach to terrorism screening and to provide for the appropriate and lawful use of Terrorist Information, a term clarified by the inclusion of "Terrorist Identifiers" in a subsequent agreement of the parties. TSC became operational on December 1, 2003, and is administered by the Federal Bureau of Investigation (FBI) with support from the Intelligence Community, the Department of Defense (DoD), the Department of Homeland Security (DHS), the Department of Justice (DOJ), the Department of State (DOS), and the Department of the Treasury (Treasury).

Under HSPD-6 and the TSC MOU, the TSC was to develop and maintain a database, to the extent permitted by law, containing the most thorough, accurate, and current information possible about known and suspected terrorists. Nominations to the U.S. Government's consolidated terrorist watchlist must satisfy two basic requirements to determine whether an individual is known or suspected of being a terrorist, and thus, appropriate for watchlisting. First, the biographic information to support a known or suspected terrorist nomination must provide a sufficient amount of identifying data so that the identity of a person being screened can be matched to the identity of a known or suspected terrorist contained within the terrorist watchlist. Second, derogatory information regarding a known or suspected terrorist nomination must establish a reasonable suspicion that the individual is, or has, engaged in terrorism or terrorist activities. HSPD-6 requires that its implementation be consistent with the Constitution and applicable laws, including those protecting the rights of all Americans. The TSC created the Terrorist Screening Database (TSDB) to meet these goals.

The DHS *Policy for Internal Information Exchange and Sharing*, commonly known as the "One DHS" policy, serves as the DHS guiding principle to facilitate improved information sharing among DHS Components. More specifically, the "One DHS" policy serves to ensure that DHS personnel "have timely access to all relevant information they need to successfully perform their duties." "One DHS" directs all DHS Components in partnership with the DHS Chief Information Officer (CIO) to standardize the "technology used to describe, access, exchange, and manage information in our automated systems" so that we may "effectively use the most current and complete data available in support of our vital missions." DHS, in partnership with the TSC,

[1] The TSC MOU was signed by the Secretary of State, the Attorney General, and the Secretary of Homeland Security. Through the execution of subsequent addenda, the Secretaries of Defense and Treasury, the Director of National Intelligence, the Director of the Central Intelligence Agency, and the Directors of TSC and NCTC all became parties to the TSC MOU and its controlling Addendum B.

has undertaken the development of the DHS Watchlist Service (DHS WLS) in furtherance of achieving the "One DHS" goals. Once implemented, the DHS WLS will comprise three major common services that will facilitate the exchange of data from the TSC to DHS and its Components and Programs, in accordance with their missions related to terrorism screening. The DHS WLS underscores the objectives of the "One DHS" policy and further supports the Homeland Security Enterprise Architecture (HLS EA).

1.1. Background

Two DHS Components currently receive TSDB data directly from the TSC through a variety of manual processes that include utilizing email, web based applications, and Compact Disc (CD). The Transportation Security Administration (TSA) receives TSDB data from the TSC, pursuant to MOUs, in support of two DHS programs: 1) Secure Flight and 2) Transportation Threat Assessment and Credentialing (TTAC). The TSC also exports TSDB data to U.S. Customs and Border Protection (CBP) that is uploaded in TECS (formerly known as the Treasury Enforcement Communications System) through a legacy arrangement that the TSC assumed when it became operational.

Collectively, Secure Flight, TTAC, and TECS are herewith referred to as "legacy arrangements." These legacy arrangements remain binding unless superseded in the WLS MOU or any addenda thereto. TSC's legacy arrangement with TECS will be memorialized appropriately in the WLS MOU.

Additionally, the DHS United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program currently receives biometrics of Known and Suspected Terrorists from the FBI's Criminal Justice Information System under a DHS/FBI Interoperability MOU and from the Department of Defense, National Ground Intelligence Center (NGIC) as outlined in an MOU between DHS and NGIC. At this time, the National Counterterrorism Center (NCTC) and the TSC cannot receive and transmit fingerprints as part of the distribution of the watchlist to screening agencies; however, in response to National Security Presidential Directive (NSPD)-59/HSPD-24, *Biometrics for Identification and Screening to Enhance National Security*, the NCTC and the TSC are developing biometrics capabilities in phases, and ultimately, biometrics will be transmitted from the TSDB to the downstream customers for immediate use and check against existing biometric holdings.

1.2. Assumptions and Constraints

The following assumptions are used in planning for implementation of the WLS:

- The TSC will continue to provide thorough, accurate, and current TSDB data in accordance with HSPD-6, the TSC MOU and applicable addenda, and any other applicable law, regulation, or presidential directive.
- Legacy arrangements with DHS Components and Programs (provided in Appendix B) will be maintained and only the data delivery provisions will be superseded after DHS

officially notifies TSC in writing that data delivered as part of WLS meets DHS operational requirements. At that time, WLS will begin supplying TSDB data in support of the legacy arrangements identified in Appendix B. All other legacy arrangement requirements and expectations remain intact.

- DHS Components and Programs will adjudicate positive or inconclusive encounters with the TSC pursuant to the WLS MOU, legacy arrangements, and operational protocols.
- TSC's legacy arrangements with TECS will be memorialized appropriately in the WLS MOU.
- TSDB exports are only allowed to DHS Components and Programs that are a party to an existing legacy arrangements or successor systems (as defined in Appendix B). Any export of TSDB data to parties beyond existing legacy arrangements or successor systems requires prior, written approval of the TSC pursuant to the WLS MOU.
- Data will not be exchanged via DHS WLS in a production environment until the WLS MOU between DHS and TSC has been signed by both parties.

1.3. Overview of DHS WLS

1.3.1. System Description

The DHS WLS is comprised of the data, systems, services, and network connections required to develop a series of three major common services that coordinate the information exchange of data between the TSC and DHS Components and Programs. The intent of the DHS WLS is to automate and simplify the process of information exchange between the TSC and DHS to realize efficiencies, increase information security/assure data integrity, and ensure consistency of TSDB data used to accomplish the DHS screening mission. The first service pending immediate implementation, the WLS Data Broker, will allow DHS to assume the responsibility to provide TSDB data to only those DHS Components and Programs with existing legacy arrangements. The second service and subject to technical development, the DHS WLS Data Store with Query, will provide a persistent data store of the TSDB within a DHS server as a duplicate of the authoritative source for the then-current version of the TSDB that remains at TSC. This service will not be implemented until this ConOps is updated and agreed to by the TSC. The third service, the DHS WLS Encounters Data Broker, will provide a central mechanism to send and receive designation and encounter information from DHS Components and Programs back to the TSC. This service will not be implemented until the DHS Watchlist Service Concept of Operations Document (ConOps) is updated and agreed to by the TSC.

WLS Service	Description
WLS Data Broker	The DHS WLS Data Broker will ensure that DHS has an authoritative, traceable and reconcilable extract of the TSDB, which will be kept intact and unmodified in WLS, for use in DHS screening missions. WLS will serve as a main repository, feeding data to DHS Components and Programs with legacy arrangements by providing automation of the processes and procedures needed to ensure the optimization of data reconciliation between the TSC and DHS as defined in the attached WLS Interface Control Document (ICD). Any export of TSDB data to DHS Components and Programs beyond existing legacy arrangements or successor systems requires prior, written approval of the TSC pursuant to the WLS MOU. DHS will not manipulate the data within the TSDB extract received by WLS. The WLS will send TSDB updates as received from the TSC to DHS Components and Programs with existing legacy arrangements for internal processing. The Data Broker will ensure that each DHS Component and Program receives only the formatted records from the TSDB which it is authorized to use under the WLS MOU.
DHS WLS Data Store with Query	The WLS Data Store with Query will provide a persistent data store of the TSDB within a DHS server as a duplicate of the authoritative source for the then-current version of the TSDB that remains at TSC. Additionally, this phase will deliver the services required for DHS Components and Programs to query this data store, either for a single entry, or in order to process a batch entry such as a manifest. This DHS WLS Data Store with Query service will be designed to ensure that queries against the data stores can be executed using the minimum data elements as defined in the DHS Core Biographic Person Data Elements (CBPDE) standard and supporting the DHS screening mission. It will be developed to ensure the support of controlled access to the queries based on screening requirements for the DHS Components and Programs as agreed to with the TSC.
DHS WLS Encounters Data Broker	The DHS WLS Encounters Data Broker will provide a central mechanism to send and receive designation and encounter information from DHS Components and Programs back to the TSC. Per the WLS MOU, DHS will electronically notify the TSC if an individual identified during the screening process is determined to be a positive or inconclusive match to one or more identities in the TSDB (defined as an Encounter). DHS will also provide, consistent with TSC MOU Addendum B, Terrorist Identifiers about the encountered individual to enable TSC to make a final adjudication (positive or negative identity match to the TSDB). This service will include the design, development and implementation of bi-lateral, standardized information exchange between DHS systems approved to receive and maintain TSDB data that results from an encounter of a person as listed in the TSDB. The standardized format for the encounter will comply with the then-current Terrorist Watchlist Person Data Exchange Standard (TWPDES) format developed and published by TSC. The DHS Components and Programs that currently report encounters to the National Counterterrorism Center (NCTC) or TSC through semi- or fully- automated means will be the focus of the first set of user requirements, followed by requirements of Components and Programs that do not yet have access for reporting such encounters. Pursuant to the WLS MOU, TSC will make the final identity match determination regarding Potential Matches and Inconclusive Matches. This determination will be a "positive," "negative," or "inconclusive" match.

1.3.2. System Scope

The WLS will connect to the following legacy systems or their successors as described below. The export of TSDB data to other DHS Components and Programs without a legacy arrangement requires prior, written approval of the TSC pursuant to the WLS MOU.

1.3.2.1. TSA Office of Transportation Threat Assessment & Credentialing (TTAC) Systems

TTAC offers enrollment and credentialing services that provide physical or virtual credentials used by an individual to gain unescorted access to special, sterile and/or secure areas in all modes of transportation after successfully completing a security threat assessment that may include all or a combination of legal status and criminal history records checks as well as checks for ties to terrorism. TTAC also performs end-to-end program management for aviation, maritime, and surface programs with core capabilities in enrollment services, vetting operations, adjudication and credential management.

1.3.2.2. TSA Secure Flight

Secure Flight is a DHS airline passenger screening program that automates the comparison of certain passenger information from Secure Flight Passenger Data elements required to be transmitted by covered air carriers under the Secure Flight Final Rule.

1.3.2.3. CBP TECS

TECS, an updated and modified version of the former Treasury Enforcement Communications System, is a CBP system established as an overarching law enforcement community information collection, analysis, and sharing environment which provides authorized users within DHS and other federal agencies with law enforcement and anti-terrorism community missions with access to computer-based enforcement files of common interest. TECS databases contain temporary and permanent enforcement, inspection and intelligence records relevant to the antiterrorism and law enforcement mission of CBP and numerous other federal agencies that it supports.

1.3.2.4. US-VISIT

The US-VISIT program through the DHS Automated Biometric Identification System (IDENT) provides U.S. visa-issuing posts and U.S. ports of entry with biometric matching capabilities that enable the U.S. government to establish and verify the identity of visitors and check biometric data on those applying for admission to the United States against government databases to identify suspected terrorists, known criminals, individuals otherwise inadmissible to the U.S., or individuals who have previously violated U.S. immigration laws. Biometrics collected through the US-VISIT program, and linked to specific biographic information, enables a person's identity to be established, and then verified, by the U.S. Government.

1.3.3. Compliance

DHS WLS will fully support the "One DHS" information sharing directives and the HLS EA,

and as such, will utilize the TSC's Terrorist Watchlist Person Data Exchange Standard (TWPDES) schema to send and receive information, as well as the DHS Core Biographic Person Data Elements (CBPDE). TWPDES and the CBPDE Information Exchange Package Documents (IEPDs) follow the standards of the National Information Exchange Model (NIEM), thereby ensuring that DHS WLS will support DHS information sharing segment architecture, directives, and standards for communications between government organizations. Additionally, DHS WLS will be considered part of the DHS Screening Segment Architecture (SSA), and as such, will be designed to ensure alignment to the DHS Credentialing Framework Initiative (CFI), specifically the CFI's high priority suites: DHS Screening Suite; DHS Account Setup/Enrollment Suite; and DHS Encounter/Status Validation Service Suite.

Further, the WLS will be developed in compliance with the privacy and data protection requirements outlined in the WLS MOU as well as the Privacy Impact Assessment (PIA) for the WLS. DHS will internally determine authoritative purpose and privacy act compliance before forwarding new system requests to the TSC for review and approval. Privacy protection and information security details are provided in the WLS Interface Control Document (ICD).

1.3.4. Stewardship of DHS WLS

DHS WLS is employing a multi-tiered stewardship model. The DHS Screening Coordination Office (SCO) will be the primary point of contact (POC) regarding the WLS program. The following descriptions of various steward assignments within DHS are for informational purposes and ease of communication with program areas.

Steward Designation	Steward Role
Business Steward	The DHS SCO will be responsible for managing the overarching framework for DHS screening programs and will ensure the coordination and gathering of WLS requirements from DHS Components and Programs with screening missions, negotiating and governing via the WLS MOU, and generally acting as the policy lead for DHS WLS.
Technical Steward	The DHS Office of the Chief Information Officer (OCIO), partnering with the SCO, will ensure that DHS WLS complies with DHS Enterprise Architecture requirements, and will assist in facilitating technology issues for the SCO with the Technology Service Steward. The OCIO will also assist with initial requirements and program management.
Technology Services Steward	The Passenger Systems Program Office (PSPO) of U.S. Customs and Border Protection (CBP), Office of Information and Technology (OIT) will document requirements, design, develop, and put DHS WLS into production. It will also be responsible for developing and maintaining the ICD in coordination with the TSC.

1.3.5. WLS Change Management

The purpose of the Watch List Service (WLS) Configuration Management Plan (CM Plan) is to disseminate guidance and information related to the identification, control, and monitoring of

controlled WLS requirements and documents. As such, the CM plan specifically addresses the following requirements:

- Process for identifying which applications/systems are in-scope and out-of-scope;
- Process for identifying which requirements are in-scope and out-of-scope;
- Process to be employed for problem resolution; and
- Process for effectively communicating, tracking and managing changes introduced into the WLS.

Those processes will be governed through a configuration control board (CCB), as defined in the CM Plan, which will be composed of stakeholders (see Section 7 for listing of stakeholders), including both technical and operational leads:

- WLS Program Manager
  - DHS SCO
  - WLS Program Management Office (DHS OCIO EDMO)
- CBP PSPO Project Manager
  - Technical Lead
  - Application Lead
- Secure Flight Project Manager
  - Technical Lead
  - Application Lead
- TTAC Project Manager
  - Technical Lead
  - Application Lead
- TSC Project Manager
  - Technical Lead
  - Operational Lead

Added as stakeholders will be representatives from future DHS Components and Programs that receive TSDB exports through the WLS, but only after DHS has received prior, written TSC authorization of new stakeholder access to TSDB exports, TSC pursuant to the WLS MOU.

1.4. Operational Documents

- Memorandum from the Secretary of DHS to all DHS Components, "DHS Policy for Internal Information Exchange and Sharing," February 1, 2007 ("One DHS" Memo).
- DHS Directive 102-01-001: Appendix B DHS System Engineering Lifecycle Document, Interim Version 1.9, November 7, 2008.
- Configuration Management Plan - DHS WLS Configuration Management Plan Document 1.2, October 30, 2008.
- Interface Control Document (ICD) for TSC Terrorist Screening Database (TSDB) Export to Department of Homeland Security (DHS) Watchlist Service (WLS), April 8, 2009.
- Applicable MOUs listed in Appendix B

- WLS MOU.

1.5. Glossary and Acronyms

A glossary of terms / list of acronyms used in this document is provided as Appendix A.

2. GOALS, OBJECTIVES, AND RATIONALE

2.1. Goals

The goals for the DHS WLS are to:

- Develop and implement a single system automated or semi-automated information exchange of the TSDB data between DHS and the TSC;
- Increase the assurance and consistency of data quality between TSC and DHS through the capability for automated reconciliation;
- Develop and implement an audit capability that meets the TSC and DHS agreed-upon requirements that ensures lawful, secure and appropriate access to and use of TSDB data;
- Ensure no degradation in current service levels;
- Utilize an integrated single source of data from TSC for both biographic and biometric information that is to be used by DHS screening organizations; and
- Optimize the use of Service Oriented Architectures (SAOs) to reduce the number of DHS connections to the TSC for information sharing, thereby realizing cost avoidance or savings for both DHS and the TSC.

2.2. Major Milestones and Planned Objectives

The important major milestones or planned objectives for the WLS are as follows:

Phase I of the WLS will include the deployment of the WLS Data Broker to those DHS Components and Programs with existing legacy arrangements. Initially, the WLS Data Broker service will be implemented as a *bulk load update* to TECS; the WLS Data Broker service will then be deployed as a *transactional service* to Secure Flight and TTAC as managed through the WLS change management process (see Section 1.3.5.). Per the WLS MOU, TSC will continue to provide TSDB records in accordance with existing legacy arrangement procedures until DHS provides notice to TSC that the WLS has been fully implemented. At that time, the data delivery provisions in the legacy arrangements will be superseded by the WLS MOU. All other provisions in the legacy arrangements will remain in effect until subsequently modified by the parties. Any new TSDB exports to DHS Components and Programs that are not a party to existing legacy arrangements require prior, written approval of the TSC pursuant to the WLS MOU.

Phase II and Phase III of the WLS are the development of the WLS Data Store with Query and the Encounters Data Broker (see Section 1.3.1.). The scope of the development of those subsequent phases will be managed through the WLS Configuration Management Plan, as discussed in Section 1.3.5 of this document.

2.3. Rationale

The rationale for the DHS WLS is to ensure that the following anticipated implementation benefits are realized:

- Timely and accurate information is provided to authorized DHS Components and Programs through a single, common channel;
- Use of a single, authoritative copy, provides accurate data sets to be leveraged consistently for authorized DHS Components and Programs;
- Costs are reduced for obtaining, managing, and sharing data by both TSC and DHS; and
- Cyber Security protection is increased by moving to the DHS infrastructure.

3. WORK PROCESSES TO BE AUTOMATED / SUPPORTED

This section briefly describes the work processes to be automated and/or supported with the implementation of the common services of DHS WLS.

3.1. Automation of Information Exchange between TSC and DHS

The TSC, in its goals to standardize information exchange, increase the integrity of data across its customers, and reduce the cost of data dissemination, is moving towards a single, downstream data feed to each consumer, and single, upstream data feed of encounter information from its consumers in a consistent format.

The automation of the information exchanges between the TSC and DHS will improve the integrity of the data used by DHS Components and Programs with screening missions, ensuring they are using the authoritative data source, the TSDB, in their decision making process. As DHS Components and Programs report encounters to the TSC, the TSC will receive the encounter data in the standardized format transmitted electronically from the DHS organizational elements with screening missions.

The new automated information exchange process for both incoming and outgoing data will be implemented as agreed upon to include the delivery of the required data from the TSC, the capability to produce audit records for traceability purposes, and the support for greater reliability by using guaranteed messaging delivery and automated reconciliation between both parties as outlined in the ICD.

DHS Components and Programs will adjudicate positive or inconclusive encounters with the TSC pursuant to the WLS MOU, legacy arrangements, and operational protocols.

3.2. Shift of Business Rules Automation

Currently, the TSC implements DHS Component and Program specific business rule logic into each application level interface with DHS. As TSC and DHS move to the single exchange standard, the responsibility of applying program-specific business rule management will be shared by WLS and DHS Components and Programs with a screening mission. This will eliminate the need for TSC to maintain an application level interface with individual DHS

Components and Programs, and will simplify the process of distributing data to authorized users.

3.3. Encounter Management

If an individual is identified during a DHS screening process who is a positive or inconclusive match to one or more identities in the TSDB, the DHS Component or Program will notify the TSC consistent with the provisions of any applicable legacy arrangements or the WLS MOU. The notification will include Terrorist Identifiers about the individual and identities in the TSDB to enable TSC to make a final adjudication (positive or negative identity match to the TSDB). If the TSC determines that an individual does not match an identity in the TSDB, the TSC will advise the appropriate DHS Component or Program. TSC will retain an electronic record of all referrals from DHS (whether positive or negative matches) in its encounter management database.

If the TSC determines that an individual matches an identity in the TSDB, the TSC will immediately notify the FBI's Terrorist Screening Operations Unit (TSOU). TSC and TSOU will then review the match based on current procedures. TSOU will coordinate the proper operational response, if any, between DHS, the FBI, the nominating agency, and other relevant agencies or entities. After the operational response has been coordinated, DHS will share with TSC the results of any actions it takes resulting from a positive TSDB match (i.e., denial of Hazmat application). DHS will also collect and share encounter information consistent with its legal authorities and Addendum B to the TSC MOU.

TSC will also notify TSOU of any indeterminate or inconclusive matches. If, after all relevant information is reviewed and an individual cannot be conclusively matched with an identity in TSDB, TSC will advise the DHS Component or Program accordingly.

4. HIGH-LEVEL FUNCTIONAL REQUIREMENTS

4.1. High-Level Functional Requirements

For this initiative, requirements have been and will continue to be gathered using various methods including interviews, focus groups, and walkthroughs with DHS staff, thus ensuring DHS WLS will support DHS modernization goals. The requirements encompass both basic and specific issues concerning the needs for DHS WLS, which include the system interface for screening functions, the administrative interface for the system administrators, database requirements, and other needs requiring software functionality and access controls.

Currently, the requirements for the rollout of the first of three major common services, DHS WLS Data Broker, are intended to support the following use cases:

- Establish Connections with DHS Components
- Manage Administrator Access
- Manage WLS Consumer Definitions
- Manage Consumer Watchlist Data Refresh
- Distribute Watchlist Designation

- Respond to Watchlist Designation
- Distribute Consumer Watchlist Designation
- Respond to Consumer Watchlist Designation
- Reconcile Watchlist System Identifiers
- Manage System Reconciliation
- Reconcile Watchlist Identities
- Manage Identity Reconciliation
- Reconcile Consumer Watchlist System Identifiers
- Manage Consumer System Reconciliation
- Reconcile Consumer Watchlist Identities
- Manage Consumer Identity Reconciliation

Additional information will be provided in the ICD and the system design documentation developed during the system engineering life cycle process.

4.2. High-Level Major Common Services

Data sharing between applications will be supported by a data transport foundation within the system. The high-level major common services, defined in Section 1.3.1 of this document and illustrated in Figure 1 below, support the current and future vision of the information sharing system and Service Oriented Architecture (SOA) capabilities. Access to data will be restricted by role and in accordance with the WLS MOU executed between TSC and DHS.

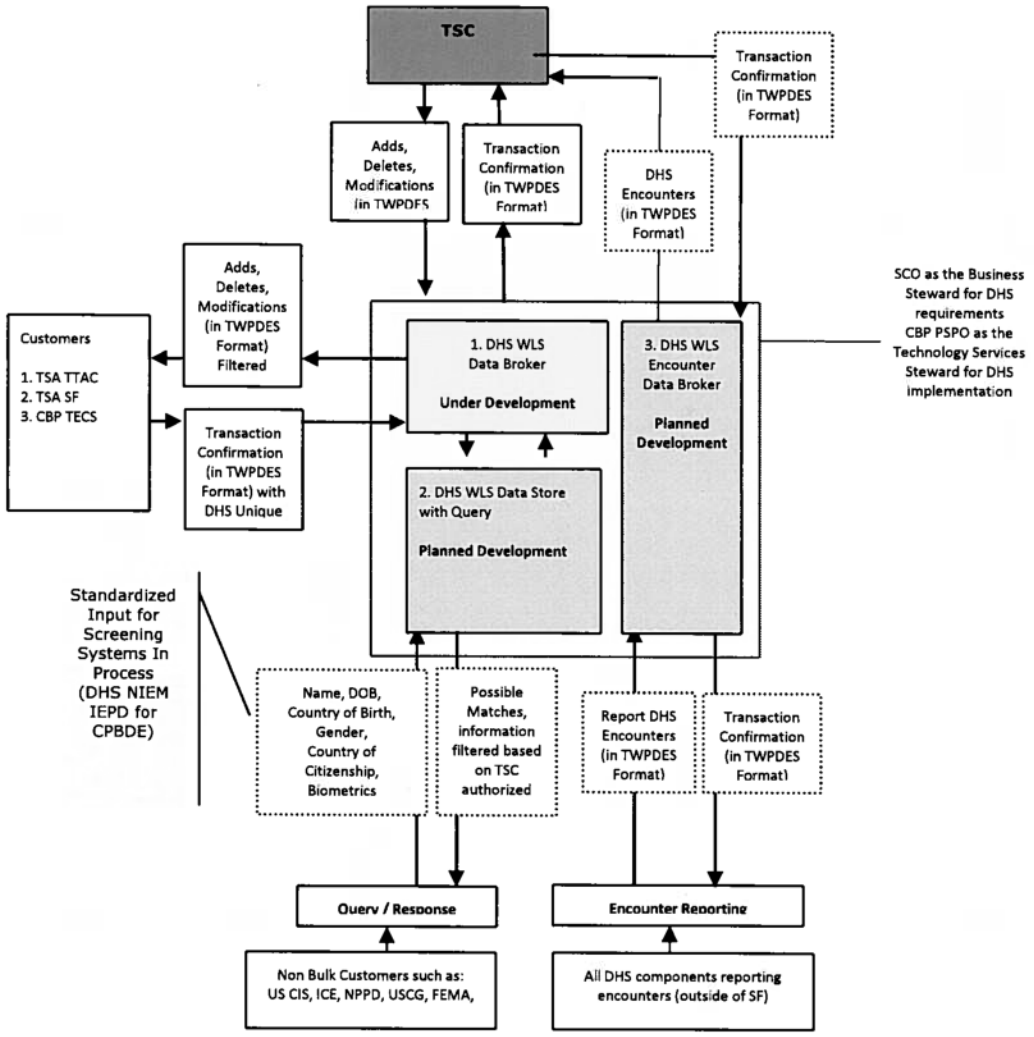

Figure 1: High Level Major Common Services for the DHS WLS Service

5. HIGH-LEVEL OPERATIONAL CAPABILITIES

5.1. Operational Capabilities

5.1.1. CBP Enterprise Service Bus (ESB) and Service-Oriented Architecture (SOA)

DHS WLS will leverage the CBP Enterprise Service Bus (ESB). The details describing the CBP ESB components being leveraged in support of WLS transactional reconciliation process are defined in the WLS ICD.

5.1.2. Deployment and Support Requirements

The DHS WLS will reside on the CBP ESB. As such, the DHS WLS will be responsible for the reliable and secure transfer of person-related terrorist screening information from TSC's TSDB to DHS WLS consumers using CBP ESB core technology as the foundation for the data

brokering. CBP currently supports the deployment of services on the ESB and has an established and regimented service deployment strategy.

5.1.3. Configuration and Implementation

Configuration and implementation requirements for the DHS WLS will follow existing DHS Systems Engineering Life Cycle / CBP Systems Life Cycle Standard Operating Procedures. A configuration control board and process is further defined in the DHS WLS CM Plan.

5.1.4. System Environment

The System Environment for the WLS Data Broker Service is defined in the DHS WLS Detailed Design Document and WLS ICD.

6. HOMELAND SECURITY ENTERPRISE ARCHITECTURE COMPLIANCE

The DHS WLS is part of a wider governmental effort to create an environment within the Department that promotes information sharing and collaboration, and moves towards standardized information exchange. As such, the services developed as part of the DHS WLS will be in compliance with the following guidance approved by the DHS Enterprise Architecture Center of Excellence, and necessitated by applicable privacy and civil liberties requirements:

- *DHS SOA Framework*, version 1.1;
- *DHS Information Sharing Segment Architecture*, version 1.0;
- *DHS Enterprise SOA Header*, version 1.0;
- *DHS Core Biographic Person Data Element (CBPDE) standard*, version 1.0 or later; and
- *Terrorist Watch Person Data Exchange Standard (TWPDES)*, version 1.2b or later.

6.1. DHS Service Oriented Architecture Framework, version 1.1

The DHS SOA Framework 1.1 provides the minimum framework standards for the development of all DHS SOA services. CBP will conform to the DHS SOA Framework, version 1.1 or later including the application of Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL), and other ESB standards. Additionally, the services developed as part of this effort will be Java 2 Enterprise Edition (J2EE) compliant and designed for deployment on the CBP enterprise service bus.

6.2. HLS Information Sharing Segment Architecture, version 1.0 or later

The Homeland Security Information Sharing Segment Architecture sets the strategy and foundation for operational information sharing that will to be followed across all mission areas to implement the DHS Information Sharing Environment. The WLS will conform to the HLS ISSA.

6.3. DHS Enterprise Service Oriented Architecture (SOA) Header, version 1.0

The DHS Enterprise SOA Header framework details the three levels of standardization within a SOA based message. The goal of header standardization is to ensure interoperability across the

federation of DHS service buses allowing for auditing, logging, and processes consistently within the enterprise. The DHS WLS will conform to the DHS Enterprise SOA Header Specification.

6.4. Core Biographic Person Data Element (CBPDE)

The CBPDE IEPD defines a set of core biographic data elements for use in biographic identity-related message exchanges developed for use in DHS programs. Consistent use of these elements across all DHS Components and business processes establishes a basis for department-wide identity information sharing and directly supports Secretary's priority goal 12.2 and the DHS Policy for Internal Information Exchange and Sharing.

6.5. Terrorist Watchlist Person Data Exchange Standard (TWPDES)

The Terrorist Watchlist Person Data Exchange Standard (TWPDES) serves as a baseline standard for the sharing of terrorism information. It will enable the transfer of information in a consistent, identifiable manner, specify common security classification and handling markings, and support both human and automated sharing of terrorism information to multiple classification levels.

7. STAKEHOLDERS ROLES AND RESPONSIBILITIES

A high-level overview of the stakeholders and their respective roles in the DHS WLS solution is described below.

Stakeholder	Role	Responsibility
DHS SCO	Business Steward	The DHS SCO will be responsible for managing the overarching framework for DHS screening programs and will ensure the coordination and gathering of WLS requirements from DHS Components and Programs with screening missions, negotiating and governing via the WLS MOU, and generally acting as the policy lead for DHS WLS.
DHS OCIO	Technical Steward (Technical Oversight and Program Management Support)	The DHS Office of the Chief Information Officer (OCIO), partnering with the SCO, will ensure that DHS WLS complies with DHS Enterprise Architecture requirements, and will assist in facilitating technology issues for the SCO with the Technology Service Steward. The OCIO will also assist with initial requirements and program management.

DHS CBP PSPO	Technology Services Steward	The Passenger Systems Program Office (PSPO) of U.S. Customs and Border Protection (CBP) will document requirements, design, develop, and put DHS WLS into production. It will also be responsible for developing and maintaining the WLS ICD in coordination with the TSC. As the technology services steward for the DHS WLS, the CPB PSPO will: Provide full life cycle project management support for each phase of implementation. • Conduct requirements gathering and management. • Provide architecture, design, and development resources. • Provide testing support, to include development of test plans and management of user acceptance testing activities. • Provide identification and project management of network support to include planning, selection, and implementation of network connectivity required to integrate TSC and DHS systems. • Provide internal network connectivity. The CBP Office of Information and Technology will maintain audit responsibilities to preclude unauthorized access to the WLS. Each DHS Component and Program that receives an export of the TSDB via WLS pursuant to the WLS MOU and its executed addenda will ensure appropriate access to the TSDB data stored in their system(s) and will certify as such annually to the WLS Business Steward.
DHS US-VISIT CIO	WLS Consumer and Technical Service Steward (Biometric)	As the technical steward for the Biometric portions of the TSDB data for DHS, the US-VISIT Office of Technology will develop the mechanism for consuming the WLS Biometric information for the purposes of receiving and storing TSDB Biometrics data. As such, US-VISIT will: • Provide information as needed for requirements. • Provide architecture, design, and development resources to develop the mechanism for consuming the Biometric information using TWPDES (See Appendix C of this document). • Provide testing support, to include development of test plans and management of user acceptance testing activities. • Provide an application administrator. • Provide identification and project management of network support to include planning, selection, and implementation of network connectivity required to integrate the DHS WLS and IDENT. • Provide internal network connectivity.
DHS Components and Programs with a Screening Mission	WLS Consumer	DHS Components and Programs with a screening mission will: • Provide information as needed for requirements. • Validate work products related to information sharing with DHS. • Provide network integration support to include planning, selection, and implementations of network connectivity required to connect to the DHS WLS. • Integrate relevant screening systems to DHS WLS services. • Provide an application administrator, server administrator, and a configuration management administrator.

TSC	Data Aggregator	As the main Service provider for the TSDB data to DHS, the TSC will: • Provide information as needed for requirements. • Validate work products related to information sharing with DHS. • Provide network integration support to include planning, selection, and implementation of network connectivity required to integrate TSC and DHS systems. • Provide an application administrator, server administrator, and a configuration management administrator.

Appendix A – Glossary of Terms

Acronym	Description
ATO	Authority to Operate
CBP	U.S. Customs and Border Protection
CCB	Change Control Board
CIO	Chief Information Officer
CM Plan	WLS Configuration Management Plan
CONOPS	Concept of Operations
COOP	Continuity of Operations
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
DHS	Department of Homeland Security
DHS Components and Programs	Individual agencies or offices of DHS that utilize TSDB records for authorized screening purposes. References to DHS shall encompass DHS Components and Programs, unless otherwise specified.
DOB	Date of Birth
Encounter	Information on a positive or inconclusive match to the TSDB through the screening process
HSPD	Homeland Security Presidential Directive
ICD	Interface Control Document (ICD); the document governing the interface between the Parties and describing the requirements and specifications necessary to support their exchange of information.
IPT	Integrated Project Team
IRTPA	Intelligence Reform and Terrorism Prevention Act (of 2004)
ISSO	Information System Security Officer
IT	Information Technology
LEO	Law Enforcement Officer
Legacy Systems	TTAC Systems, Secure Flight, TECS and IDENT
NTC	National Targeting Center (DHS)
O&M	Operations and Management
OCISO	Office of the Chief Information Security Officer
PII	Personally Identifiable Information
PSPO	Passenger System Program Office, a US CBP
SCO	Screening Coordination Office (DHS)
SOA	service oriented architecture
Successor Systems	Successor Systems conduct the same or materially similar screening to that of legacy systems.
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TSOC	Transportation Security Operation Center
TSOU	Terrorist Screening Operation Unit
TTAC	Office of Transportation Threat Assessment and Credentialing
XML	Extensible Markup Language

Appendix B – TSC and DHS Component and Program Legacy Arrangements.

1. Memorandum of Understanding between the Transportation Security Administration and the Terrorist Screening Center regarding the use of Terrorist Information for Security Threat Assessment Programs, effective May 12, 2006 (TTAC).

a. Addendum A to the Memorandum of Understanding between the Transportation Security Administration and the Terrorist Screening Center regarding the use of Terrorist Information for Security Threat Assessment Programs, effective September 29, 2006 (TTAC).

b. Addendum B to the Memorandum of Understanding between the Transportation Security Administration and the Terrorist Screening Center regarding the use of Terrorist Information for Security Threat Assessment Programs, effective December 16, 2006 (TTAC).

2. Memorandum of Understanding between the Terrorist Screening Center and the U.S. Department of Homeland Security, through the Transportation Security Administration, regarding the Secure Flight Program, effective December 30, 2008.

3. Memorandum of Understanding between the U.S. Department of Homeland Security, National Protection and Programs Directorate, and the National Ground Intelligence Center (NGIC), U.S. Army, U.S. Department of Defense for the purpose of sharing relevant biometric and biographic records, effective June 2, 2009 (US-VISIT).

Appendix C – Data Standards

1.1 Introduction

Common information sharing standards serve as baseline requirements for the sharing of terrorism information. Such standards enable the transfer of information in a consistent, identifiable manner, specify common security classification and handling markings, and support both human and automated sharing of terrorism information to multiple classification levels.

Also common Metadata methods and properties are critical elements of an information architecture that encourages information sharing and collaboration. They are essential to the rigorous exploitation of a robust knowledge management capability.

The Terrorist Watchlist Person Data Exchange Standard (TWPDES) is one of the emerging standards to facilitate and promote data interoperability throughout the Intelligence Community (IC) and other national security communities of interest.

1.2 Background

As identified in the 9/11 Commission findings, information sharing improvements are required to ensure terrorism information is readily shared and distributed to those organizations having counterterrorism missions. Executive Order 13388, dated October 25, 2005 titled "Further Strengthening the Sharing of Terrorism Information To Protect Americans" (revoking Executive Order 13356) directs federal agencies to design and use their information systems to give the highest priority to the detection, prevention, disruption, preemption, and mitigation of terrorist activities and the sharing of terrorism information while protecting the freedom, information privacy and other legal rights of Americans. To assist in the maximum distribution of terrorism information, Executive Order 13388 mandated that common standards for the sharing of terrorism information be used as appropriate.

1.3 Terrorist Watchlist Person Data Exchange Standard (TWPDES)

TWPDES was initially developed by the Intelligence Community Metadata Working Group (IC MWG), has been accepted by the National Information Exchange Model (NIEM), and is currently used by several Federal agencies. By updating TWPDES to be NIEM compliant, TWPDES is now accessible to Federal, State, Local and Tribal interagency organizations providing a foundation for seamless information exchange. Please refer to the NIEM website at http://www.niem.gov/TWPDES.php to learn or to get a copy of the XML instantiation of the TWPDES Standard Version 1.2b, rev 1.

TWPDES is not a database, information system or database schema. It is a standard that defines the content and format of information to be exchanged between systems. TWPDES has been defined as an object model, which was then used to create an XML structure. The XML template that defines the TWPDES implementation standard has been updated over the past several years. It leverages layered schema architectural principles and now includes a message component, a watchlist component, an encounter component, biometric identifiers as well as the

original person/identify based model. The TWPDES XML template also includes data validation rules to improve data quality. TWPDES 1.2b allows the exchange of both biographic and biometric information within a single message.

1.4 Core Biographic Person Data Elements (CBPDE)

As communicated in the Core Biographic IEPD, the CBPDE is a core set of biographic data elements (and their formats) that are to be included in any biographic identity-related information exchange. These elements represent the minimum elements used for establishing unique biographic identities for information exchange throughout DHS.

Element	NIEM	NIEM Definition
First Name	nc:PersonGivenName	The first name of a person.
Last Name	nc:PersonSurName	The last name or family name of a person.
Middle Name	nc:PersonMiddleName	The middle name of a person.
Name Translation	nc:PersonPrimaryLanguage	Data type for the language capability of an individual
Date of Birth	nc:PersonBirthDate	The date a person was born.
Country of Birth	nc:PersonBirthLocation/ nc:LocationCountry (Selected ISO and FIPS country code lists)	The location where a person was born.
Gender	nc:PersonSexCode (Selected code list)	The gender or sex of a person.
Country of Citizenship	nc:PersonCitizenship abstract (Selected ISO and FIPS country code lists)	A county that assigns rights, duties, and privileges to a person because of the birth or naturalization of the person in that country.

1.5 Controlled Vocabulary and Other Data Standards.

The Metadata and content standards make use of authoritative sets of codes (or controlled vocabularies), such as for countries and languages, and specific data types, such as for dates and times. Vocabulary standards are important because they ensure that the codes used in the XML instance documents are translated correctly on both sides of the data transaction. The basic vocabulary standards that are utilized in TWPDES include:

1. International Standard ISO 3166, Codes for the Representation of Names of Countries and their Sub-Divisions. The three-character country codes from this standard are integral to the information security markings defined by the CAPCO. These codes are also used by many of the producers of intelligence reports and records to categorize geospatial coverage and collection requirements. There are noted examples of the use of the two character, three character, and three digit codes within the communities.

2. Federal Information Processing Standard (FIPS) Pub 10-4, Countries, Dependencies, Areas of Special Sovereignty, and their Principal Administrative Divisions. This alternative country code vocabulary is used by some intelligence producers and other agencies, such as the Terrorist Screening Center, to categorize geospatial coverage.

3. International Standard ISO 639-2, Codes for the Representation of Names of Languages Part 2: Alpha-3 Code. Intelligence records and reports may, in their entirety or in portions, use languages other than the U.S. form of English. A standard for languages is needed to support presentation and machine translation.

4. International Standard ISO 8601, Representation of dates and times. A standard representation for dates and times is required in order to provide consistent characterization of reports and records in terms of temporal coverage. A standard representation is also needed for consistent reporting of events.

5. International Standard ISO 4217, Codes for the representation of currencies and funds. This provides a structure for a three-letter alphabetic code and an equivalent three-digit numeric code for the representation of currencies and funds.

6. United Nations Economic Commission for Europe (UNECE), Recommendation 20, Codes for units of measure used in international trade.

7. International Standard ISO 10646, Universal Multiple-Octet Coded Character Set (UCS). This is applicable to the representation, transmission, interchange, processing, storage, input and presentation of the written form of the languages of the world as well as additional symbols.

8. Intelligence Community Register of Authorized Controlled Markings (also known as the Controlled Access Program Coordination Office (CAPCO) Register). Director of Central Intelligence Directive (DCID) 6/6 mandates a classification marking system for the Intelligence Community. The CAPCO system uses a uniform list of security classification and control markings authorized for all dissemination of classified information. These classification and control markings, and their authorized abbreviations, are compiled in the Authorized Classification and Control Markings Register maintained by the CAPCO. CAPCO is an implementation of Executive Order 12958 (as amended), *Classified National Security Information*, and Information Security Oversight Office (ISOO) Directive 1. The DSSC has been working with the DOD and elements of DOJ and DHS to consider extensions to the system to accommodate and reconcile their particular security and control markings.