Department of Homeland Security

Common Enterprise Security Architecture (CESA)

Kuppusami Natesan, Chief Architect, knates@yahoo.com

Nick Strapko, Senior Business Analyst, nicholasstrapko@yahoo.com

Robert Daniel, Chief Scientist, daniel@bluegrid.com

Vijay Reddiar, System Architect, vijay@vvk-inc.com

Table of Contents

- CESA Project Overview
- Current State Analysis
- Future State Analysis
- Transition Strategy / Plan
- CESA Benefits
- Appendix A - FEA Reference Models
- Appendix B - EA Products (As-Is Analysis)

CESA Project Overview

Vision Statement

- Establish an Enterprise Security Architecture for Department of Homeland Security to Improve ***National Security***
  - ***Integrate*** stove-pipe systems to improve information accuracy for better decision making
  - Enable ***real-time information sharing*** with ***right people*** at the ***right time*** and at the ***right place***
  - Establish a ***trust platform*** to enable secure and timely information sharing between federal, state, local, foreign government and private sector entities
  - Minimize ***implementation*** & ongoing ***operations cost***

BETTER DECISIONS FASTER – DECISIVE ACTIONS SOONER

Program Background

- Department of Homeland Security is undertaking multiple identity and credentialing initiatives to improve national security and reduce terrorism:
    - ***Secure Flight***
    - ***Detention and Removal Operations (DRO)***
    - ***US-VISIT / Air and Sea Biometric Exit***
    - ***Homeland Security Presidential Directive (HSPD-12)***
    - ***Registered Traveller (RT)***
    - ***Transportation Worker Identification Cards (TWIC)***
    - ***First Responder Authentication Cards (FRAC)***
    - ***Western Hemisphere Travel Initiative (WHTI)***

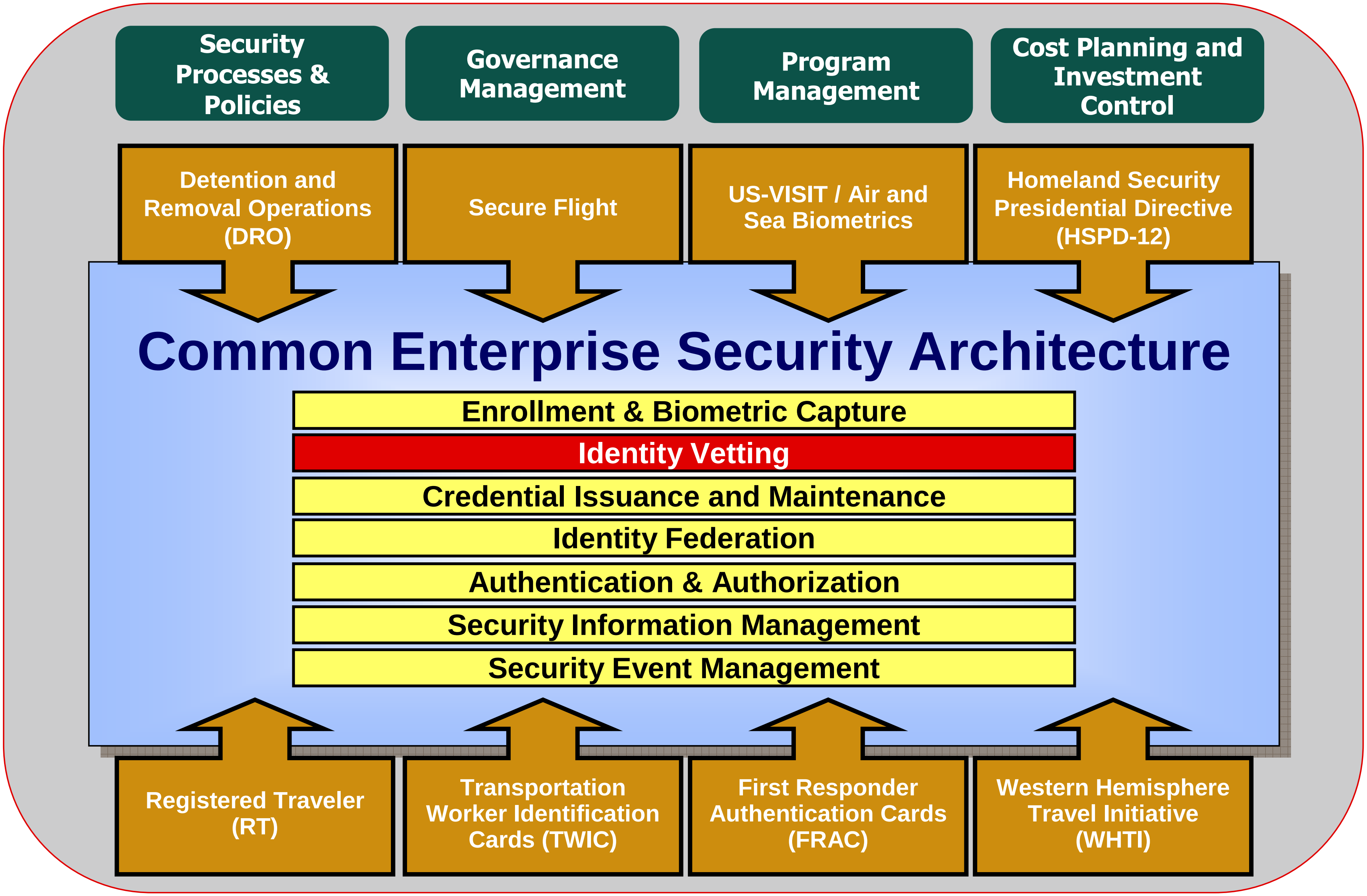
CESA Program Objective

- Establish a Common Enterprise Security Architecture (CESA) for Department of Homeland Security (DHS) with the following capabilities:
  - Enrollment & Biometric Capture
  - Identity Vetting
  - Credential Issuance and Maintenance
  - Identity Federation
  - Authentication & Authorization
  - Security Information Management
  - Security Event Management

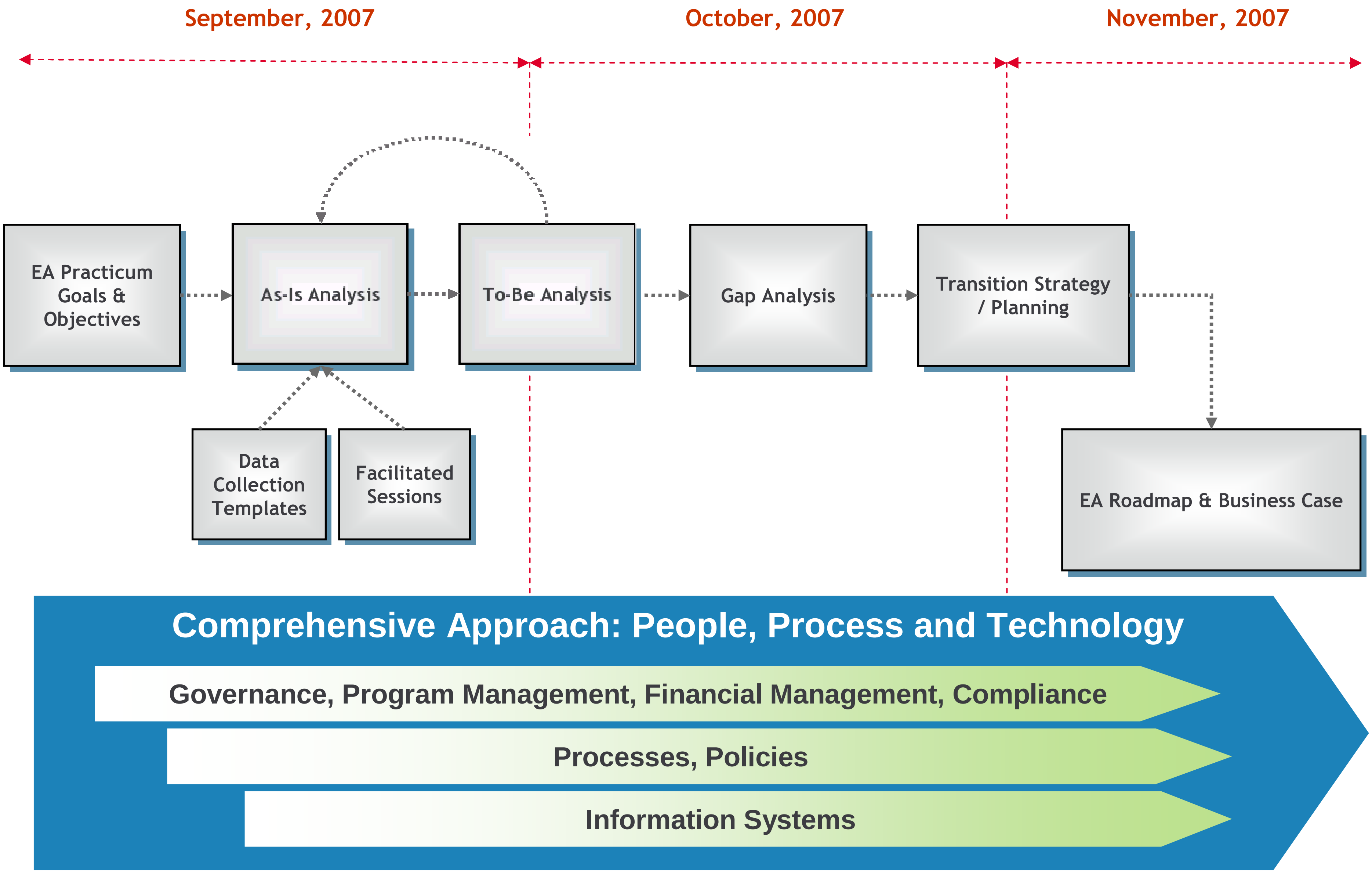
TO

- Enable reuse across current / future Identity and Credentialing Management Programs at DHS:
  - ***Secure Flight***
  - ***Detention and Removal Operations (DRO)***
  - ***US-VISIT / Air and Sea Biometrics***
  - ***Homeland Security Presidential Directive (HSPD-12)***
  - **Registered Traveler (RT)**
  - **Transportation Worker Identification Cards (TWIC)**
  - **First Responder Authentication Cards (FRAC)**
  - **Western Hemisphere Travel Initiative (WHTI)**

Practicum Project Scope


Security Processes & Policies
Governance Management
Program Management
Cost Planning and Investment Control
Detention and Removal Operations (DRO)
Secure Flight
US-VISIT / Air and Sea Biometrics
Homeland Security Presidential Directive (HSPD-12)
Common Enterprise Security Architecture
Enrollment & Biometric Capture
Identity Vetting
Credential Issuance and Maintenance
Identity Federation
Authentication & Authorization
Security Information Management
Security Event Management
Registered Traveler (RT)
Transportation Worker Identification Cards (TWIC)
First Responder Authentication Cards (FRAC)
Western Hemisphere Travel Initiative (WHTI)

Practicum Project Approach & Schedule


September, 2007
October, 2007
November, 2007
EA Practicum Goals & Objectives
As-Is Analysis
To-Be Analysis
Gap Analysis
Transition Strategy / Planning
Data Collection Templates
Facilitated Sessions
EA Roadmap & Business Case
Comprehensive Approach: People, Process and Technology
Governance, Program Management, Financial Management, Compliance
Processes, Policies
Information Systems

Practicum Project Deliverables

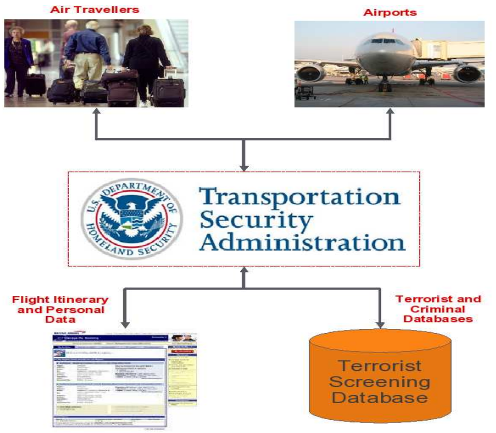
- Enterprise Architecture Products (As-Is & To-Be States)
  - Problem Statement and Roadmap
  - Business Operations Concept Diagram
  - Business Node Connection Model
  - System Node Connection Model
  - Information Exchange Matrix
  - Organization Chart and Relationship Model
  - Data Model
- Service Oriented Architecture (SOA) Enabled CESA
- Transition Strategy / Plan
  - Gap Analysis and Sequencing Plan
  - Governance Framework
  - Communication Plan
  - Risk Management Plan
  - Business Case
- FEA Reference Models

Current State Analysis

Current State Concept Model (“As-Is”)

Stove-pipe implementations of systems, processes, ...

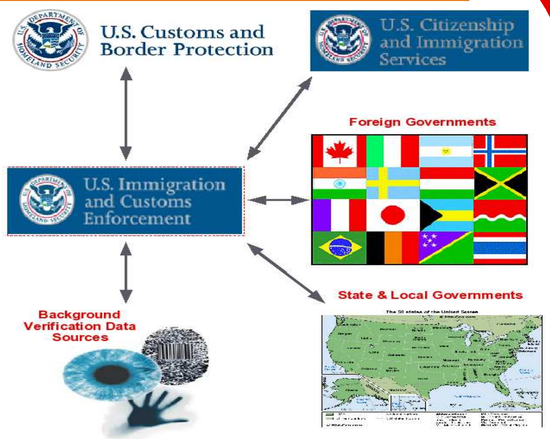
Secure Flight


Air Travellers
Airports
Transportation Security Administration
Flight Itinerary and Personal Data
Terrorist and Criminal Databases
Terrorist Screening Database

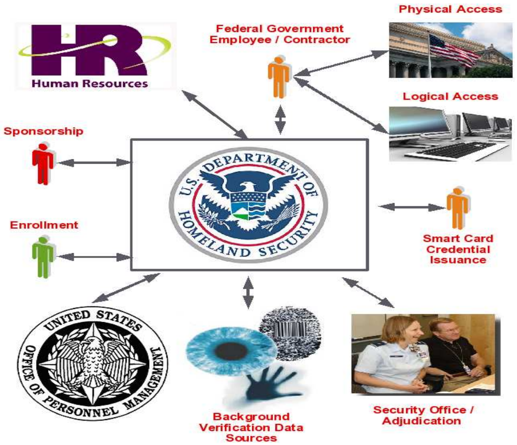
- Travel Reservation Systems
- Screening Gateway
- Background Verification System
- Monitoring & Audit Logging

Detention and Removal Operations

- Case Management System
- Data Sharing
- Advanced Authentication
- Monitoring & Audit Logging


U.S. Customs and Border Protection
U.S. Citizenship and Immigration Services
Foreign Governments
U.S. Immigration and Customs Enforcement
State & Local Governments
Background Verification Data Sources

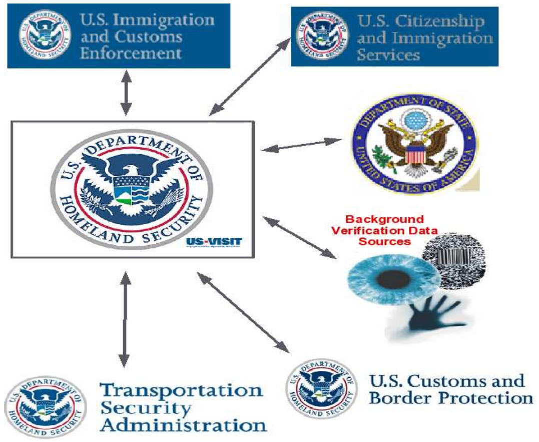
HSPD-12


Human Resources
Federal Government Employee / Contractor
Physical Access
Logical Access
Sponsorship
Enrollment
Smart Card Credential Issuance
Background Verification Data Sources
Security Office / Adjudication

- Enrollment System
- Background Verification System
- Credential Issuance & Maintenance
- Monitoring & Audit Logging

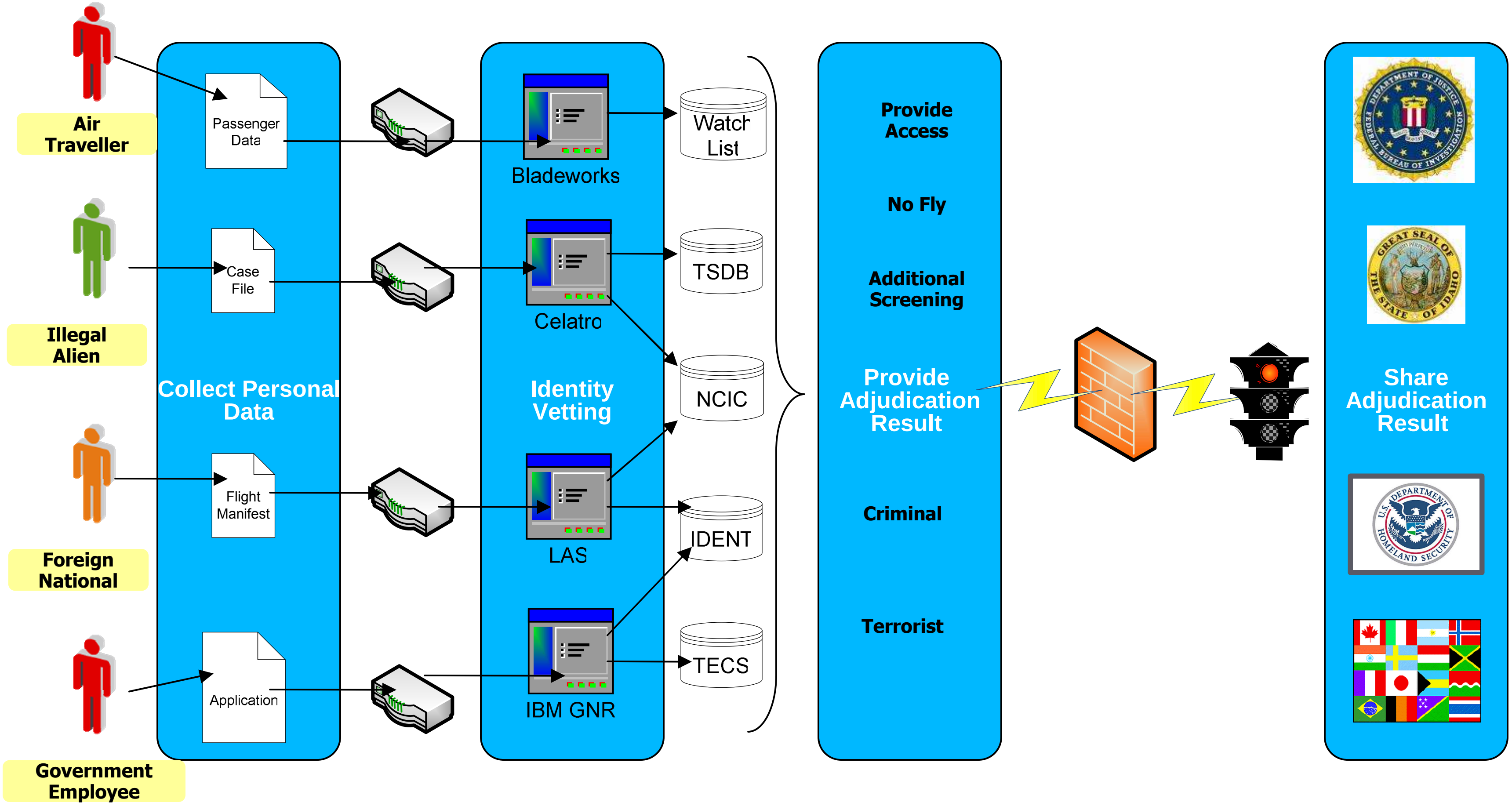
US-VISIT / Air & Sea Biometrics Program

- Biometric Capture System
- Background Verification System
- Authentication & Authorization
- Monitoring & Audit Logging


U.S. Immigration and Customs Enforcement
U.S. Citizenship and Immigration Services
US-VISIT
Background Verification Data Sources
Transportation Security Administration
U.S. Customs and Border Protection

.... security policies and organizations

Identity Vetting Platform (“As-Is”)



As-Is Analysis Approach & Products Used

Program	Activity Flow Model	Business Node Connectivity Model	System Connection Model	Information Exchange Matrix	Organizational Relationship Model	Logical Data Model
Secure Flight Program (As-Is State)	√	√	√	√	√	√
DRO Program (As-Is State)	√	√	√	√	√	√
US-VISIT Air/Sea Biometric Exit (As-Is State)	√	√	√	√	√	√
HSPD-12 Program (As-Is State)						
Questions about the Enterprise						
What relevant actions occur in your enterprise?	√					
Who performs these actions?	√	√				
What relationships exist between those who perform these actions?					√	
Who needs to communicate with whom?		√			√	
What information do they need to exchange?		√	√			
What hardware/software do they use to communicate?			√			
What is the relationship between data entities?						√

Key Findings

- Organizational or resource redundancy exists within each DHS subcomponent
- Each program utilizes different resources to perform the activities and has disparate policy and standards
- Each program operates and maintains separate data aggregation systems and vetting platforms
- Each program provides similar information in different message formats, size, media, security classifications, and authorization requirements
- Each of the programs provide similar data objects and entities containing the same data attributes and exhibiting the same relationships between entities

Problem Statement & Roadmap

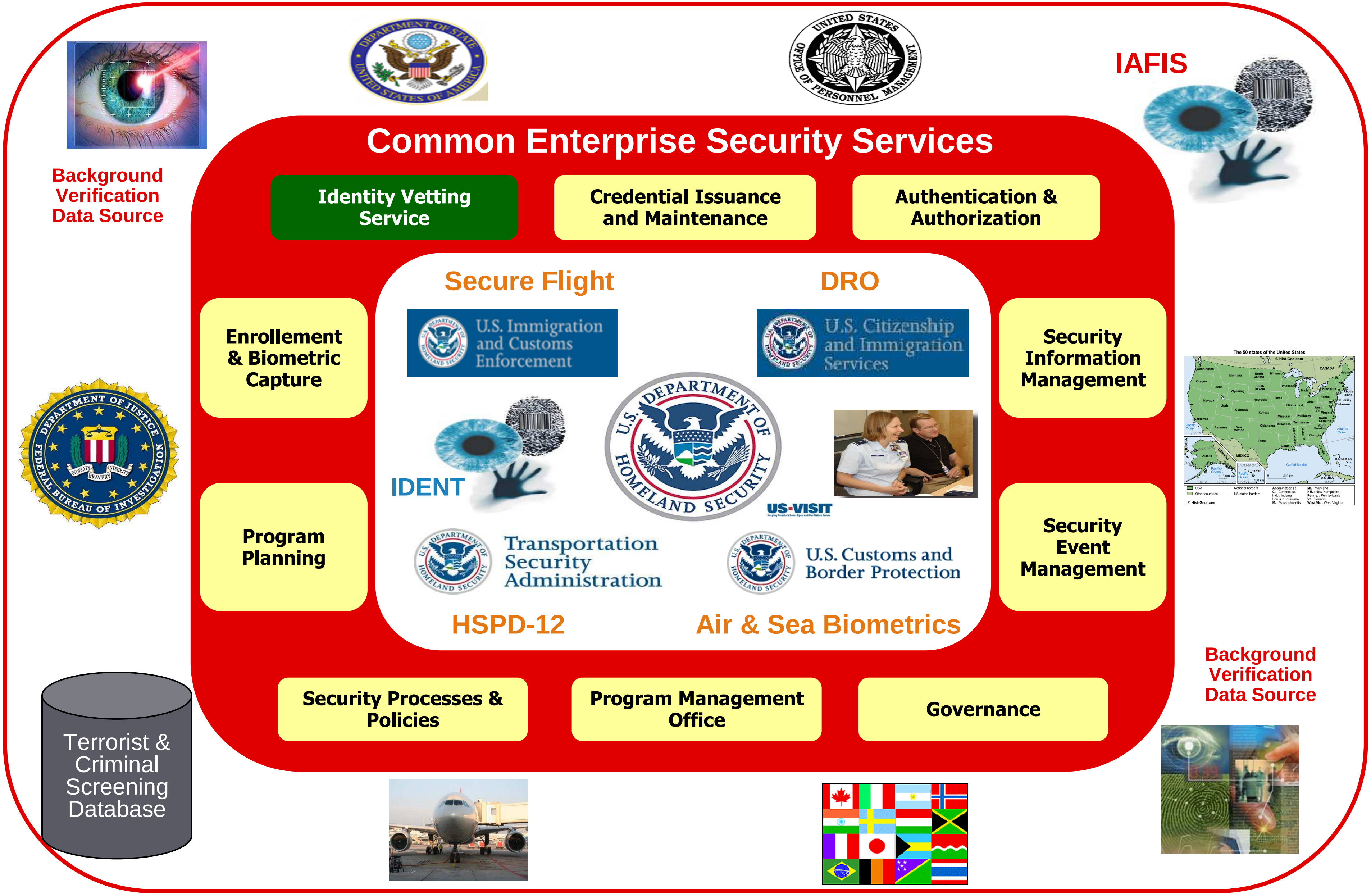
- Isolated security programs leading to inefficient decisions affecting national security
  - Multiple screening gateways and vetting systems
  - Data collection / retention policies and privacy constraints
  - Information sharing and process efficiency concerns
- Lack of common approach to background verification against existing background verification systems / sources
- Higher cost of implementations and ongoing operations
- Common requirements / needs
  - Identification, background checks and credential management
  - Strong / multi-factor authentication
  - Monitoring and Auditing Logging
  - Drive to move from biographic based identification to biometrics

Problem Statement & Roadmap

- Implement Common Enterprise Security Architecture to enable reuse across DHS security programs / initiatives
- Develop a common and standardized approach to background verification against existing biometrics and related data sources
- Establish governance organization, program management office, security policies and processes to facilitate the implementation, usage and ongoing operations of Common Enterprise Security Architecture
- Create an integrated trust platform to securely share information between federal, state, local, foreign and private sector entities
- Build an end-to-end security services infrastructure supporting physical, network and logical access using advanced authentication credentials

Future State Analysis

Future State Concept Model ("To-Be")



IAFIS

Background Verification Data Source

Common Enterprise Security Services

Identity Vetting Service

Credential Issuance and Maintenance

Authentication & Authorization

Enrollement & Biometric Capture

Program Planning

Security Information Management

Security Event Management

Secure Flight

DRO

U.S. Immigration and Customs Enforcement

U.S. Citizenship and Immigration Services

IDENT

US-VISIT

Transportation Security Administration

U.S. Customs and Border Protection

HSPD-12

Air & Sea Biometrics

Security Processes & Policies

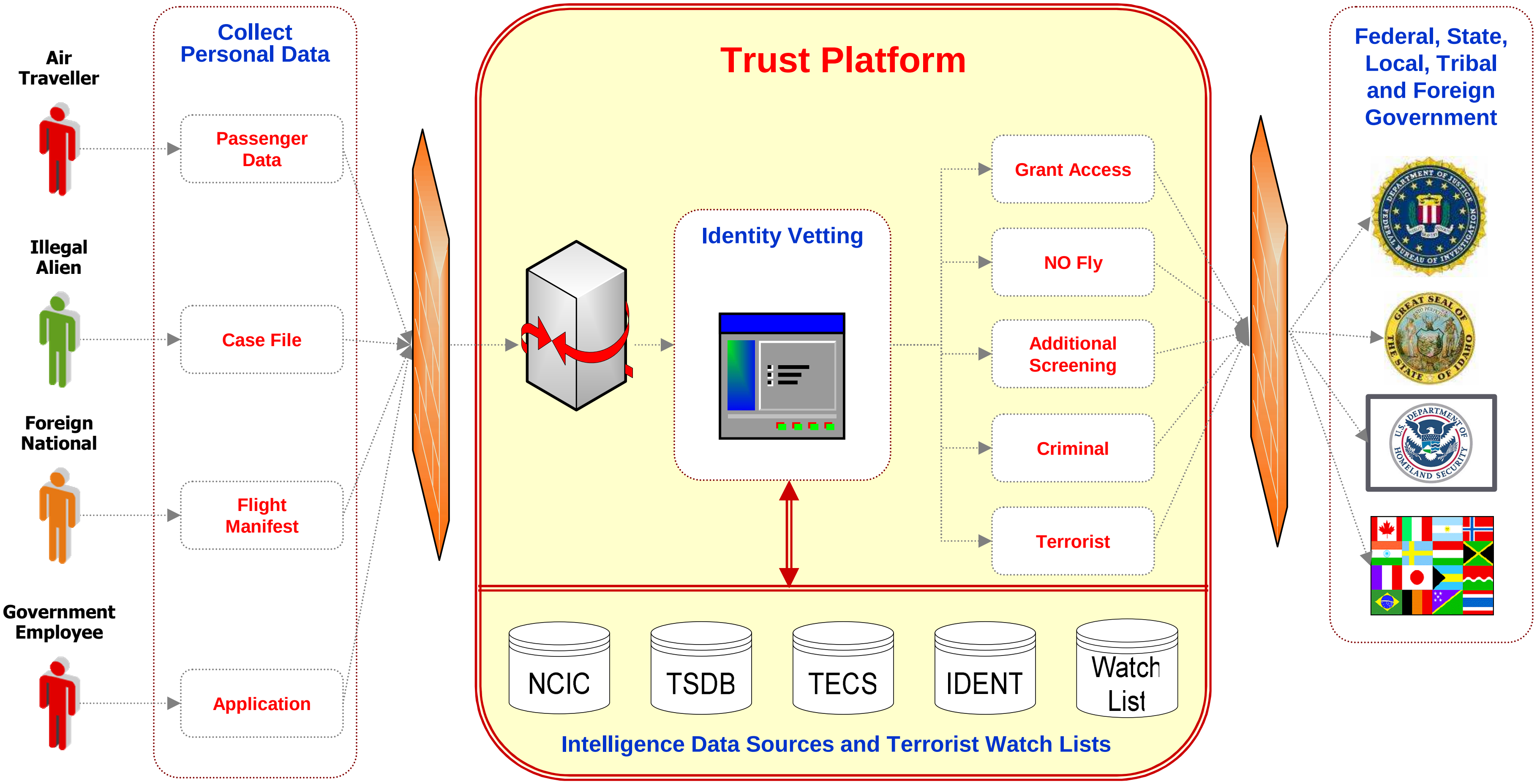
Program Management Office

Governance

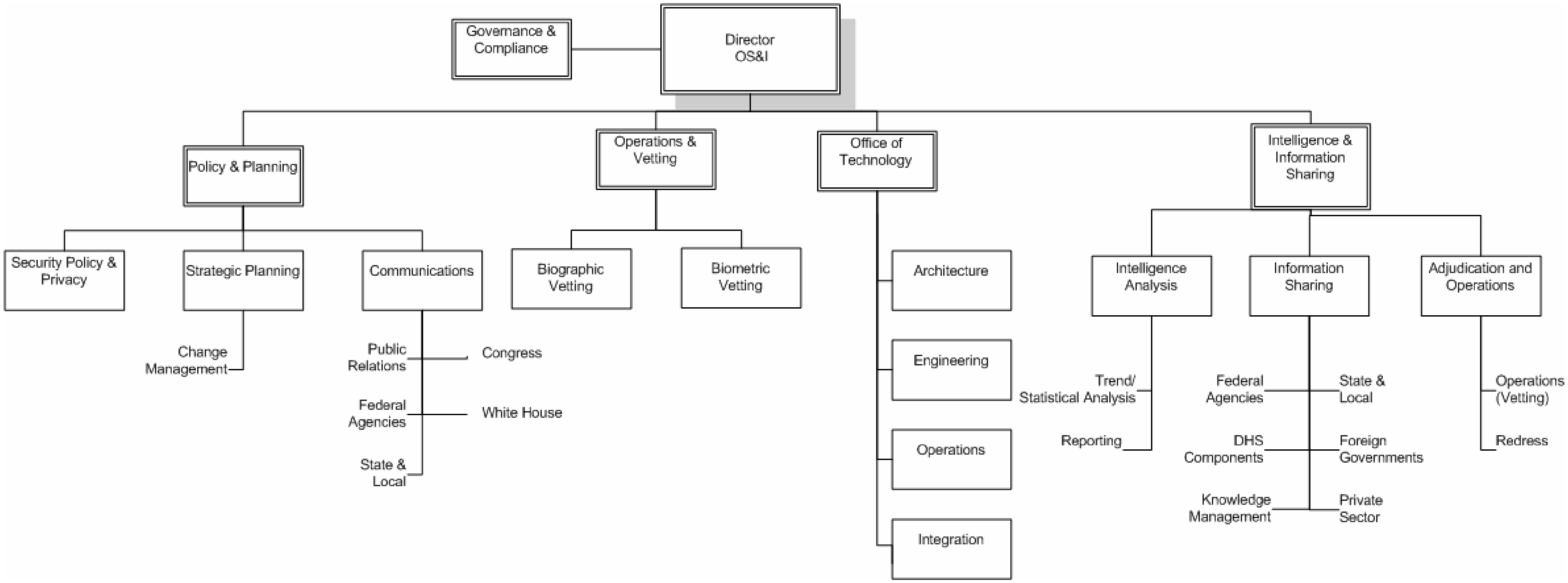
Background Verification Data Source

Terrorist & Criminal Screening Database

Identity Vetting Platform (“To-Be”)



Organization Model (OS&I)



Director OS&I

Governance & Compliance

Policy & Planning

Security Policy & Privacy

Strategic Planning

Change Management

Communications

Public Relations

Congress

Federal Agencies

White House

State & Local

Operations & Vetting

Biographic Vetting

Biometric Vetting

Office of Technology

Architecture

Engineering

Operations

Integration

Intelligence & Information Sharing

Intelligence Analysis

Trend/ Statistical Analysis

Reporting

Information Sharing

Federal Agencies

State & Local

DHS Components

Foreign Governments

Knowledge Management

Private Sector

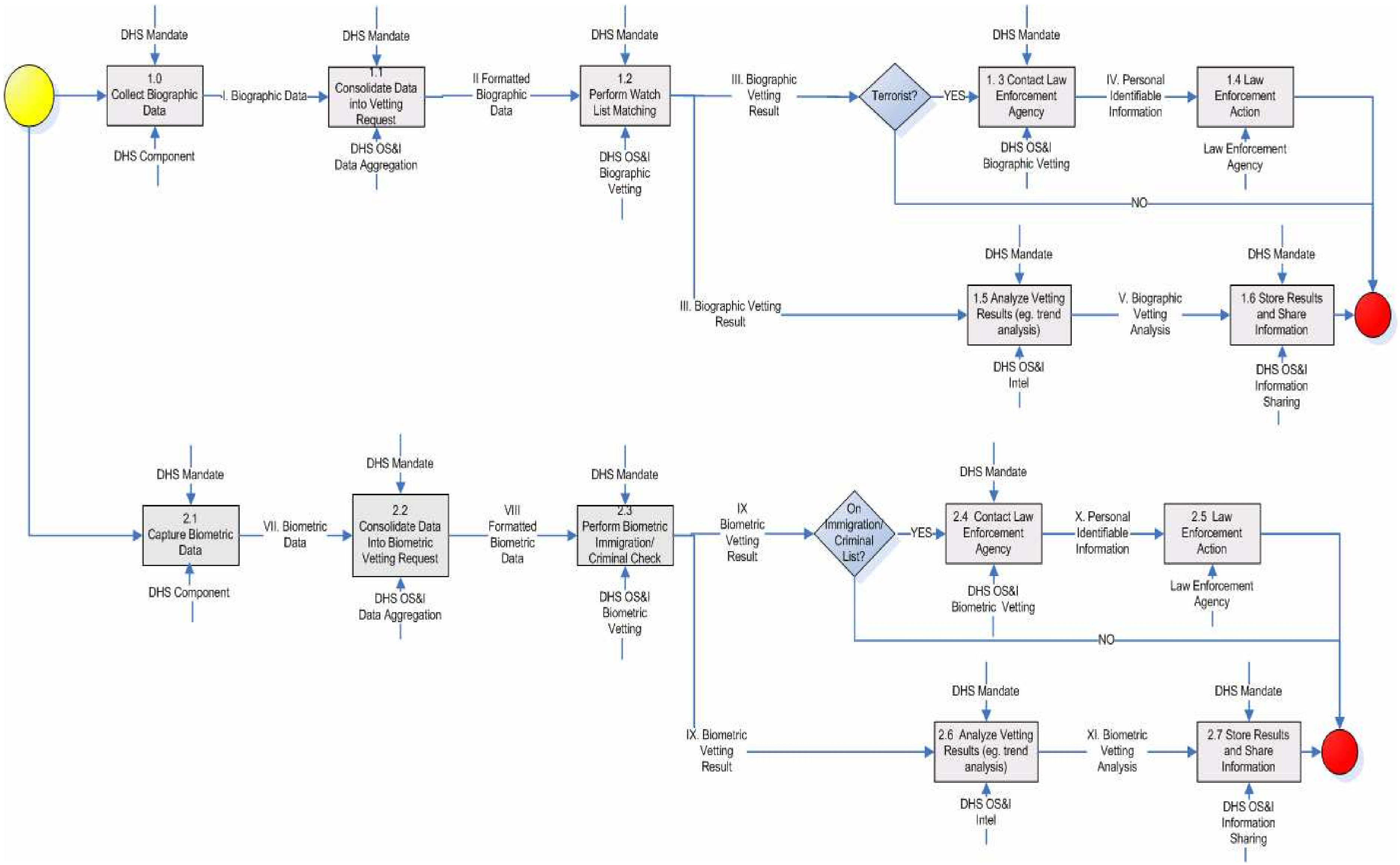
Adjudication and Operations

Operations (Vetting)

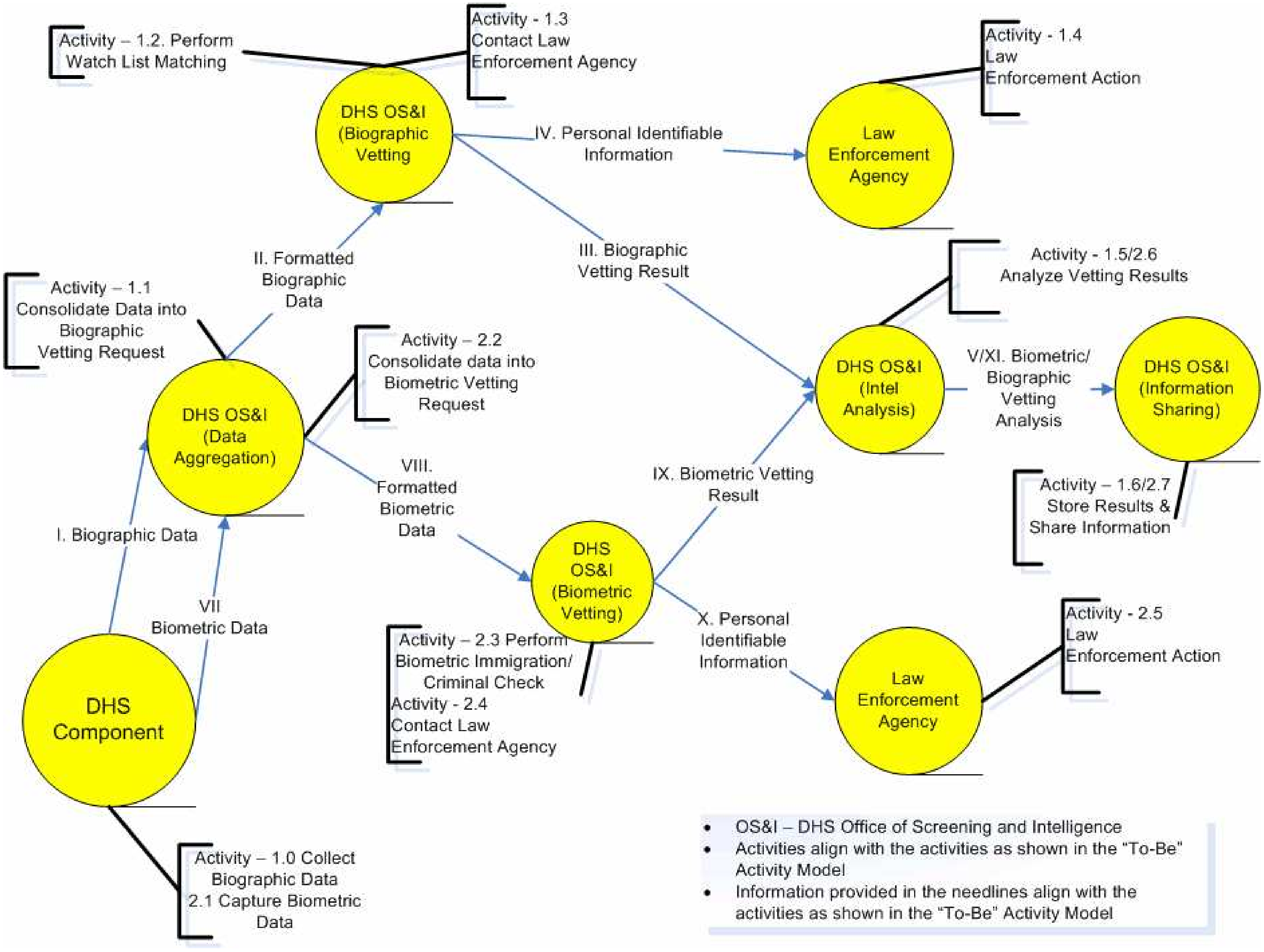
Redress

- Consolidate vetting and credentialing operations through the Office of Screening and Intelligence Analysis (OS&I)
  - Primary functions/roles:
    - Policy and Planning
    - Operations and Vetting
    - Office of Technology
    - Intelligence and Information Sharing

Activity Model

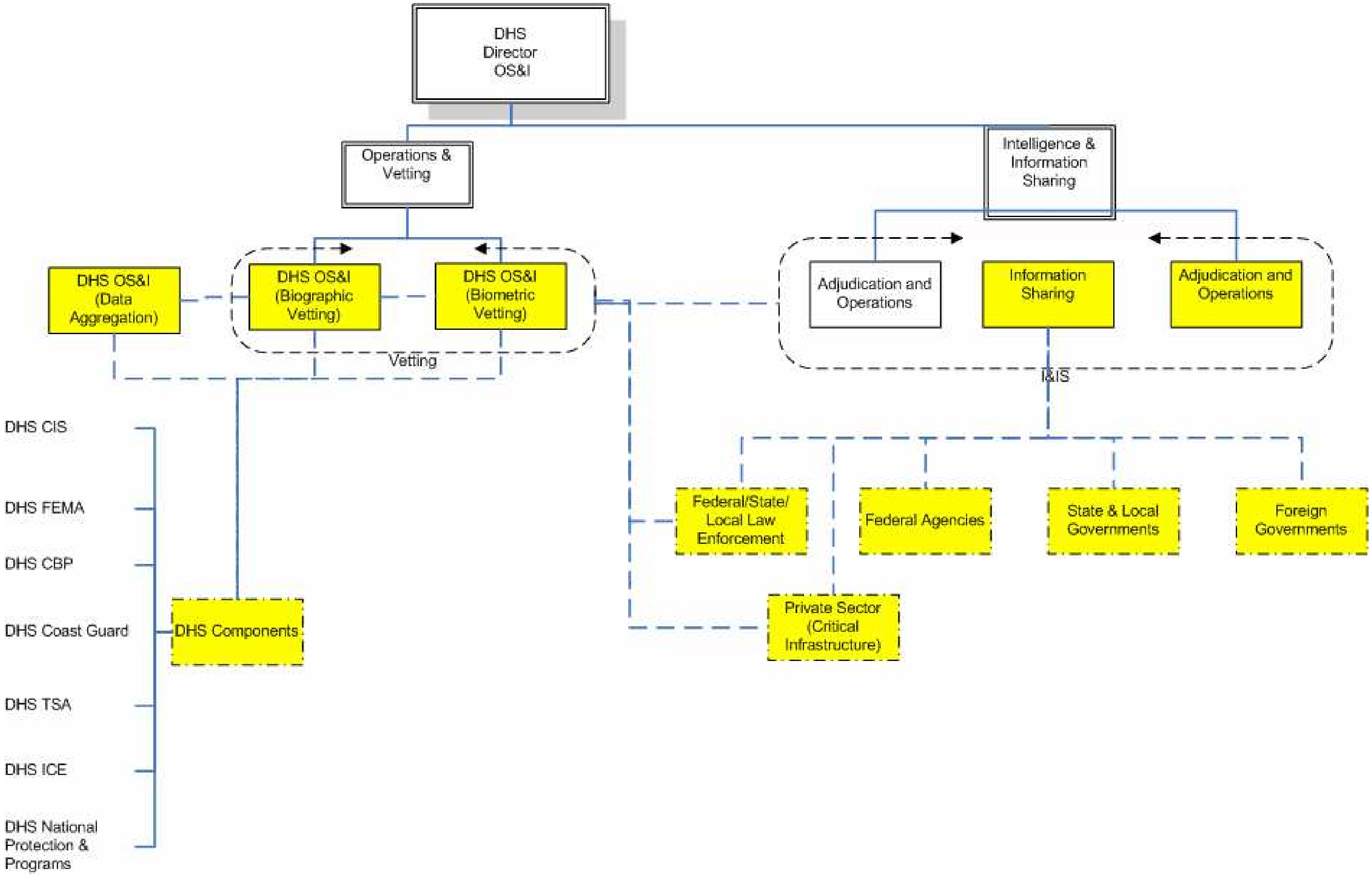

DHS Mandate
1.0 Collect Biographic Data
DHS Component
I. Biographic Data
DHS Mandate
1.1 Consolidate Data into Vetting Request
DHS OS&I Data Aggregation
II Formatted Biographic Data
DHS Mandate
1.2 Perform Watch List Matching
DHS OS&I Biographic Vetting
III. Biographic Vetting Result
Terrorist?
YES
NO
DHS Mandate
1. 3 Contact Law Enforcement Agency
DHS OS&I Biographic Vetting
IV. Personal Identifiable Information
DHS Mandate
1.4 Law Enforcement Action
Law Enforcement Agency
III. Biographic Vetting Result
DHS Mandate
1.5 Analyze Vetting Results (eg. trend analysis)
DHS OS&I Intel
V. Biographic Vetting Analysis
DHS Mandate
1.6 Store Results and Share Information
DHS OS&I Information Sharing
DHS Mandate
2.1 Capture Biometric Data
DHS Component
VII. Biometric Data
DHS Mandate
2.2 Consolidate Data Into Biometric Vetting Request
DHS OS&I Data Aggregation
VIII Formatted Biometric Data
DHS Mandate
2.3 Perform Biometric Immigration/ Criminal Check
DHS OS&I Biometric Vetting
IX Biometric Vetting Result
On Immigration/ Criminal List?
YES
NO
DHS Mandate
2.4 Contact Law Enforcement Agency
DHS OS&I Biometric Vetting
X. Personal Identifiable Information
DHS Mandate
2.5 Law Enforcement Action
Law Enforcement Agency
IX. Biometric Vetting Result
DHS Mandate
2.6 Analyze Vetting Results (eg. trend analysis)
DHS OS&I Intel
XI. Biometric Vetting Analysis
DHS Mandate
2.7 Store Results and Share Information
DHS OS&I Information Sharing

Business Node Connection Model

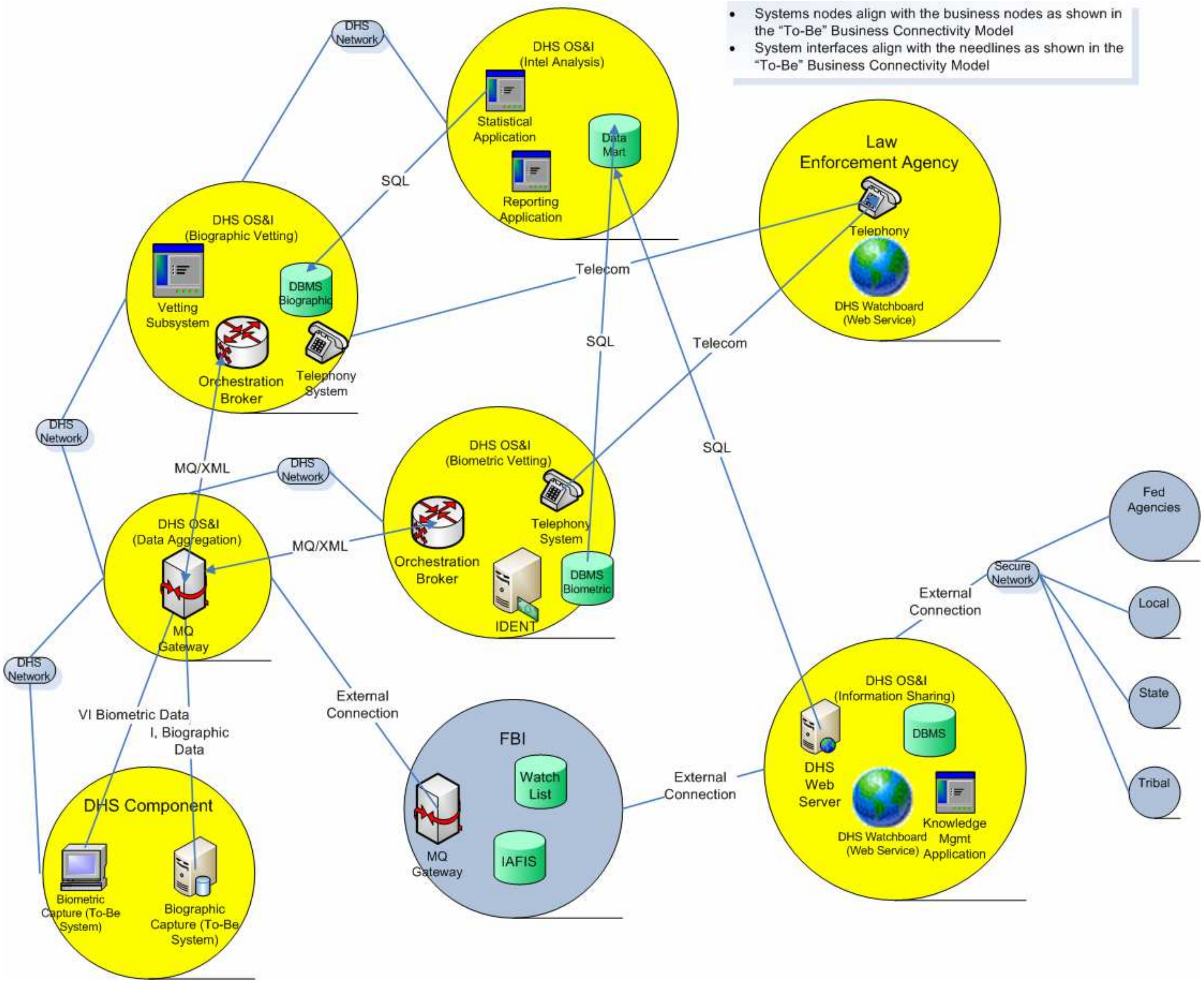

Activity – 1.2. Perform Watch List Matching
Activity - 1.3 Contact Law Enforcement Agency
Activity - 1.4 Law Enforcement Action
DHS OS&I (Biographic Vetting)
IV. Personal Identifiable Information
Law Enforcement Agency
II. Formatted Biographic Data
III. Biographic Vetting Result
Activity - 1.5/2.6 Analyze Vetting Results
Activity – 1.1 Consolidate Data into Biographic Vetting Request
Activity – 2.2 Consolidate data into Biometric Vetting Request
DHS OS&I (Intel Analysis)
V/XI. Biometric/ Biographic Vetting Analysis
DHS OS&I (Information Sharing)
DHS OS&I (Data Aggregation)
VIII. Formatted Biometric Data
IX. Biometric Vetting Result
Activity – 1.6/2.7 Store Results & Share Information
I. Biographic Data
DHS OS&I (Biometric Vetting)
VII Biometric Data
X. Personal Identifiable Information
Activity - 2.5 Law Enforcement Action
Activity – 2.3 Perform Biometric Immigration/ Criminal Check
Activity - 2.4 Contact Law Enforcement Agency
DHS Component
Law Enforcement Agency
Activity – 1.0 Collect Biographic Data
2.1 Capture Biometric Data

- OS&I – DHS Office of Screening and Intelligence
- Activities align with the activities as shown in the “To-Be” Activity Model
- Information provided in the needlines align with the activities as shown in the “To-Be” Activity Model

Organization Relationship Model

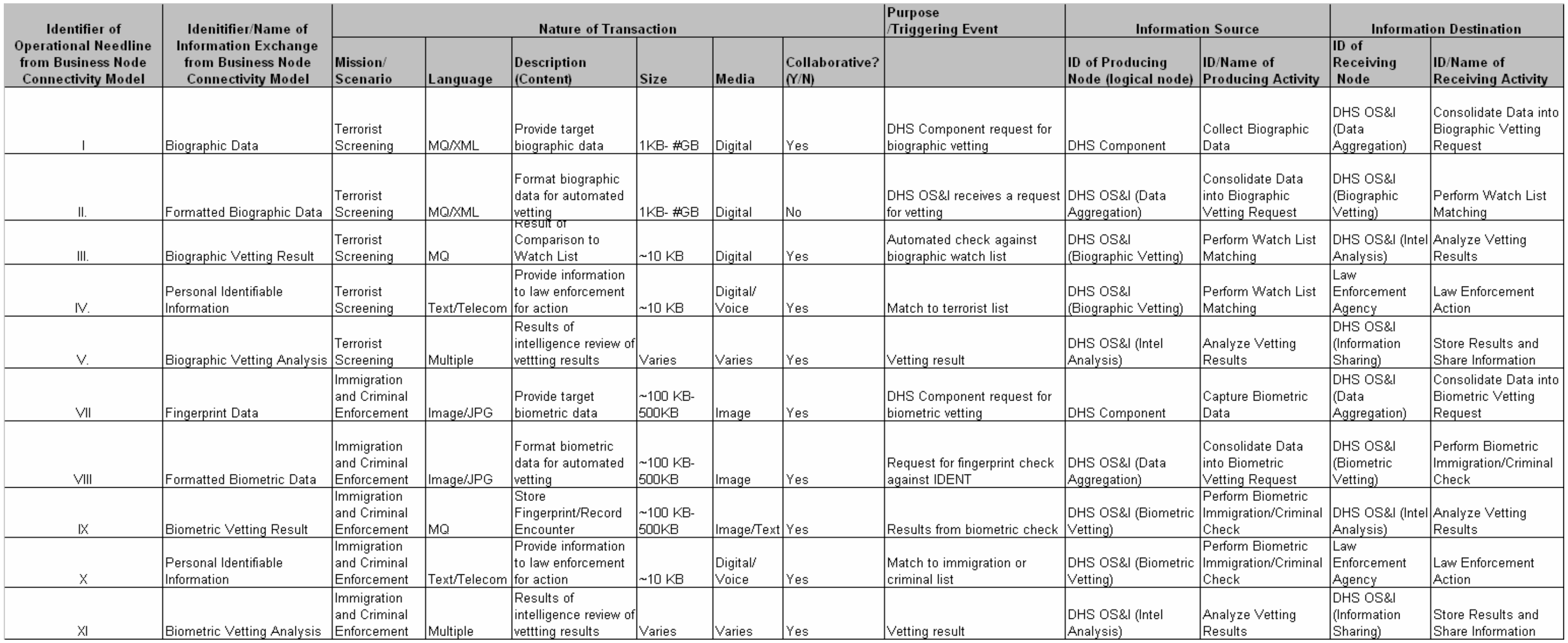

DHS Director OS&I
Operations & Vetting
Intelligence & Information Sharing
DHS OS&I (Data Aggregation)
DHS OS&I (Biographic Vetting)
DHS OS&I (Biometric Vetting)
Vetting
Adjudication and Operations
Information Sharing
Adjudication and Operations
I&IS
DHS CIS
DHS FEMA
DHS CBP
DHS Coast Guard
DHS TSA
DHS ICE
DHS National Protection & Programs
DHS Components
Federal/State/ Local Law Enforcement
Federal Agencies
State & Local Governments
Foreign Governments
Private Sector (Critical Infrastructure)

System Node Connection Model

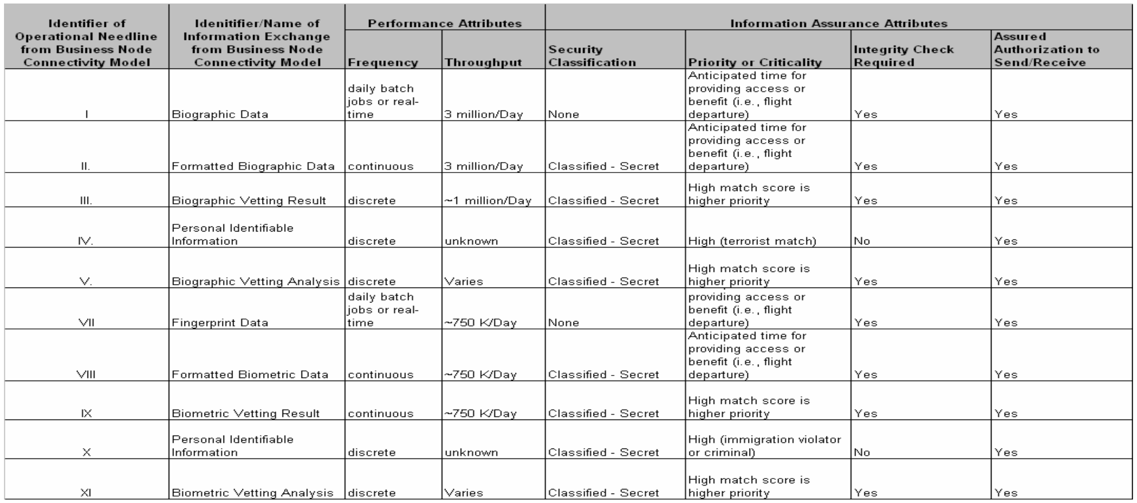


- Systems nodes align with the business nodes as shown in the "To-Be" Business Connectivity Model
- System interfaces align with the needlines as shown in the "To-Be" Business Connectivity Model

Information Exchange Matrix



Identifier of Operational Needline from Business Node Connectivity Model	Idenitifier/Name of Information Exchange from Business Node Connectivity Model	Nature of Transaction						Purpose /Triggering Event	Information Source		Information Destination	
		Mission/ Scenario	Language	Description (Content)	Size	Media	Collaborative? (Y/N)		ID of Producing Node (logical node)	ID/Name of Producing Activity	ID of Receiving Node	ID/Name of Receiving Activity
I	Biographic Data	Terrorist Screening	MQ/XML	Provide target biographic data	1KB- #GB	Digital	Yes	DHS Component request for biographic vetting	DHS Component	Collect Biographic Data	DHS OS&I (Data Aggregation)	Consolidate Data into Biographic Vetting Request
II.	Formatted Biographic Data	Terrorist Screening	MQ/XML	Format biographic data for automated vetting	1KB- #GB	Digital	No	DHS OS&I receives a request for vetting	DHS OS&I (Data Aggregation)	Consolidate Data into Biographic Vetting Request	DHS OS&I (Biographic Vetting)	Perform Watch List Matching
III.	Biographic Vetting Result	Terrorist Screening	MQ	Result of Comparison to Watch List	~10 KB	Digital	Yes	Automated check against biographic watch list	DHS OS&I (Biographic Vetting)	Perform Watch List Matching	DHS OS&I (Intel Analysis)	Analyze Vetting Results
IV.	Personal Identifiable Information	Terrorist Screening	Text/Telecom	Provide information to law enforcement for action	~10 KB	Digital/ Voice	Yes	Match to terrorist list	DHS OS&I (Biographic Vetting)	Perform Watch List Matching	Law Enforcement Agency	Law Enforcement Action
V.	Biographic Vetting Analysis	Terrorist Screening	Multiple	Results of intelligence review of vettting results	Varies	Varies	Yes	Vetting result	DHS OS&I (Intel Analysis)	Analyze Vetting Results	DHS OS&I (Information Sharing)	Store Results and Share Information
VII	Fingerprint Data	Immigration and Criminal Enforcement	Image/JPG	Provide target biometric data	~100 KB- 500KB	Image	Yes	DHS Component request for biometric vetting	DHS Component	Capture Biometric Data	DHS OS&I (Data Aggregation)	Consolidate Data into Biometric Vetting Request
VIII	Formatted Biometric Data	Immigration and Criminal Enforcement	Image/JPG	Format biometric data for automated vetting	~100 KB- 500KB	Image	Yes	Request for fingerprint check against IDENT	DHS OS&I (Data Aggregation)	Consolidate Data into Biometric Vetting Request	DHS OS&I (Biometric Vetting)	Perform Biometric Immigration/Criminal Check
IX	Biometric Vetting Result	Immigration and Criminal Enforcement	MQ	Store Fingerprint/Record Encounter	~100 KB- 500KB	Image/Text	Yes	Results from biometric check	DHS OS&I (Biometric Vetting)	Perform Biometric Immigration/Criminal Check	DHS OS&I (Intel Analysis)	Analyze Vetting Results
X	Personal Identifiable Information	Immigration and Criminal Enforcement	Text/Telecom	Provide information to law enforcement for action	~10 KB	Digital/ Voice	Yes	Match to immigration or criminal list	DHS OS&I (Biometric Vetting)	Perform Biometric Immigration/Criminal Check	Law Enforcement Agency	Law Enforcement Action
XI	Biometric Vetting Analysis	Immigration and Criminal Enforcement	Multiple	Results of intelligence review of vettting results	Varies	Varies	Yes	Vetting result	DHS OS&I (Intel Analysis)	Analyze Vetting Results	DHS OS&I (Information Sharing)	Store Results and Share Information



Identifier of Operational Needline from Business Node Connectivity Model	Idenitifier/Name of Information Exchange from Business Node Connectivity Model	Performance Attributes		Information Assurance Attributes			
		Frequency	Throughput	Security Classification	Priority or Criticality	Integrity Check Required	Assured Authorization to Send/Receive
I	Biographic Data	daily batch jobs or real-time	3 million/Day	None	Anticipated time for providing access or benefit (i.e., flight departure)	Yes	Yes
II.	Formatted Biographic Data	continuous	3 million/Day	Classified - Secret	Anticipated time for providing access or benefit (i.e., flight departure)	Yes	Yes
III.	Biographic Vetting Result	discrete	~1 million/Day	Classified - Secret	High match score is higher priority	Yes	Yes
IV.	Personal Identifiable Information	discrete	unknown	Classified - Secret	High (terrorist match)	No	Yes
V.	Biographic Vetting Analysis	discrete	Varies	Classified - Secret	High match score is higher priority	Yes	Yes
VII	Fingerprint Data	daily batch jobs or real-time	~750 K/Day	None	providing access or benefit (i.e., flight departure)	Yes	Yes
VIII	Formatted Biometric Data	continuous	~750 K/Day	Classified - Secret	Anticipated time for providing access or benefit (i.e., flight departure)	Yes	Yes
IX	Biometric Vetting Result	continuous	~750 K/Day	Classified - Secret	High match score is higher priority	Yes	Yes
X	Personal Identifiable Information	discrete	unknown	Classified - Secret	High (immigration violator or criminal)	No	Yes
XI	Biometric Vetting Analysis	discrete	Varies	Classified - Secret	High match score is higher priority	Yes	Yes

Data Model

Entity Name: VETTING REQUEST
Description: A electronic message sent to the DHS CONSOLIDATED VETTING UNIT requesting a background check and providing an individuals reference data for vetting against a reference database.
Attributes (not a complete list of attributes):

4

Name: DHS Organizational Unit
Description: DHS organizational unit requesting a background check.
Name: Unique Identifier
Description: A unique number for each vetting request.
Name: Time
Description: The time when the vetting request was submitted (in Eastern time)
Name: Date
Description: The date when the vetting request was submitted (Month/Day/Year)
Relationships: The request is provided to the DHS Consolidated Vetting Unit .

Entity Name: CONSOLIDATED VETTING UNIT
Description: A unique DHS unit that provides DHS organizational units/ programs vetting services for all screening or targeting of individuals against various federal reference databases.
Attributes (not a complete list of attributes):

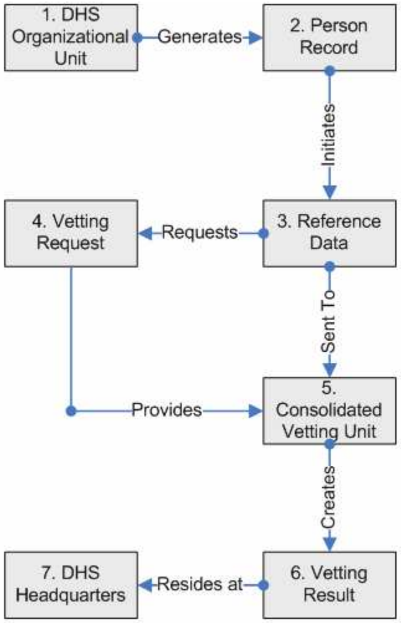
5

Name: Organizational Number
Description: A unique number to identify the DHS organizational unit
Name: Location
Description: Geographical location of the organizational unit.
Name: EDI information
Description: Instructions on exchanging data with other organizations/entities
Name: Vetting History
Description: Chronological record of all vetting requests.
Relationships: The unit will create a VETTING RESULT for each vetting request.

Entity Name: VETTING RESULT
Description: The automated result from a identity search engine or the manual result performed by an intel analyst identifying the status of a vetting request against a reference database (e.g., Cleared, No Fly, Criminal).
Attributes (not a complete list of attributes):

6

Name: DHS Organizational Unit
Description: DHS organizational unit requesting a background check.
Name: Unique Identifier
Description: A unique number for the vetting result.
Name: Time
Description: The time when the vetting result was created (in Eastern time)
Name: Date
Description: The date when the vetting result was created (Month/Day/Year)
Relationships: The vetting results are stored and archived at DHS HQ .



Entity Name: DHS HEADQUARTERS
Description: The specific location/network/database vetting results are stored and archived at DHS headquarters.
Attributes:

7

Name: Component Number
Description: A unique number to identify the organizational unit where the vetting results are stored and archived.
Name: Network
Description: The network name for accessing the vetting results records.
Name: Database
Description: The type/configuration for the database storing the vetting results.
Name: Vetting History
Description: Chronological record of vetting events with the organizational unit.
Relationships: Receives and stores all VETTING RESULTS from DHS units.

Entity Name: DHS ORGANIZATIONAL UNIT
Description: A DHS component (e.g., CBP) or organization/program within a component (e.g., Secure Flight) that provides screening or targeting of individuals using either biographic or biometric data.
Attributes:

1

Name: Component Number
Description: A unique number to identify the organizational unit
Name: Identification Data
Description: Personal identifiable information collected by the organizational unit.
Name: EDI information
Description: Instructions on exchanging data with other organizations/entities
Name: Vetting History
Description: Chronological record of vetting events with the organizational unit.
Relationships: Generates a PERSON RECORD for screening or targeting.

Entity Name: PERSON RECORD
Description: A record an DHS organizational unit develops providing biographic and/or biometric data that identifies an individual for screening or targeting against a reference database (e.g., Watch List).
Attributes (not a complete list of attributes):

2

Name: First Name
Description: First name of the individual having at least one letter (ie., initial)
Name: Last Name
Description: Last name of the individual having at least two letters
Name: Date of Birth
Description: Date of Birth of the individual represented as month/day/year
Name: Fingerprint
Description: An image generated from the fingerprint of the individual.
Relationships: Initiates REFERENCE DATA for submitting a vetting request.

Entity Name: REFERENCE DATA
Description: Unique personal identifiable information extracted from the PERSON RECORD used to vet an individual as defined by each DHS organizational unit/program.
Attributes (not a complete list of attributes):

3

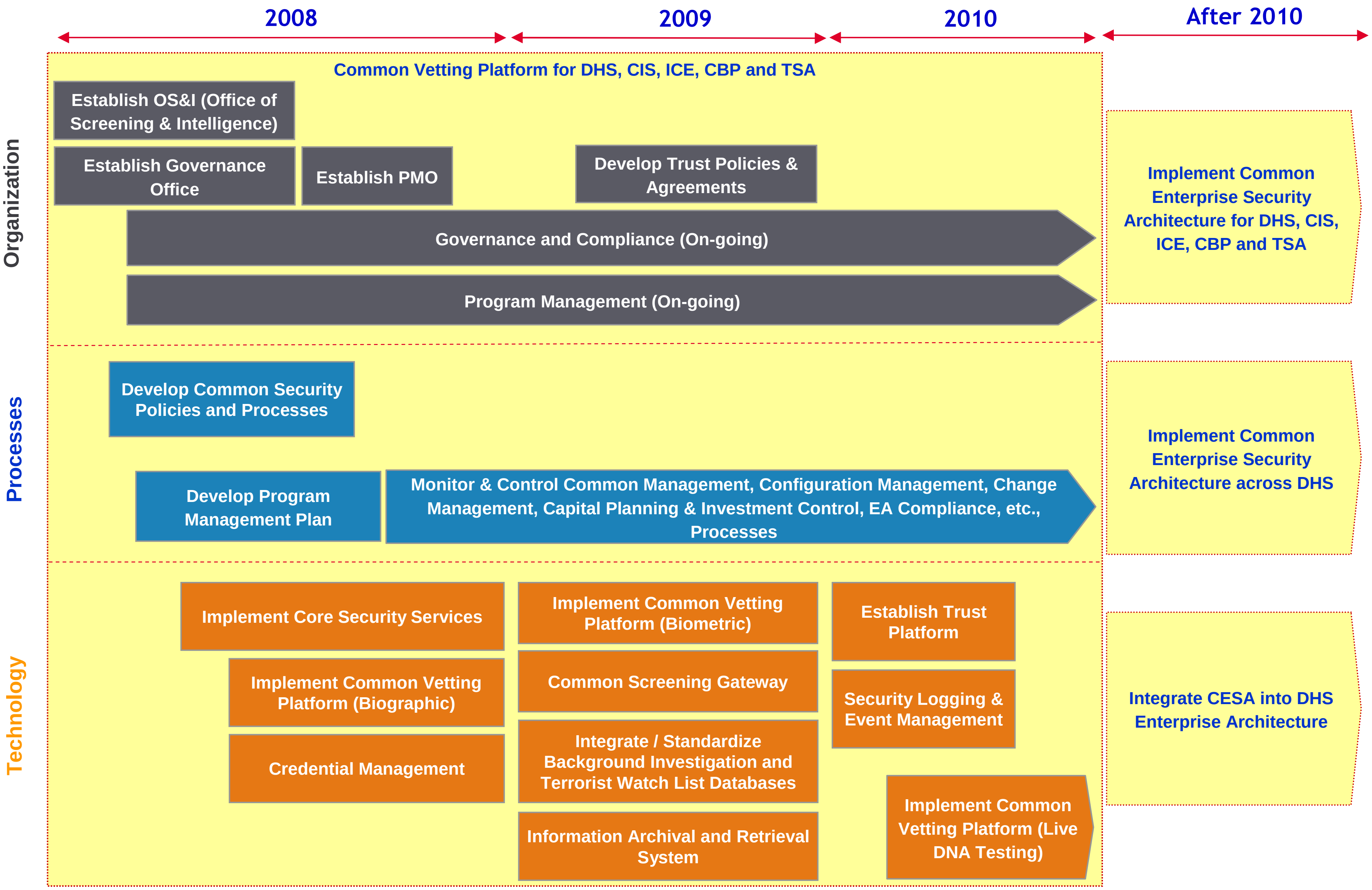
Name: First Name
Description: First name of the individual having at least one letter (ie., initial)
Name: Last Name
Description: Last name of the individual having at least two letters
Name: Date of Birth
Description: Date of Birth of the individual represented as month/day/year
Name: Gender
Description: Sex of the individual represented as M or F.
Relationships: Data provided for in the VETTING REQUEST.

Key CESA Limitations

- CESA is a segment architecture focusing on Security and sub-agency (DHS, CIS, ICE, CBP & TSA) specific identity & credentialing programs
- CESA is not integrated with DHS Enterprise Architecture
- CESA Assessment Framework and Maturity Model has not been defined yet
- EA Repository Management Framework has been developed yet

Transition Strategy / Plan

DHS CESA Sequencing Plan



2008

2009

2010

After 2010

Common Vetting Platform for DHS, CIS, ICE, CBP and TSA

Organization

Establish OS&I (Office of Screening & Intelligence)

Establish Governance Office

Establish PMO

Develop Trust Policies & Agreements

Governance and Compliance (On-going)

Program Management (On-going)

Implement Common Enterprise Security Architecture for DHS, CIS, ICE, CBP and TSA

Processes

Develop Common Security Policies and Processes

Develop Program Management Plan

Monitor & Control Common Management, Configuration Management, Change Management, Capital Planning & Investment Control, EA Compliance, etc., Processes

Implement Common Enterprise Security Architecture across DHS

Technology

Implement Core Security Services

Implement Common Vetting Platform (Biographic)

Credential Management

Implement Common Vetting Platform (Biometric)

Common Screening Gateway

Integrate / Standardize Background Investigation and Terrorist Watch List Databases

Information Archival and Retrieval System

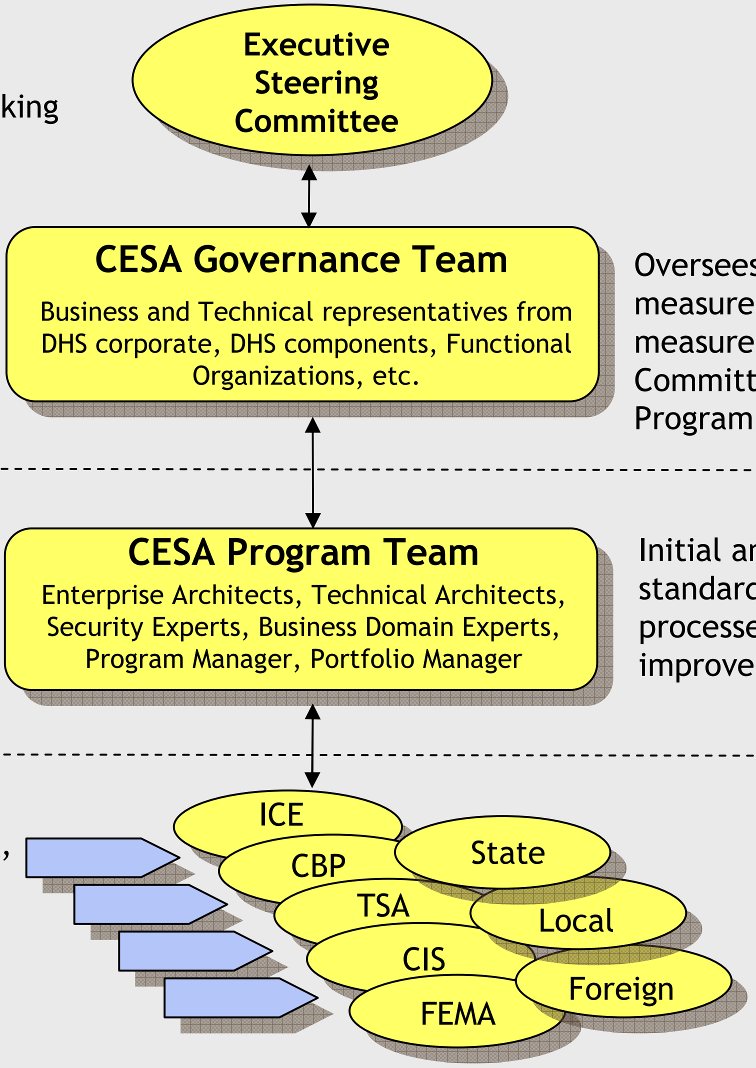
Establish Trust Platform

Security Logging & Event Management

Implement Common Vetting Platform (Live DNA Testing)

Integrate CESA into DHS Enterprise Architecture

DHS CESA Governance Framework



Provides leadership, commitment, driving consensus and decision-making

Executive Steering Committee

Set Direction

Setting strategic priorities, provides resources and driving synergy across CESA initiatives

CESA Governance Team

Business and Technical representatives from DHS corporate, DHS components, Functional Organizations, etc.

Oversees overall program and measurements; reports measurements to Steering Committee; coordination with Program Team

CESA Program Management

Day-to-day operations management, communication, escalation and support across CESA initiatives

CESA Program Team

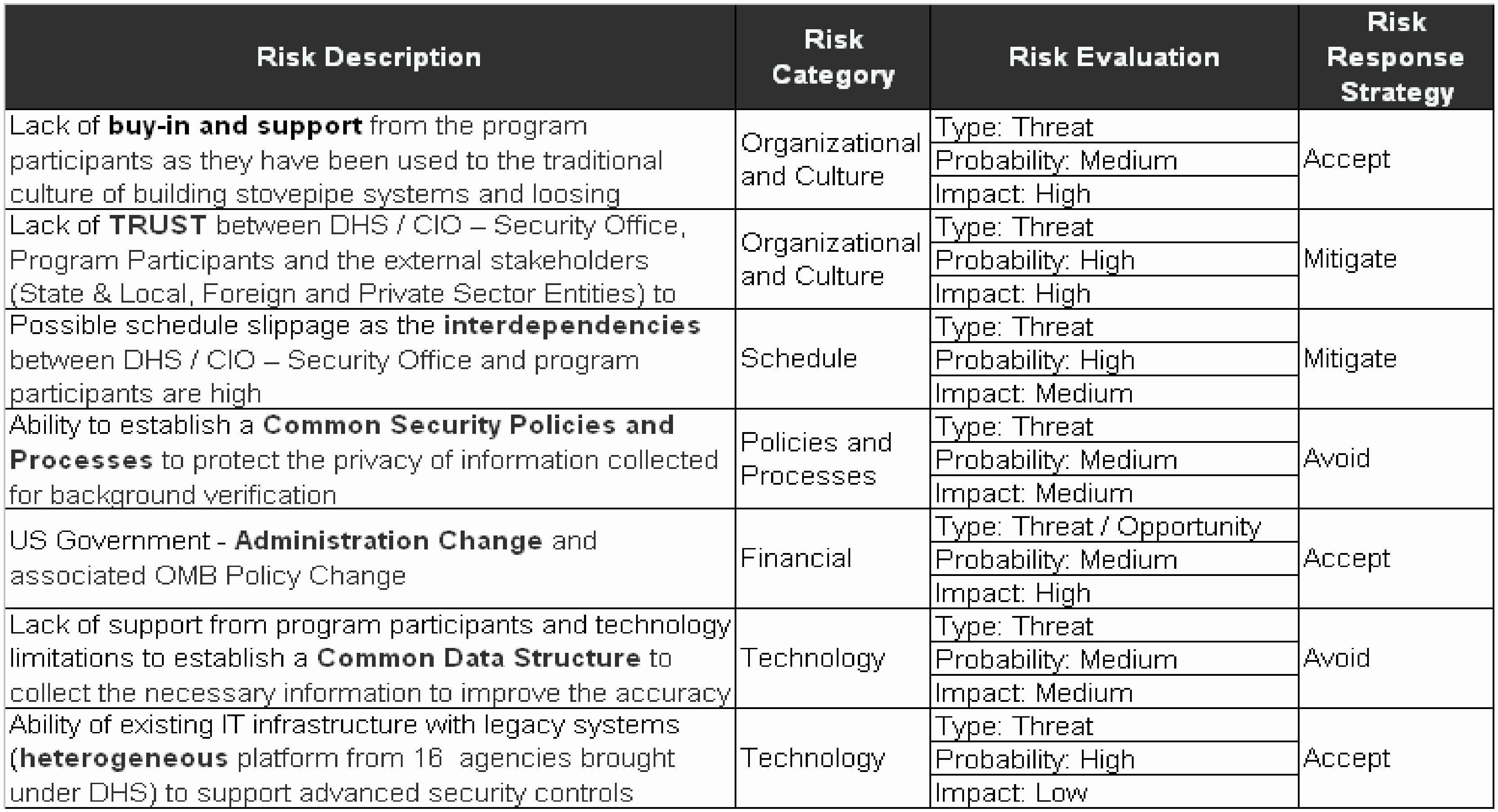
Enterprise Architects, Technical Architects, Security Experts, Business Domain Experts, Program Manager, Portfolio Manager

Initial and ongoing management of standards, policies, controls, and processes, driving continual improvement

CESA Program Integration

Managing deployment of initiatives, communicating, establishing technical and business requirements, reporting, and escalation

Risk Management Plan

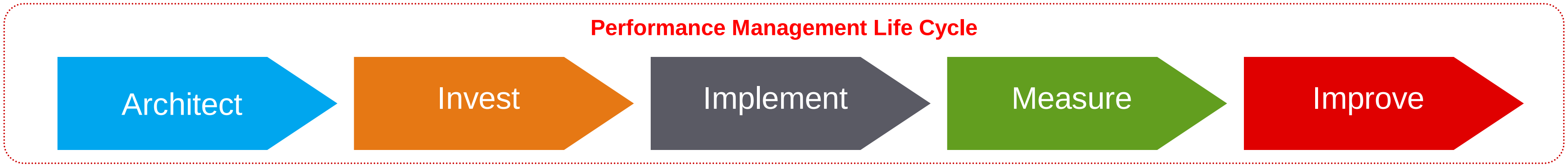


Risk Description	Risk Category	Risk Evaluation	Risk Response Strategy
Lack of **buy-in and support** from the program participants as they have been used to the traditional culture of building stovepipe systems and loosing	Organizational and Culture	Type: Threat Probability: Medium Impact: High	Accept
Lack of **TRUST** between DHS / CIO – Security Office, Program Participants and the external stakeholders (State & Local, Foreign and Private Sector Entities) to	Organizational and Culture	Type: Threat Probability: High Impact: High	Mitigate
Possible schedule slippage as the **interdependencies** between DHS / CIO – Security Office and program participants are high	Schedule	Type: Threat Probability: High Impact: Medium	Mitigate
Ability to establish a **Common Security Policies and Processes** to protect the privacy of information collected for background verification	Policies and Processes	Type: Threat Probability: Medium Impact: Medium	Avoid
US Government - **Administration Change** and associated OMB Policy Change	Financial	Type: Threat / Opportunity Probability: Medium Impact: High	Accept
Lack of support from program participants and technology limitations to establish a **Common Data Structure** to collect the necessary information to improve the accuracy	Technology	Type: Threat Probability: Medium Impact: Medium	Avoid
Ability of existing IT infrastructure with legacy systems (**heterogeneous** platform from 16 agencies brought under DHS) to support advanced security controls	Technology	Type: Threat Probability: High Impact: Low	Accept

Communication Plan

What needs to be communicated	Why	Between Whom	Best Method for Communication	Responsibility	When and How Often
Vetting / Background Investigation Results	Apprehend and deport illegal aliens and take legal actions on potential terrorists	DHS and Law Enforcement Entities	Electronic Communication (Written, Formal)	Department of Homeland Security – Office of Screening and Investigation (OS&I)	Real-Time and Event Driven (When Travel Reservations Made, Illegal Alien is Identified, etc.)
Security Policy	Ensure consistent enforcement of DHS security policy across DHS and its 22 component agencies	DHS / CSO Office and DHS OS&I Office	Electronic Communication (Written, Formal)	DHS / CSO Office	When initial security policy is developed and ongoing refinements are made
Trust Agreements for Information Sharing	Enable trust and information sharing	DHS and State, Local, Tribal & Foreign Government Entities	Electronic Communication (Written, Formal)	DHS / CSO Office	When trust agreements are established initially and when refinements are made to the original agreement
Program Management Plan, Initiative Progress	Communicate Plan and Progress to participating DHS components to ensure alignment, buy-in and ongoing support for the program	CESA / PMO Office and Participating DHS Components	Electronic Communication (Written, Informal)	CESA / PMO Office	Weekly / Monthly Communications
Lessons Learned and Best Practices	Communicate Lessons Learned and Best Practices to enable continuous improvement and eliminate duplication of efforts	CESA PMO Office and Participating DHS Components	Electronic Communication (Written, Informal)	CESA / PMO Office	Weekly / Monthly Communication

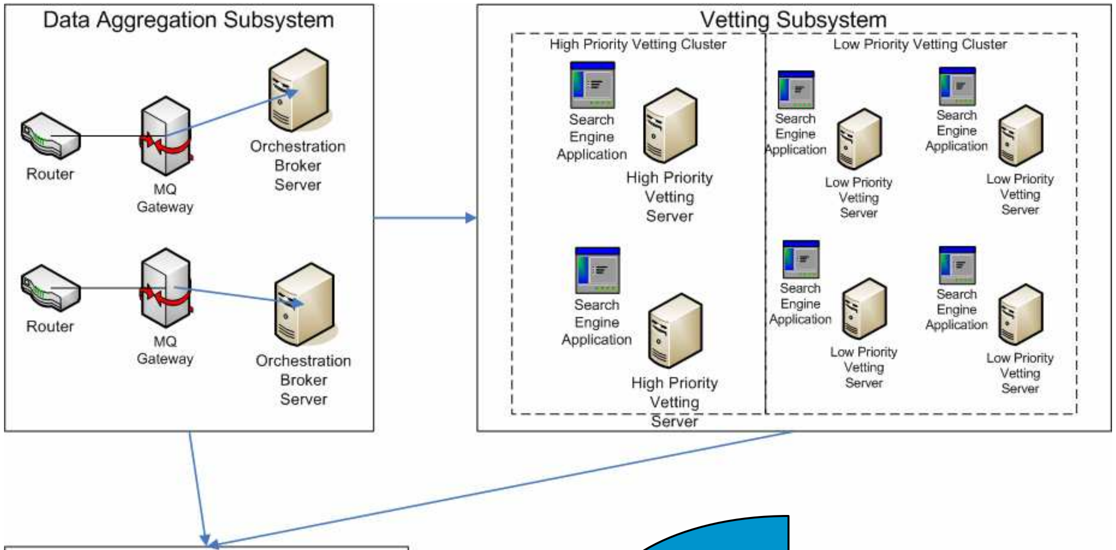
Performance Management Plan

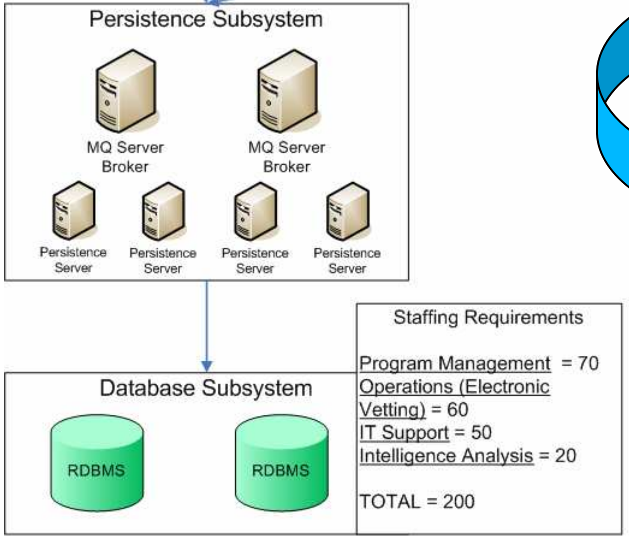

Performance Management Life Cycle

Measurement Areas	Measurement Category	Measurement Category	Measurement Indicator	Baseline Performance	Target Performance	Actual Performance
Mission and Business Results	Homeland Security	Border and Transportation Security	Reduction in threat level to national security over a period of time	Orange	Yellow	
			Reduction in % of bad people entering the country	25%	80%	
			Increase in number of deportation of bad people	20%	90%	
		Key Asset and Critical Infrastructure Protection	Decrease time to revoke access to critical assets and infrastructure	50%	99%	
Customer Results	Homeland Security	1.Border & Transportation Security	% of reduction in false negatives	20%	70%	
		2.Key Asset & Critical Infrastructure Protection	% of reduction in false positives	20%	70%	
Processes & Activities	Knowledge Creation and Management	Research & Development	Reduction in cost of vetting an identity	$1000s	$100s	
Technology	Information & Technology Management	Information Systems Development, Maintenance, Security, Record Protection, Sharing and Monitoring	Reduction in cost of implementing and operating vetting programs at DHS component agency level	5%	80%	

Business Case (Technology Area)

Common Vetting Platform Architecture


Data Aggregation Subsystem
Router
MQ Gateway
Orchestration Broker Server
Router
MQ Gateway
Orchestration Broker Server
Vetting Subsystem
High Priority Vetting Cluster
Search Engine Application
High Priority Vetting Server
Search Engine Application
High Priority Vetting Server
Low Priority Vetting Cluster
Search Engine Application
Low Priority Vetting Server
Search Engine Application
Low Priority Vetting Server
Search Engine Application
Low Priority Vetting Server
Search Engine Application
Low Priority Vetting Server

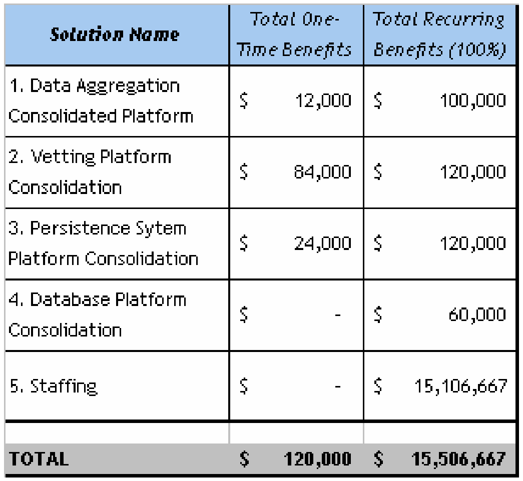


Staffing Requirements

Program Management = 70
Operations (Electronic Vetting) = 60
IT Support = 50
Intelligence Analysis = 20

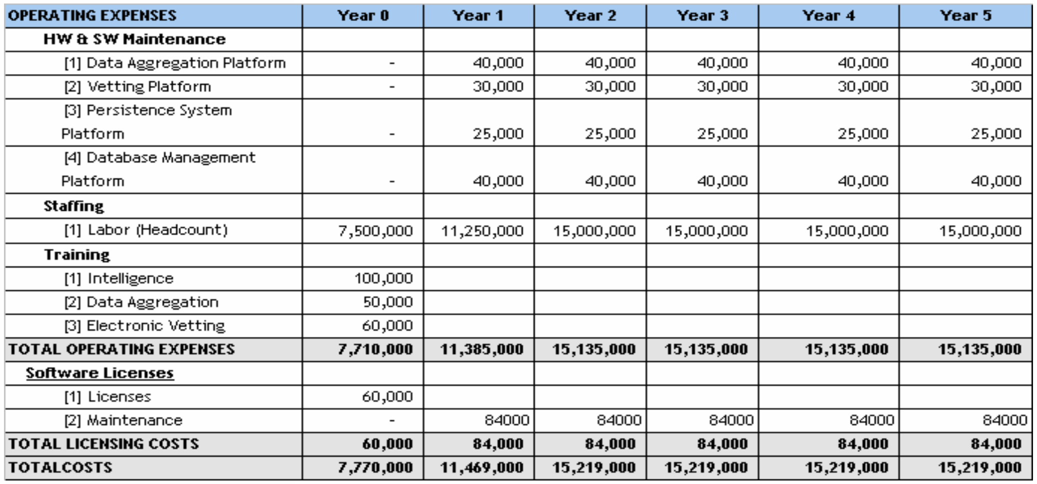
TOTAL = 200

Benefits



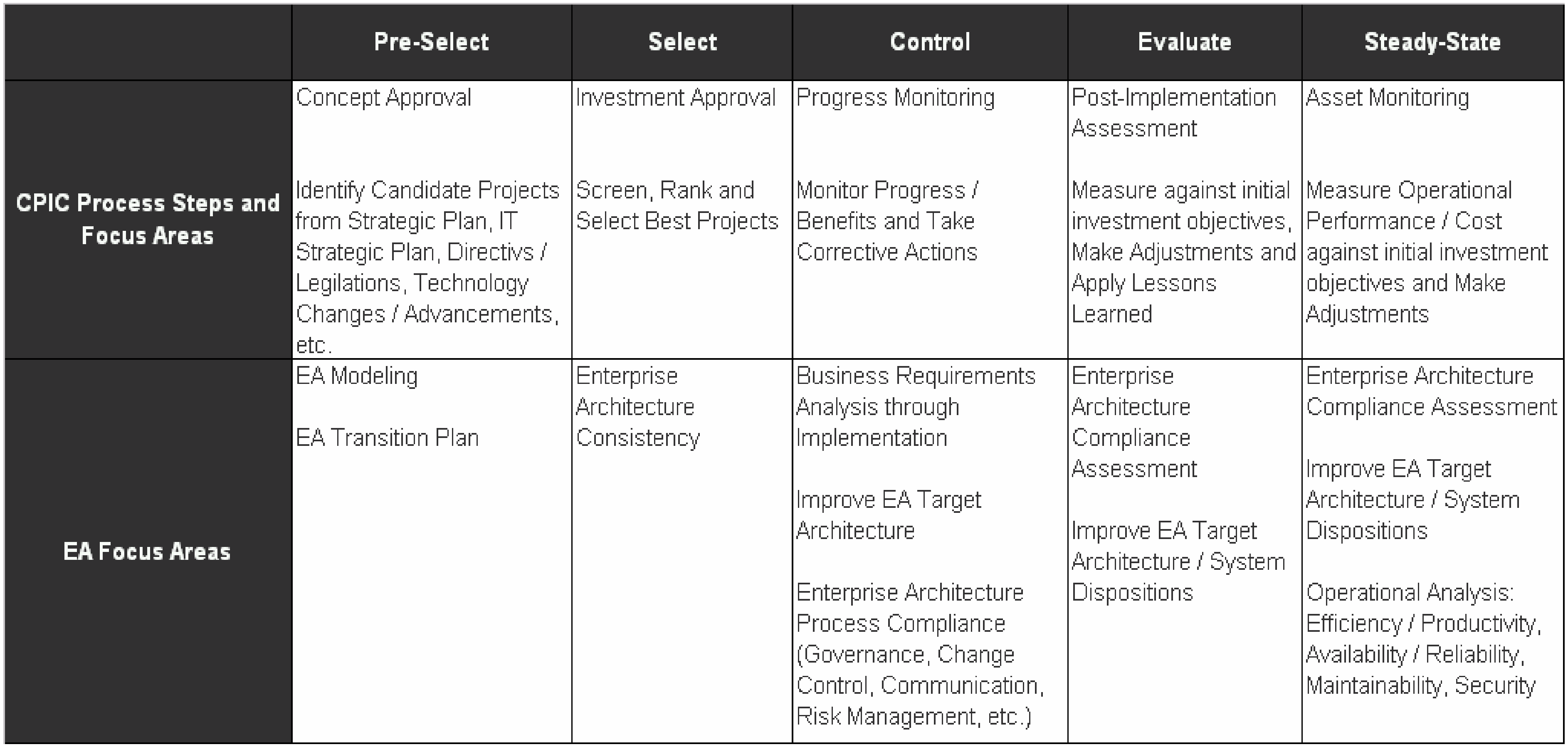
Solution Name	Total One-Time Benefits	Total Recurring Benefits (100%)
1. Data Aggregation Consolidated Platform	$ 12,000	$ 100,000
2. Vetting Platform Consolidation	$ 84,000	$ 120,000
3. Persistence Sytem Platform Consolidation	$ 24,000	$ 120,000
4. Database Platform Consolidation	$ -	$ 60,000
5. Staffing	$ -	$ 15,106,667
TOTAL	**$ 120,000**	**$ 15,506,667**

Costs



OPERATING EXPENSES	Year 0	Year 1	Year 2	Year 3	Year 4	Year 5
HW & SW Maintenance						
[1] Data Aggregation Platform	-	40,000	40,000	40,000	40,000	40,000
[2] Vetting Platform	-	30,000	30,000	30,000	30,000	30,000
[3] Persistence System Platform	-	25,000	25,000	25,000	25,000	25,000
[4] Database Management Platform	-	40,000	40,000	40,000	40,000	40,000
Staffing						
[1] Labor (Headcount)	7,500,000	11,250,000	15,000,000	15,000,000	15,000,000	15,000,000
Training						
[1] Intelligence	100,000					
[2] Data Aggregation	50,000					
[3] Electronic Vetting	60,000					
TOTAL OPERATING EXPENSES	**7,710,000**	**11,385,000**	**15,135,000**	**15,135,000**	**15,135,000**	**15,135,000**
Software Licenses						
[1] Licenses	60,000					
[2] Maintenance	-	84000	84000	84000	84000	84000
TOTAL LICENSING COSTS	**60,000**	**84,000**	**84,000**	**84,000**	**84,000**	**84,000**
TOTALCOSTS	**7,770,000**	**11,469,000**	**15,219,000**	**15,219,000**	**15,219,000**	**15,219,000**

EA & CPIC Integration Plan



	Pre-Select	Select	Control	Evaluate	Steady-State
CPIC Process Steps and Focus Areas	Concept Approval Identify Candidate Projects from Strategic Plan, IT Strategic Plan, Directivs / Legilations, Technology Changes / Advancements, etc.	Investment Approval Screen, Rank and Select Best Projects	Progress Monitoring Monitor Progress / Benefits and Take Corrective Actions	Post-Implementation Assessment Measure against initial investment objectives, Make Adjustments and Apply Lessons Learned	Asset Monitoring Measure Operational Performance / Cost against initial investment objectives and Make Adjustments
EA Focus Areas	EA Modeling EA Transition Plan	Enterprise Architecture Consistency	Business Requirements Analysis through Implementation Improve EA Target Architecture Enterprise Architecture Process Compliance (Governance, Change Control, Communication, Risk Management, etc.)	Enterprise Architecture Compliance Assessment Improve EA Target Architecture / System Dispositions	Enterprise Architecture Compliance Assessment Improve EA Target Architecture / System Dispositions Operational Analysis: Efficiency / Productivity, Availability / Reliability, Maintainability, Security

CESA Benefits Summary

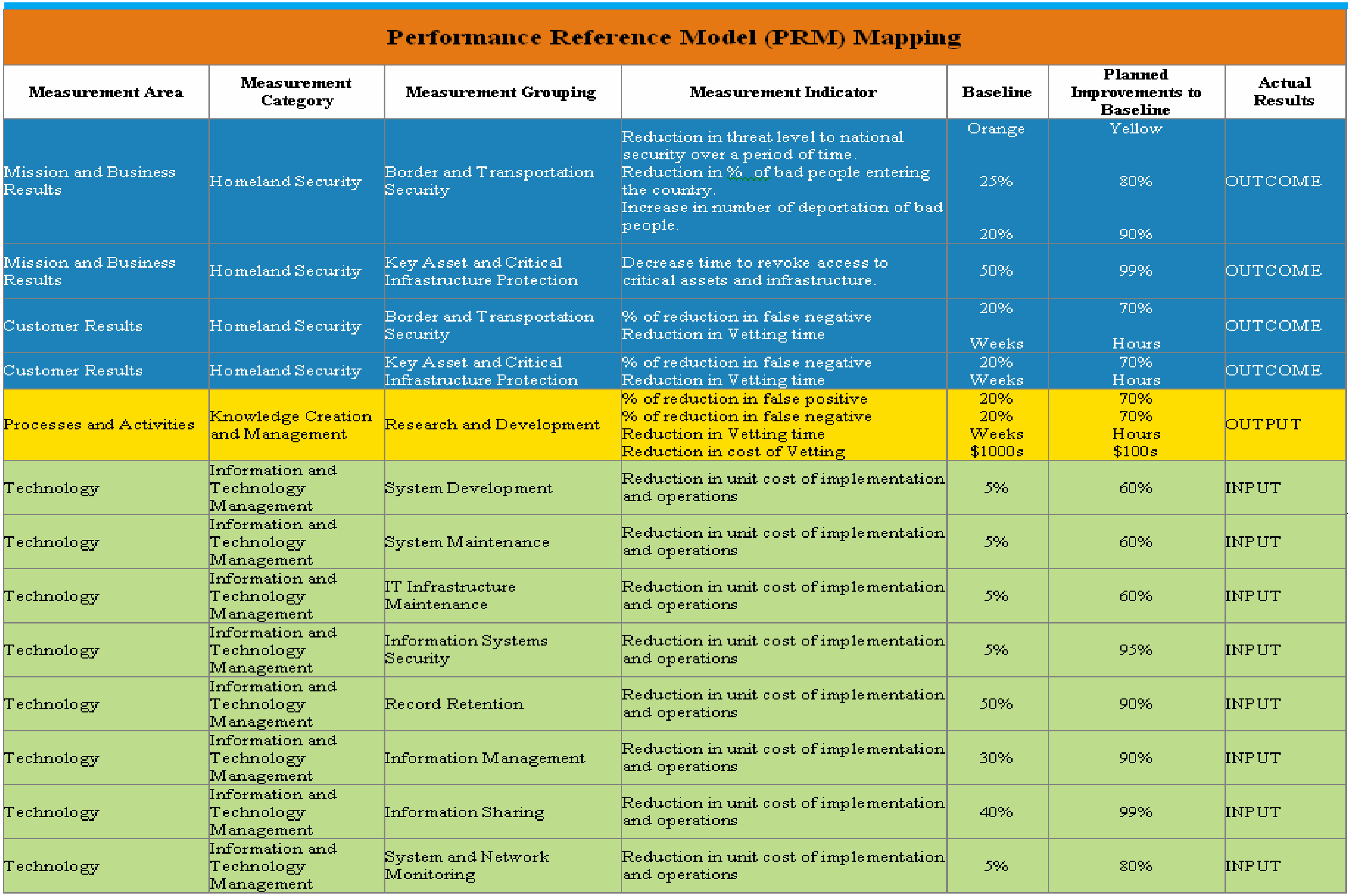
CESA Benefits Summary

Implementing the CESA would lead to significant improvements in terms of people, process, policy and technology

- **Organizational Advantages:** Create one organization responsible for managing and integrating common vetting and credentialing capabilities that would eliminate “silo” development of technology and use of resources
- **Process Advantages:** Instill standard processes across the different programs but also ensure best practices are adhered to and implement automation and process improvement in areas where it is needed
- **Policy Advantages:** Consolidate processes and policies through collaboration and consensus to ensure proper adoption across DHS subcomponents
- **Technical Advantages:** Lower implementation, operation and maintenance costs through eliminating redundant systems *and* consistent vetting and adjudication results for the same individual. The CESA would also provide for improved access and control of critical information and consistent technical standards and security controls

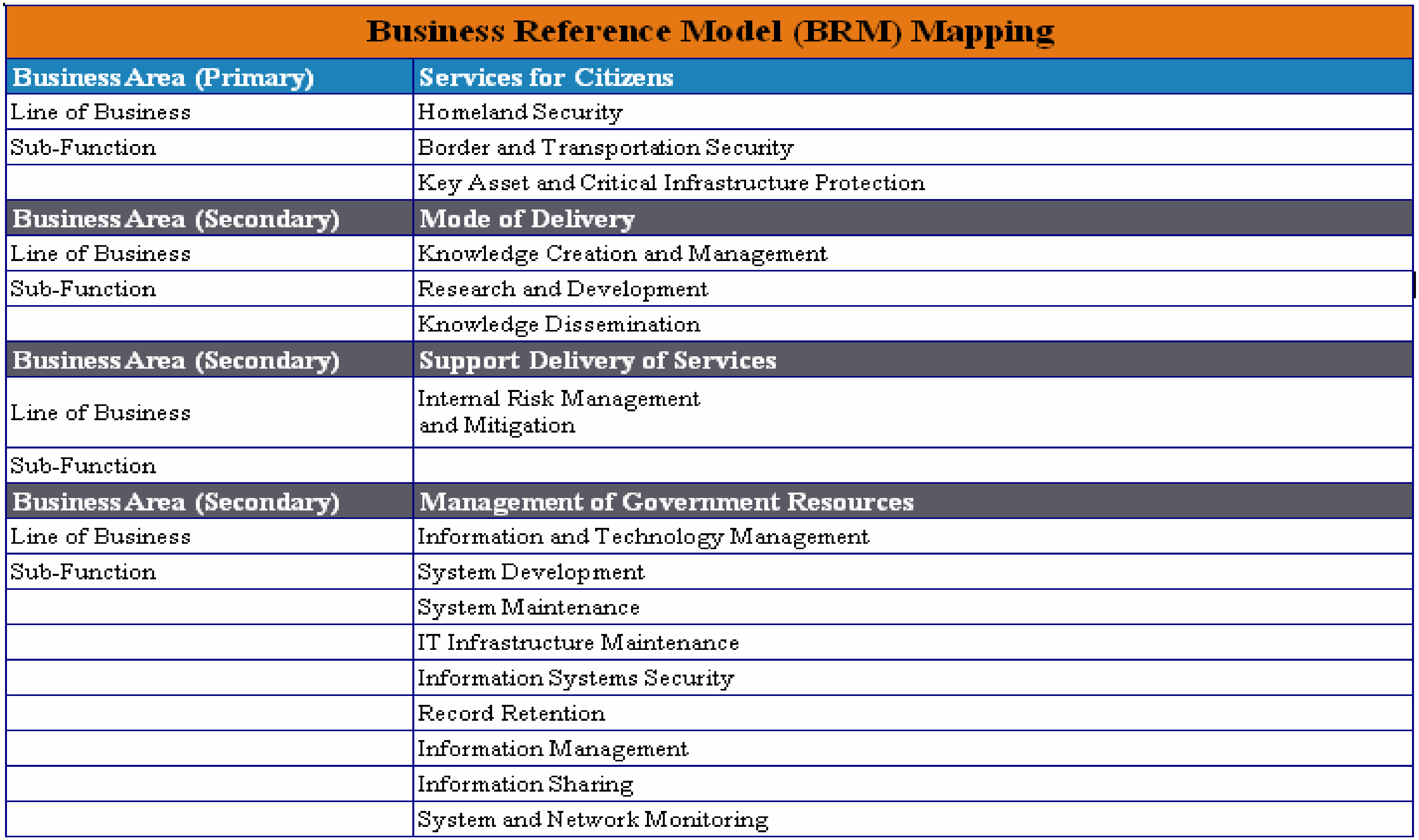
Appendix A - FEA Reference Models

PRM



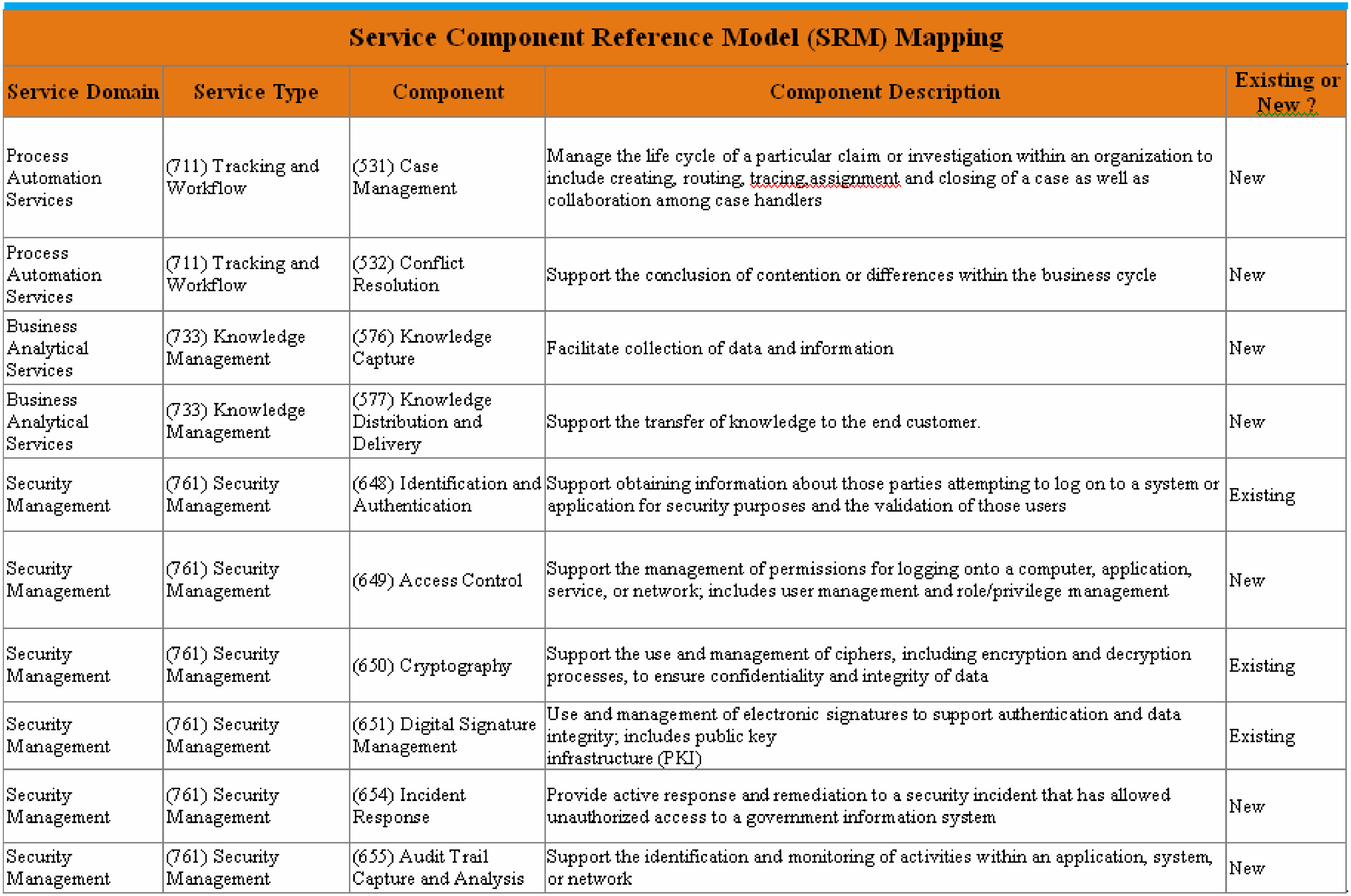
Performance Reference Model (PRM) Mapping						
Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	Baseline	Planned Improvements to Baseline	Actual Results
Mission and Business Results	Homeland Security	Border and Transportation Security	Reduction in threat level to national security over a period of time. Reduction in % of bad people entering the country. Increase in number of deportation of bad people.	Orange 25% 20%	Yellow 80% 90%	OUTCOME
Mission and Business Results	Homeland Security	Key Asset and Critical Infrastructure Protection	Decrease time to revoke access to critical assets and infrastructure.	50%	99%	OUTCOME
Customer Results	Homeland Security	Border and Transportation Security	% of reduction in false negative Reduction in Vetting time	20% Weeks	70% Hours	OUTCOME
Customer Results	Homeland Security	Key Asset and Critical Infrastructure Protection	% of reduction in false negative Reduction in Vetting time	20% Weeks	70% Hours	OUTCOME
Processes and Activities	Knowledge Creation and Management	Research and Development	% of reduction in false positive % of reduction in false negative Reduction in Vetting time Reduction in cost of Vetting	20% 20% Weeks $1000s	70% 70% Hours $100s	OUTPUT
Technology	Information and Technology Management	System Development	Reduction in unit cost of implementation and operations	5%	60%	INPUT
Technology	Information and Technology Management	System Maintenance	Reduction in unit cost of implementation and operations	5%	60%	INPUT
Technology	Information and Technology Management	IT Infrastructure Maintenance	Reduction in unit cost of implementation and operations	5%	60%	INPUT
Technology	Information and Technology Management	Information Systems Security	Reduction in unit cost of implementation and operations	5%	95%	INPUT
Technology	Information and Technology Management	Record Retention	Reduction in unit cost of implementation and operations	50%	90%	INPUT
Technology	Information and Technology Management	Information Management	Reduction in unit cost of implementation and operations	30%	90%	INPUT
Technology	Information and Technology Management	Information Sharing	Reduction in unit cost of implementation and operations	40%	99%	INPUT
Technology	Information and Technology Management	System and Network Monitoring	Reduction in unit cost of implementation and operations	5%	80%	INPUT

BRM



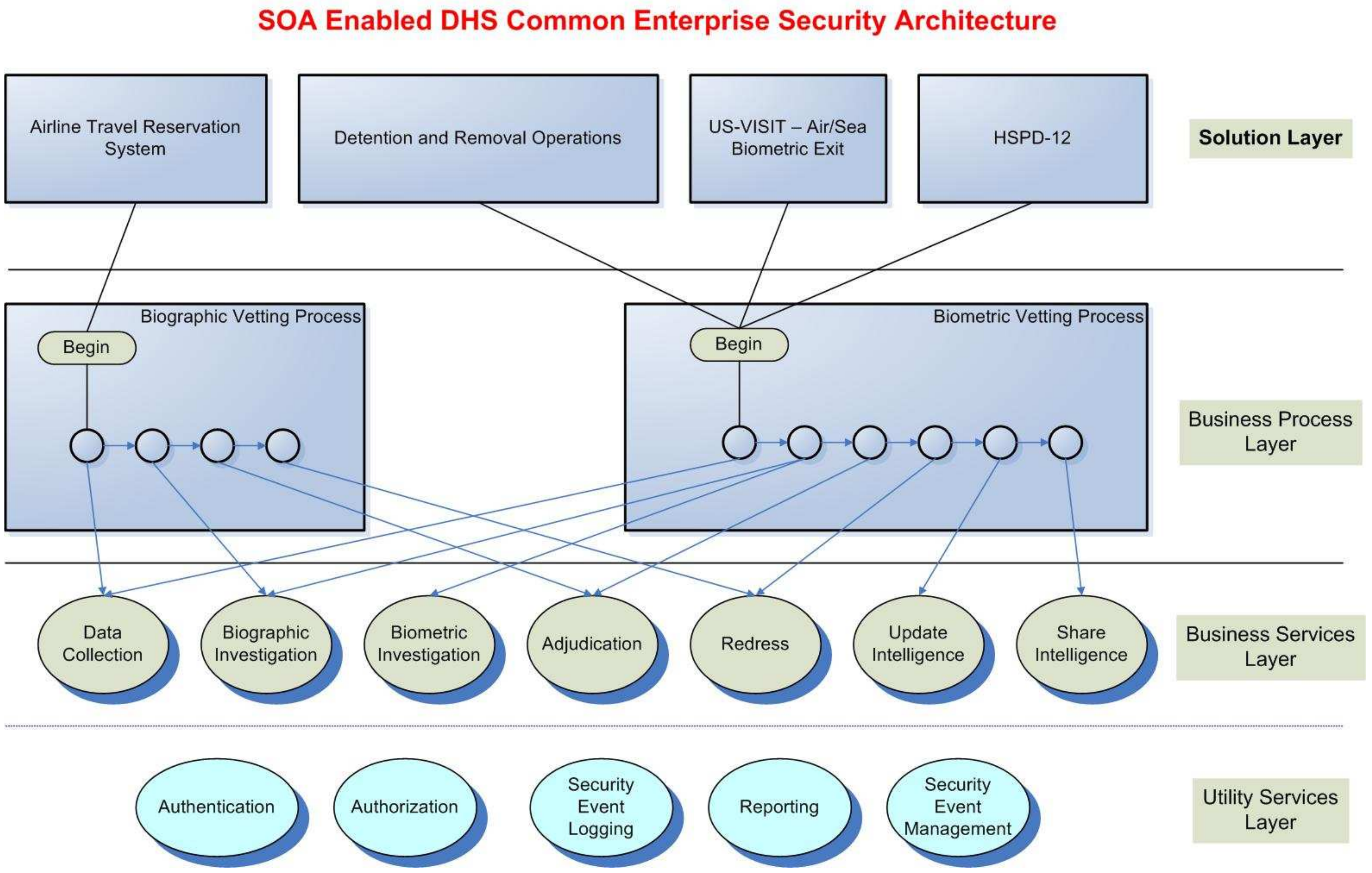
Business Reference Model (BRM) Mapping	
Business Area (Primary)	**Services for Citizens**
Line of Business	Homeland Security
Sub-Function	Border and Transportation Security
	Key Asset and Critical Infrastructure Protection
Business Area (Secondary)	**Mode of Delivery**
Line of Business	Knowledge Creation and Management
Sub-Function	Research and Development
	Knowledge Dissemination
Business Area (Secondary)	**Support Delivery of Services**
Line of Business	Internal Risk Management and Mitigation
Sub-Function	
Business Area (Secondary)	**Management of Government Resources**
Line of Business	Information and Technology Management
Sub-Function	System Development
	System Maintenance
	IT Infrastructure Maintenance
	Information Systems Security
	Record Retention
	Information Management
	Information Sharing
	System and Network Monitoring

SRM



Service Component Reference Model (SRM) Mapping				
Service Domain	Service Type	Component	Component Description	Existing or New ?
Process Automation Services	(711) Tracking and Workflow	(531) Case Management	Manage the life cycle of a particular claim or investigation within an organization to include creating, routing, tracing assignment and closing of a case as well as collaboration among case handlers	New
Process Automation Services	(711) Tracking and Workflow	(532) Conflict Resolution	Support the conclusion of contention or differences within the business cycle	New
Business Analytical Services	(733) Knowledge Management	(576) Knowledge Capture	Facilitate collection of data and information	New
Business Analytical Services	(733) Knowledge Management	(577) Knowledge Distribution and Delivery	Support the transfer of knowledge to the end customer.	New
Security Management	(761) Security Management	(648) Identification and Authentication	Support obtaining information about those parties attempting to log on to a system or application for security purposes and the validation of those users	Existing
Security Management	(761) Security Management	(649) Access Control	Support the management of permissions for logging onto a computer, application, service, or network; includes user management and role/privilege management	New
Security Management	(761) Security Management	(650) Cryptography	Support the use and management of ciphers, including encryption and decryption processes, to ensure confidentiality and integrity of data	Existing
Security Management	(761) Security Management	(651) Digital Signature Management	Use and management of electronic signatures to support authentication and data integrity; includes public key infrastructure (PKI)	Existing
Security Management	(761) Security Management	(654) Incident Response	Provide active response and remediation to a security incident that has allowed unauthorized access to a government information system	New
Security Management	(761) Security Management	(655) Audit Trail Capture and Analysis	Support the identification and monitoring of activities within an application, system, or network	New

SOA Enabled CESA

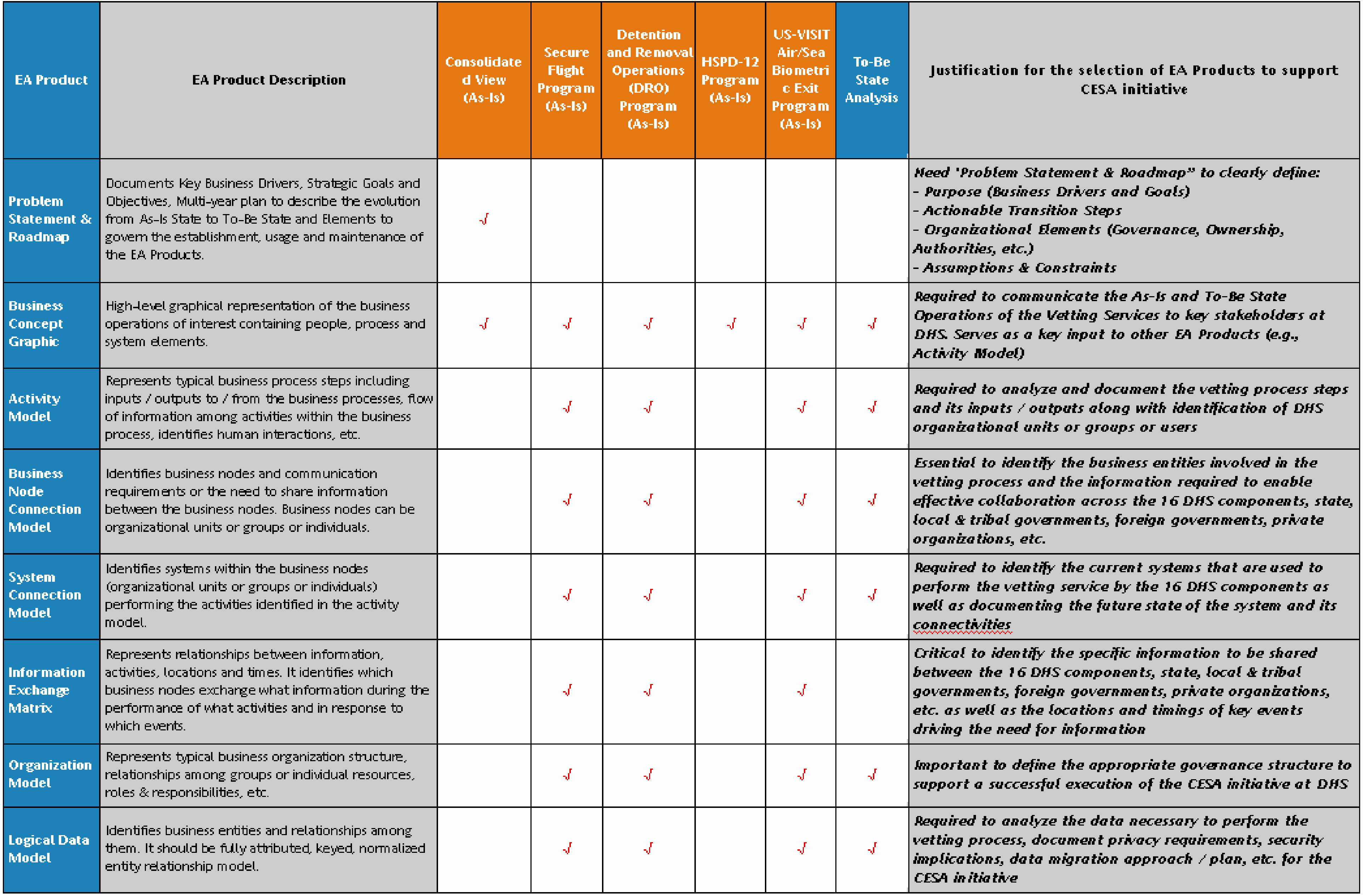


TRM

Service Area	Service Category	Service Standard	Standards Mapping
Service Access and Delivery	Access Channels	Web Browser	FireFox Internet Explorer Netscape Communicator
		Wireless / PDA	Palm Operating System Blackberry
		Collaboration / Communications	Email
	Delivery Channels	Intranet	
		Extranet	
		Virtual Private Network(VPN)	
	Service Requirements	Legislative / Compliance	Security, Privacy(P3P), Privacy (Liberty Alliance)
		Authentication	
		Hosting	Internal
	Service Transport	Support Network Services	IMAP / POP3, MIME, SMTP, ESMTP, T.120, H.323, SNMP, LDAP, X.500, DHCP, DNS, BGP, X400
		Service Transport	TCP, IP, HTTP, HTTPS, WAP, FTP, IPSEC
Service Platform and Infrastructure	Support Platforms	Platform Independent	J2EE, Linux
		Platform Dependent	Windows OS
	Delivery Servers	Web Servers	Apache
		Application Servers	JBoss
	Hardware / Infrastructure	Servers / Computers	Intel Servers
		Embedded Technology	RAM, Hard disk drives, Microprocessor, RAID(Redundant Array Of Independent Disk)
		Devices Peripherals	Scanner
		WAN	Frame Relay, ATM(Asynchronous Transfer Mode)
		LAN	Ethernet, VLAN(Virtual LAN)
		Network Devices / Standards	Hub, Switch, Router, NIC(Network Interface Card), Transceivers, Gateway, ISDN, T1/T3, DSL, Firewall
	Software Engineering	IDE	Visual studio
		Software Configuration Management	Version Management, Defect Tracking / Issue Management, Task Management, Change Management, Deployment Management, Requirements Management and Traceability
		Test Management	Functional Testing, Business cycle testing, Usability testing, Performance profiling, Load/Stress/Volume testing, Security and access control testing, Reliability testing , Configuration Testing, Installation Testing
		Modeling	UML
	Database / Storage	Database	Oracle
		Storage	(SAN) Storage Area Network
Component Framework	Security	Certificates /Digital Signature	Digital Certificate Authentication, FIPS, SSL
	Presentation / Interface	Static Display	HTML, PDF/A, /X
		Dynamic Server Side Display	JSP (Java Server Pages), ASP(Active Server Pages), ASP .Net
		Content Rendering	DHTML, XHTML, CSS, X3D
		Wireless / Mobile / Voice	WML, XHTMLMP, VXML
	Business Logic	Platform Independent	EJB and JSR168 Portlet
	Data Interchange	Data Exchange	XML, SOAP
	Data Management	Database Connectivity	JDBC
		Reporting and Analysis	OLAP, XML for Analysis
Service Interface and Integration	Integration	Middleware	JMS, SOAP
		Enterprise Application Integration	Business Process Management
	Interoperability	Data Format / Classification	XML
		Data Types / Validation	DTD
		Data Transformation	XSLT
	Interface	Service Discovery	UDDI
		Service Description / Interface	WSDL

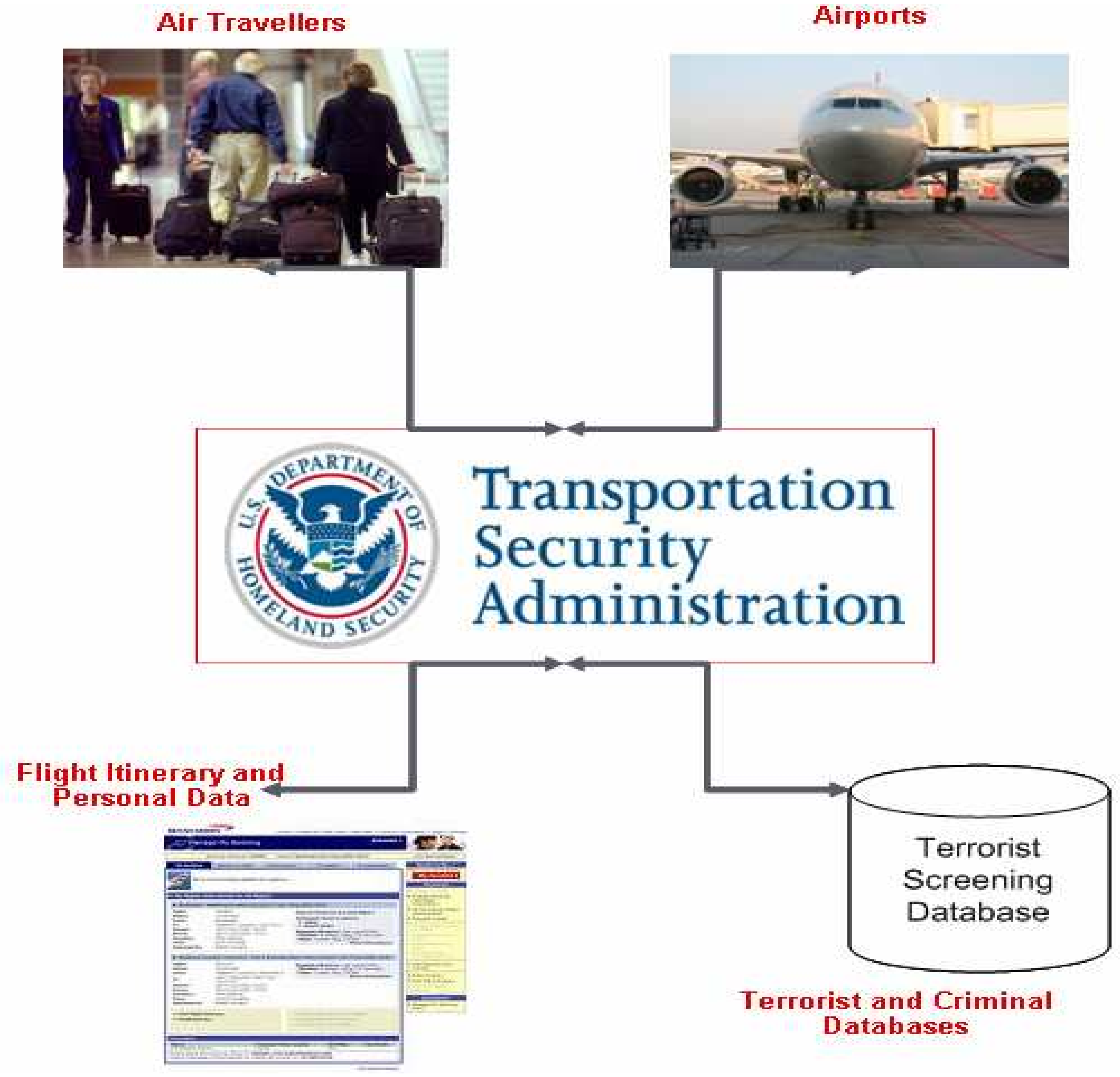
Appendix B - EA Products (As-Is Analysis)

(As-Is) Products



EA Product	EA Product Description	Consolidated View (As-Is)	Secure Flight Program (As-Is)	Detention and Removal Operations (DRO) Program (As-Is)	HSPD-12 Program (As-Is)	US-VISIT Air/Sea Biometric Exit Program (As-Is)	To-Be State Analysis	Justification for the selection of EA Products to support CESA initiative
Problem Statement & Roadmap	Documents Key Business Drivers, Strategic Goals and Objectives, Multi-year plan to describe the evolution from As-Is State to To-Be State and Elements to govern the establishment, usage and maintenance of the EA Products.	✓						*Need 'Problem Statement & Roadmap" to clearly define:* *- Purpose (Business Drivers and Goals)* *- Actionable Transition Steps* *- Organizational Elements (Governance, Ownership, Authorities, etc.)* *- Assumptions & Constraints*
Business Concept Graphic	High-level graphical representation of the business operations of interest containing people, process and system elements.	✓	✓	✓	✓	✓	✓	*Required to communicate the As-Is and To-Be State Operations of the Vetting Services to key stakeholders at DHS. Serves as a key input to other EA Products (e.g., Activity Model)*
Activity Model	Represents typical business process steps including inputs / outputs to / from the business processes, flow of information among activities within the business process, identifies human interactions, etc.		✓	✓		✓	✓	*Required to analyze and document the vetting process steps and its inputs / outputs along with identification of DHS organizational units or groups or users*
Business Node Connection Model	Identifies business nodes and communication requirements or the need to share information between the business nodes. Business nodes can be organizational units or groups or individuals.		✓	✓		✓	✓	*Essential to identify the business entities involved in the vetting process and the information required to enable effective collaboration across the 16 DHS components, state, local & tribal governments, foreign governments, private organizations, etc.*
System Connection Model	Identifies systems within the business nodes (organizational units or groups or individuals) performing the activities identified in the activity model.		✓	✓		✓	✓	*Required to identify the current systems that are used to perform the vetting service by the 16 DHS components as well as documenting the future state of the system and its connectivities*
Information Exchange Matrix	Represents relationships between information, activities, locations and times. It identifies which business nodes exchange what information during the performance of what activities and in response to which events.		✓	✓		✓		*Critical to identify the specific information to be shared between the 16 DHS components, state, local & tribal governments, foreign governments, private organizations, etc. as well as the locations and timings of key events driving the need for information*
Organization Model	Represents typical business organization structure, relationships among groups or individual resources, roles & responsibilities, etc.		✓	✓		✓	✓	*Important to define the appropriate governance structure to support a successful execution of the CESA initiative at DHS*
Logical Data Model	Identifies business entities and relationships among them. It should be fully attributed, keyed, normalized entity relationship model.		✓	✓		✓	✓	*Required to analyze the data necessary to perform the vetting process, document privacy requirements, security implications, data migration approach / plan, etc. for the CESA initiative*

DHS – Secure Flight



Air Travellers

Airports

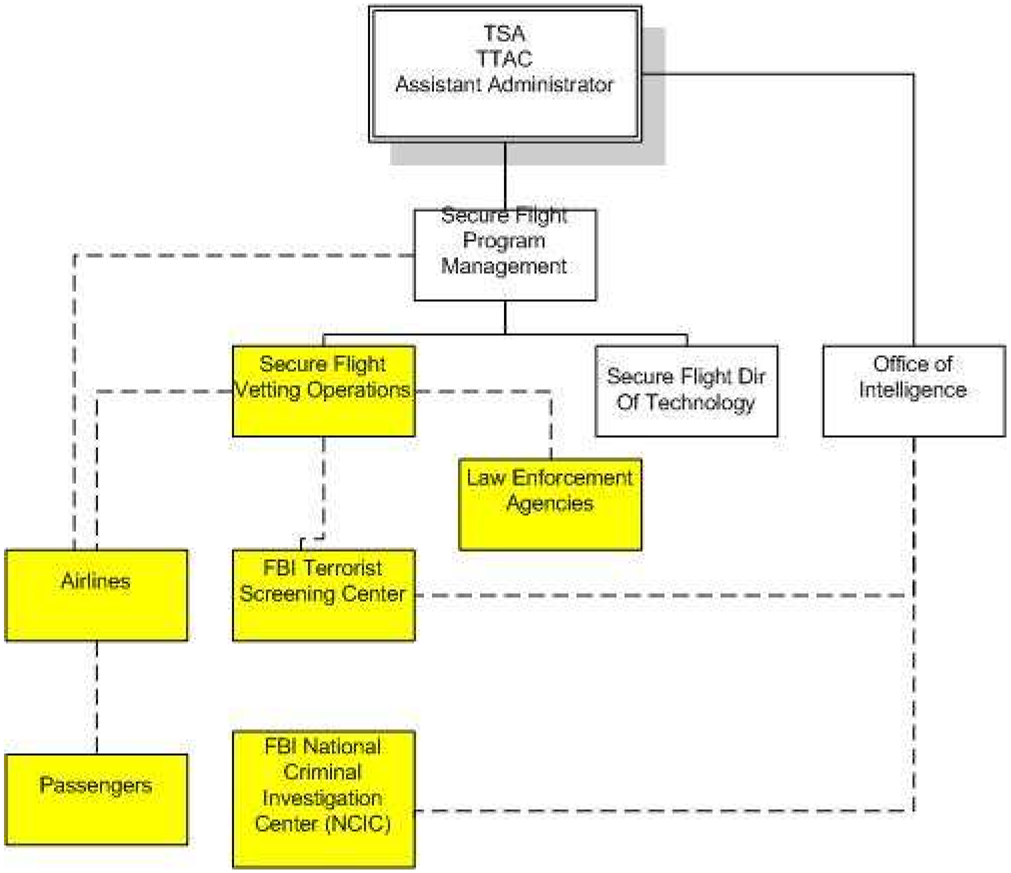
Transportation Security Administration

Flight Itinerary and Personal Data

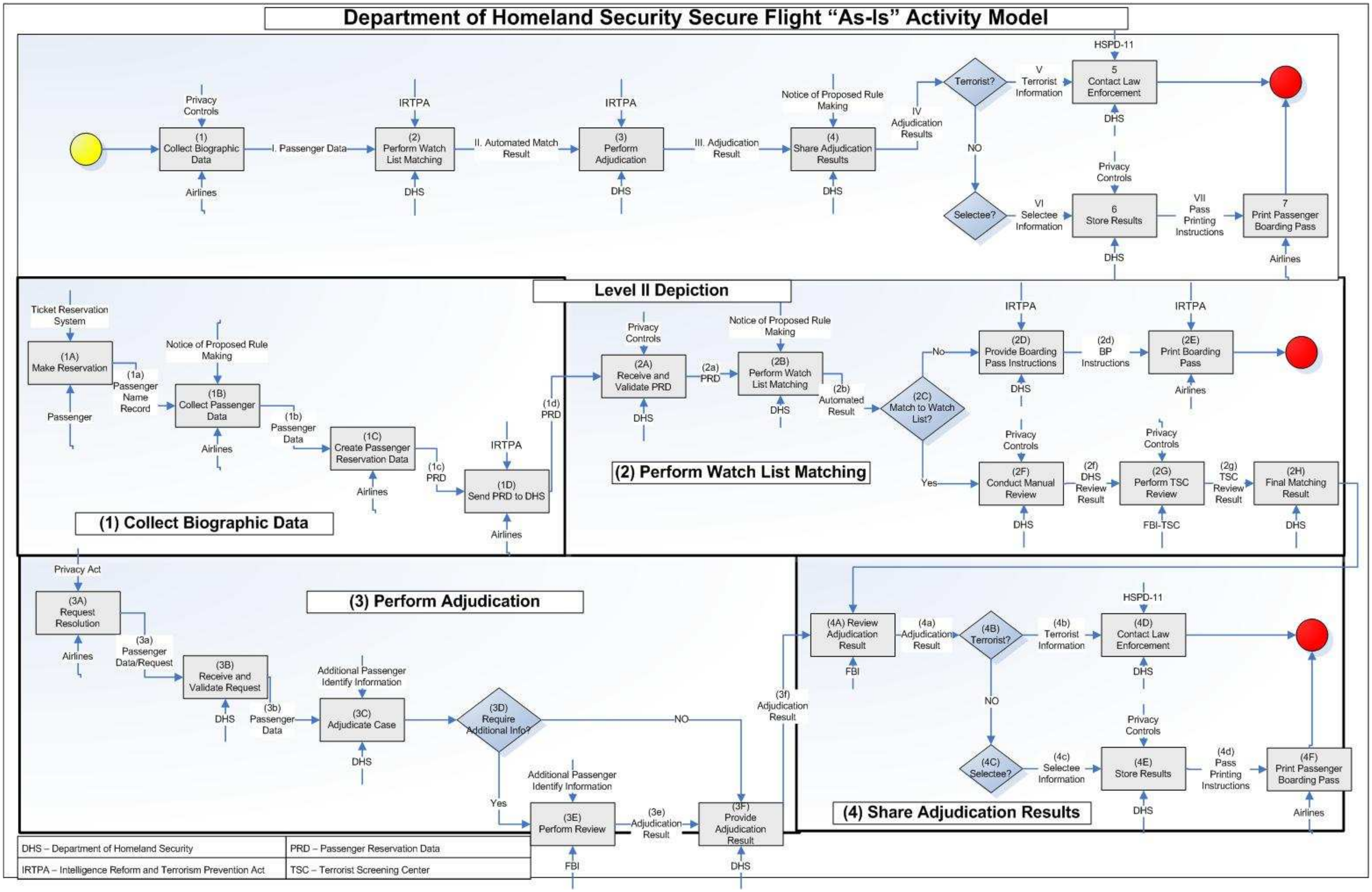
Terrorist Screening Database

Terrorist and Criminal Databases

DHS – Secure Flight


TSA
TTAC
Assistant Administrator
Secure Flight Program Management
Secure Flight Vetting Operations
Secure Flight Dir Of Technology
Office of Intelligence
Law Enforcement Agencies
Airlines
FBI Terrorist Screening Center
Passengers
FBI National Criminal Investigation Center (NCIC)

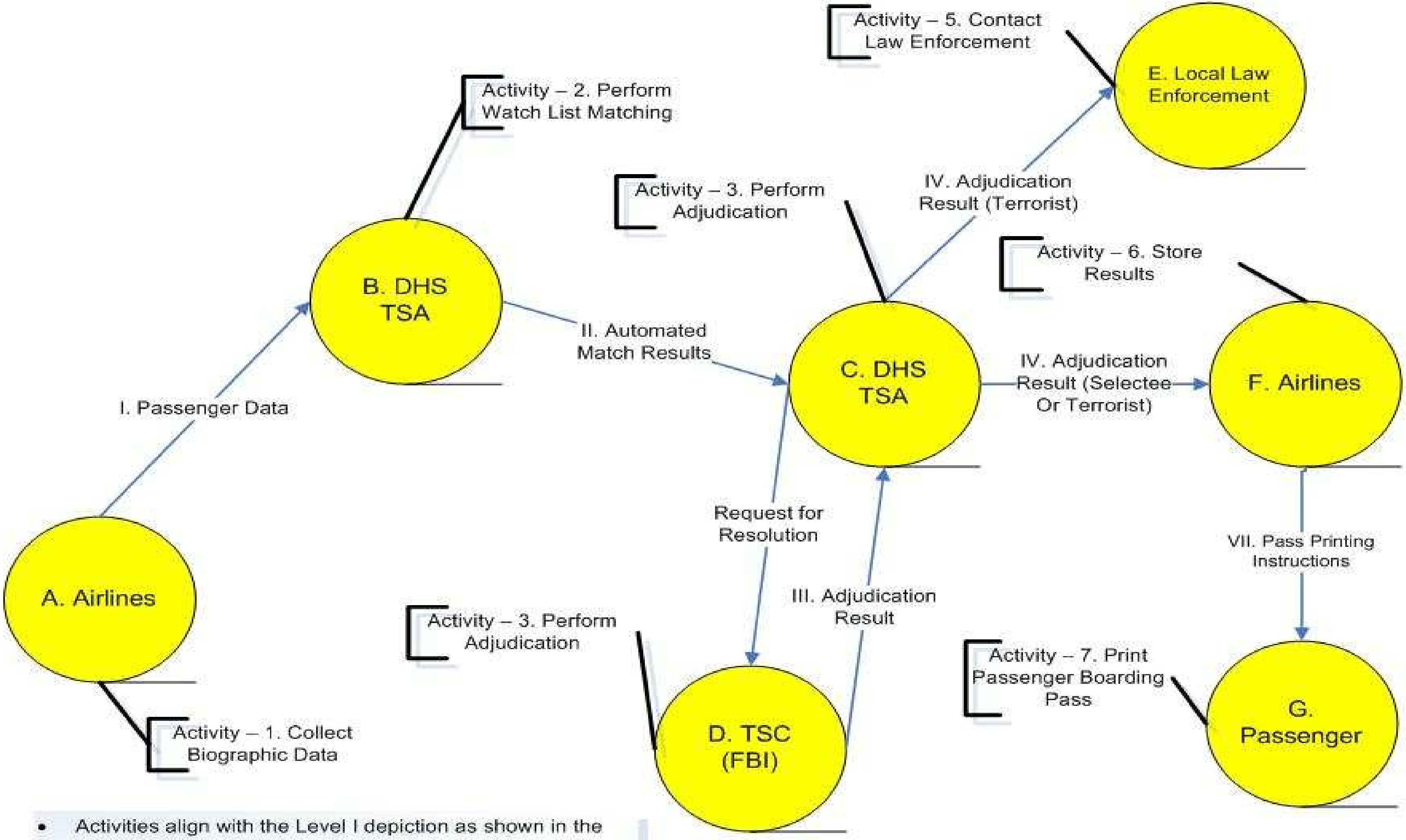
DHS – Secure Flight


Department of Homeland Security Secure Flight "As-Is" Activity Model
Privacy Controls
(1) Collect Biographic Data
Airlines
I. Passenger Data
IRTPA
(2) Perform Watch List Matching
DHS
II. Automated Match Result
IRTPA
(3) Perform Adjudication
DHS
III. Adjudication Result
Notice of Proposed Rule Making
(4) Share Adjudication Results
DHS
IV Adjudication Results
Terrorist?
V Terrorist Information
HSPD-11
5 Contact Law Enforcement
DHS
NO
Selectee?
VI Selectee Information
Privacy Controls
6 Store Results
DHS
VII Pass Printing Instructions
7 Print Passenger Boarding Pass
Airlines
Level II Depiction
Ticket Reservation System
(1A) Make Reservation
Passenger
(1a) Passenger Name Record
Notice of Proposed Rule Making
(1B) Collect Passenger Data
Airlines
(1b) Passenger Data
(1C) Create Passenger Reservation Data
Airlines
(1c) PRD
IRTPA
(1D) Send PRD to DHS
Airlines
(1d) PRD
(1) Collect Biographic Data
Privacy Controls
(2A) Receive and Validate PRD
DHS
(2a) PRD
Notice of Proposed Rule Making
(2B) Perform Watch List Matching
DHS
(2b) Automated Result
(2C) Match to Watch List?
No
Yes
IRTPA
(2D) Provide Boarding Pass Instructions
DHS
(2d) BP Instructions
IRTPA
(2E) Print Boarding Pass
Airlines
(2) Perform Watch List Matching
Privacy Controls
(2F) Conduct Manual Review
DHS
(2f) DHS Review Result
Privacy Controls
(2G) Perform TSC Review
FBI-TSC
(2g) TSC Review Result
(2H) Final Matching Result
DHS
Privacy Act
(3A) Request Resolution
Airlines
(3a) Passenger Data/Request
(3B) Receive and Validate Request
DHS
(3b) Passenger Data
Additional Passenger Identify Information
(3C) Adjudicate Case
DHS
(3D) Require Additional Info?
NO
Yes
(3) Perform Adjudication
Additional Passenger Identify Information
(3E) Perform Review
FBI
(3e) Adjudication Result
(3F) Provide Adjudication Result
DHS
(3f) Adjudication Result
(4A) Review Adjudication Result
FBI
(4a) Adjudication Result
(4B) Terrorist?
(4b) Terrorist Information
HSPD-11
(4D) Contact Law Enforcement
DHS
NO
(4C) Selectee?
(4c) Selectee Information
Privacy Controls
(4E) Store Results
DHS
(4d) Pass Printing Instructions
(4F) Print Passenger Boarding Pass
Airlines
(4) Share Adjudication Results

DHS – Department of Homeland Security	PRD – Passenger Reservation Data
IRTPA – Intelligence Reform and Terrorism Prevention Act	TSC – Terrorist Screening Center

DHS – Secure Flight

Figure 2.0 Department of Homeland Security – "As-Is" Secure Flight Business Node Connection Model



A. Airlines

Activity – 1. Collect Biographic Data

I. Passenger Data

B. DHS TSA

Activity – 2. Perform Watch List Matching

II. Automated Match Results

C. DHS TSA

Activity – 3. Perform Adjudication

Request for Resolution

D. TSC (FBI)

Activity – 3. Perform Adjudication

III. Adjudication Result

IV. Adjudication Result (Terrorist)

E. Local Law Enforcement

Activity – 5. Contact Law Enforcement

IV. Adjudication Result (Selectee Or Terrorist)

F. Airlines

Activity – 6. Store Results

VII. Pass Printing Instructions

G. Passenger

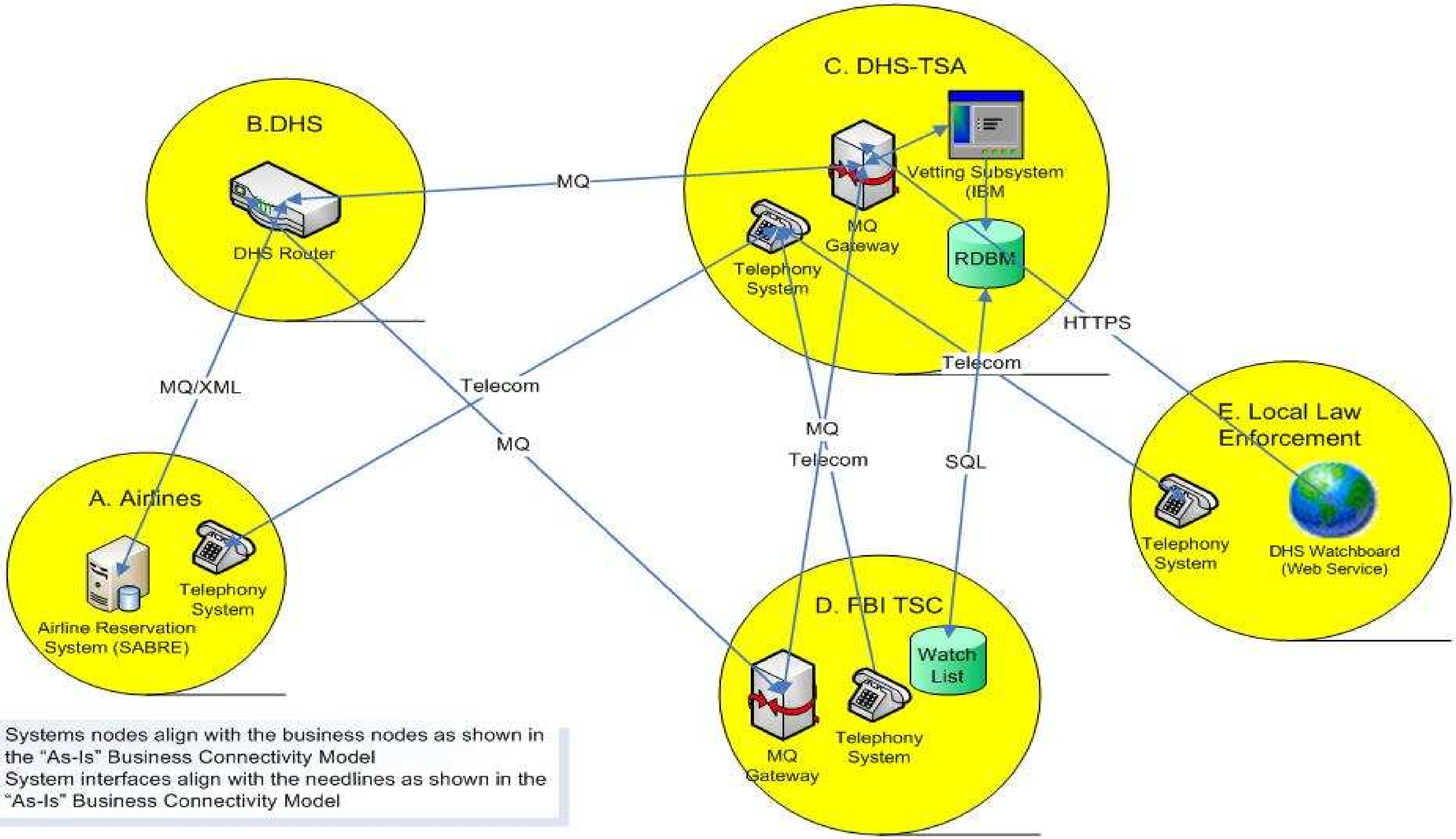
Activity – 7. Print Passenger Boarding Pass

- Activities align with the Level I depiction as shown in the "As-Is" Activity Model
- Information provided in the needlines align with the Level I depiction as shown in the "As-Is" Activity Model

DHS – Department of Homeland Security
TSC – Terrorist Screening Center

DHS – Secure Flight

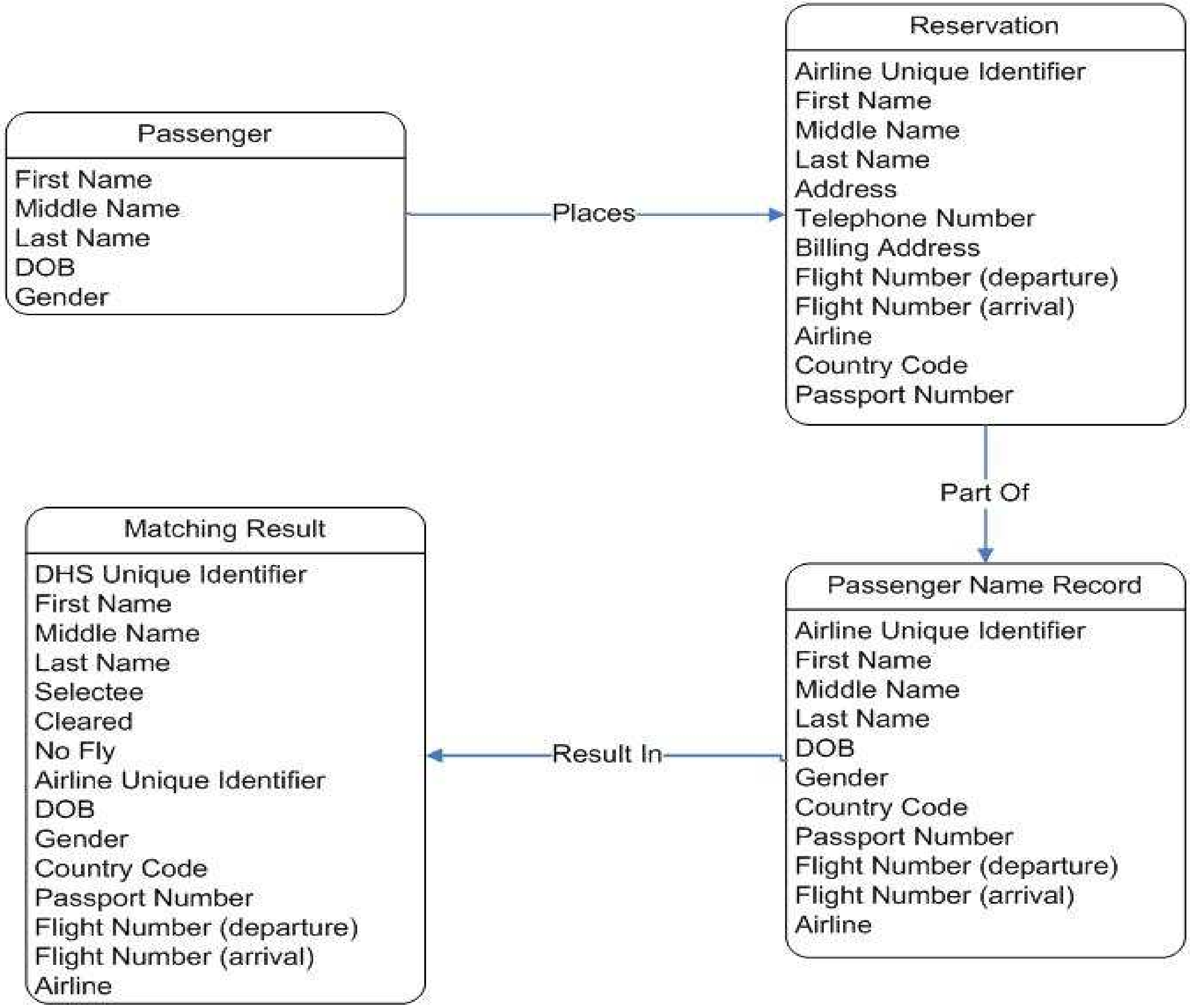
Figure 3.0 Department of Homeland Security – "As-Is" Secure Flight Systems Connection Model



- Systems nodes align with the business nodes as shown in the "As-Is" Business Connectivity Model
- System interfaces align with the needlines as shown in the "As-Is" Business Connectivity Model

DHS – Secure Flight

Figure 5.0 Department of Homeland Security – "As-Is" Secure Flight Logical Data Model



Reservation

Airline Unique Identifier
First Name
Middle Name
Last Name
Address
Telephone Number
Billing Address
Flight Number (departure)
Flight Number (arrival)
Airline
Country Code
Passport Number

Passenger

First Name
Middle Name
Last Name
DOB
Gender

Places

Part Of

Matching Result

DHS Unique Identifier
First Name
Middle Name
Last Name
Selectee
Cleared
No Fly
Airline Unique Identifier
DOB
Gender
Country Code
Passport Number
Flight Number (departure)
Flight Number (arrival)
Airline

Passenger Name Record

Airline Unique Identifier
First Name
Middle Name
Last Name
DOB
Gender
Country Code
Passport Number
Flight Number (departure)
Flight Number (arrival)
Airline

Result In

DHS – ICE/DRO

U.S. Customs and Border Protection

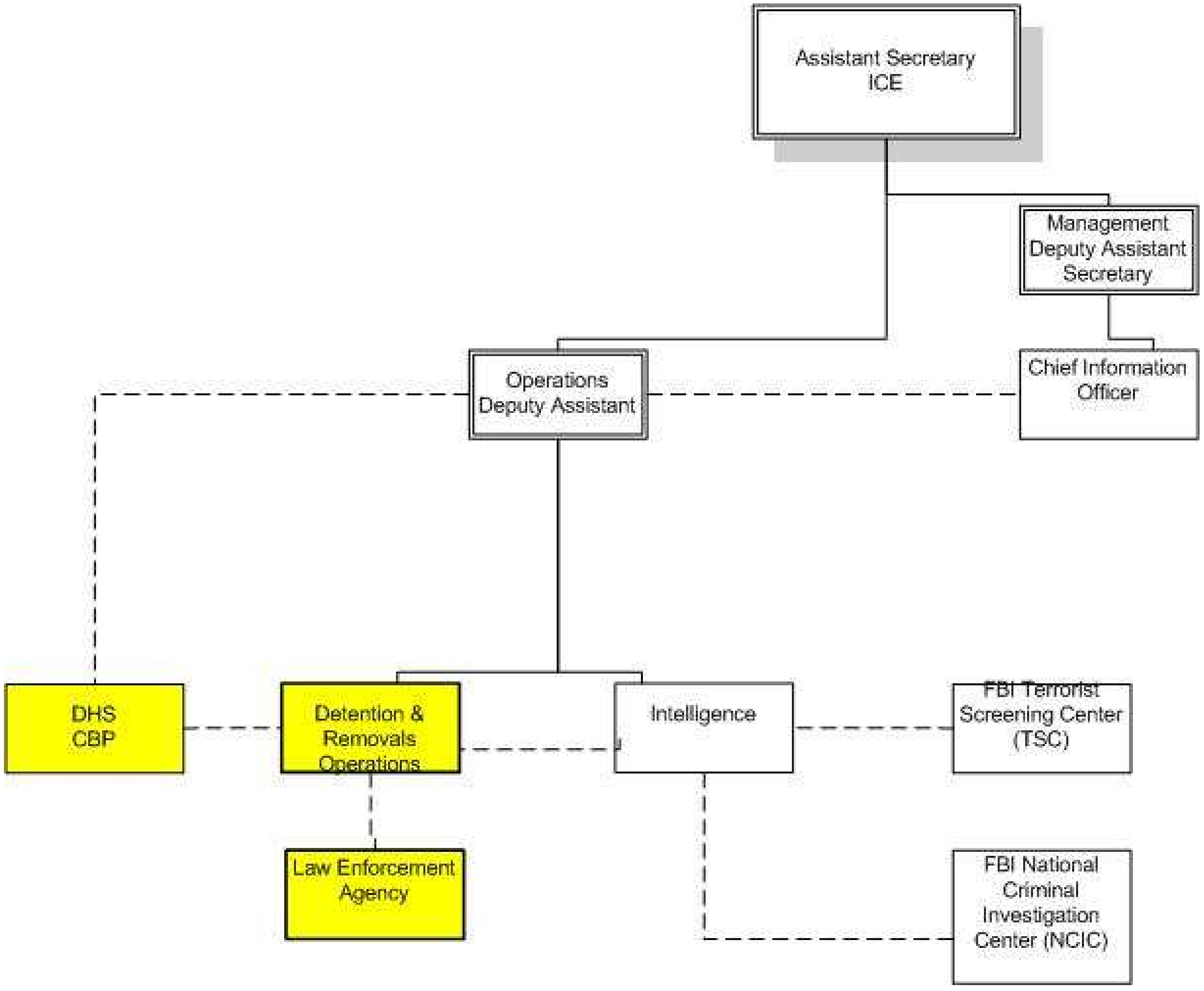
U.S. Citizenship and Immigration Services

Foreign Governments

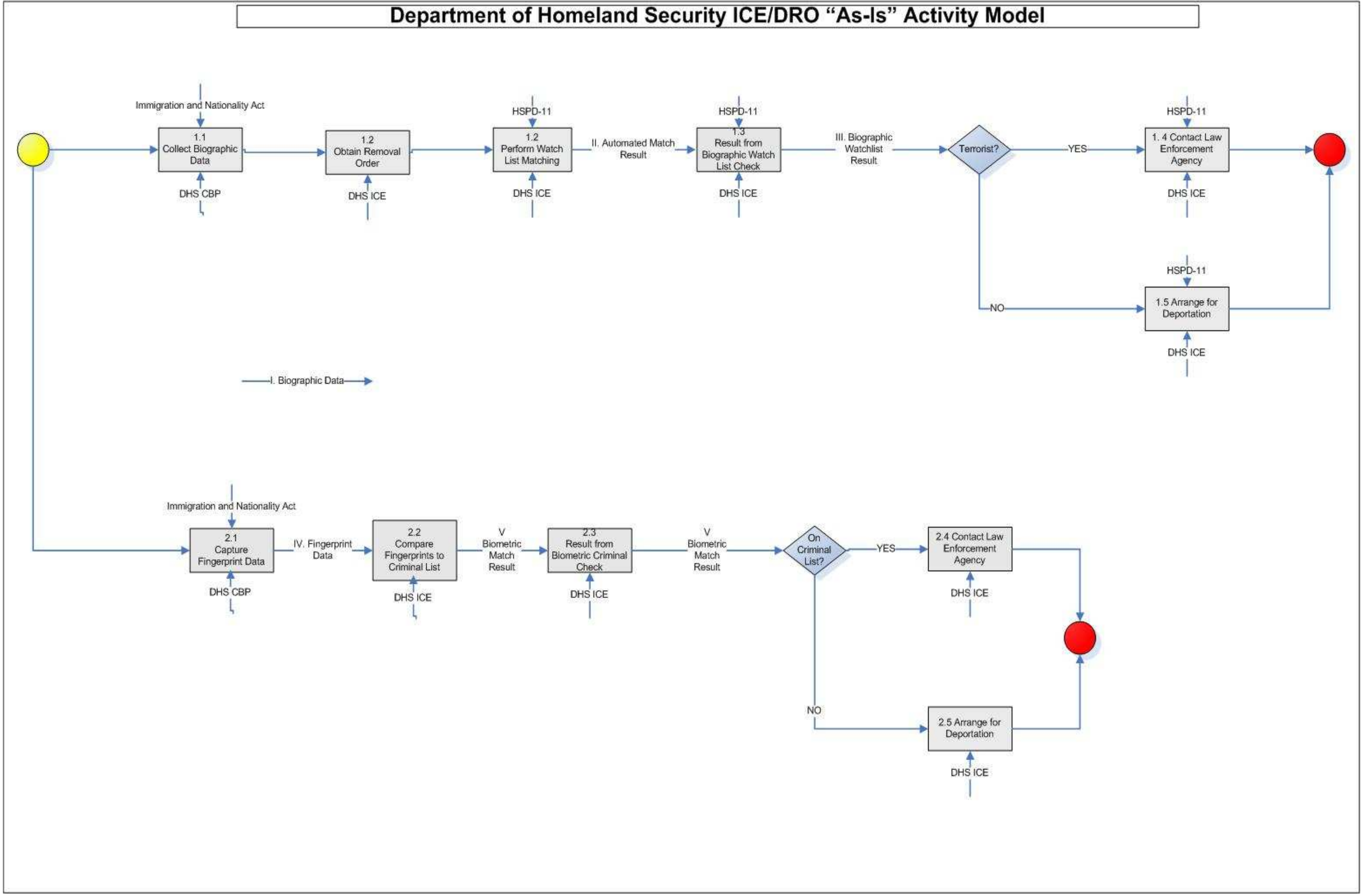
U.S. Immigration and Customs Enforcement

State & Local Governments

DHS – ICE/DRO


Assistant Secretary
ICE
Management
Deputy Assistant
Secretary
Operations
Deputy Assistant
Chief Information
Officer
DHS
CBP
Detention &
Removals
Operations
Intelligence
FBI Terrorist
Screening Center
(TSC)
Law Enforcement
Agency
FBI National
Criminal
Investigation
Center (NCIC)

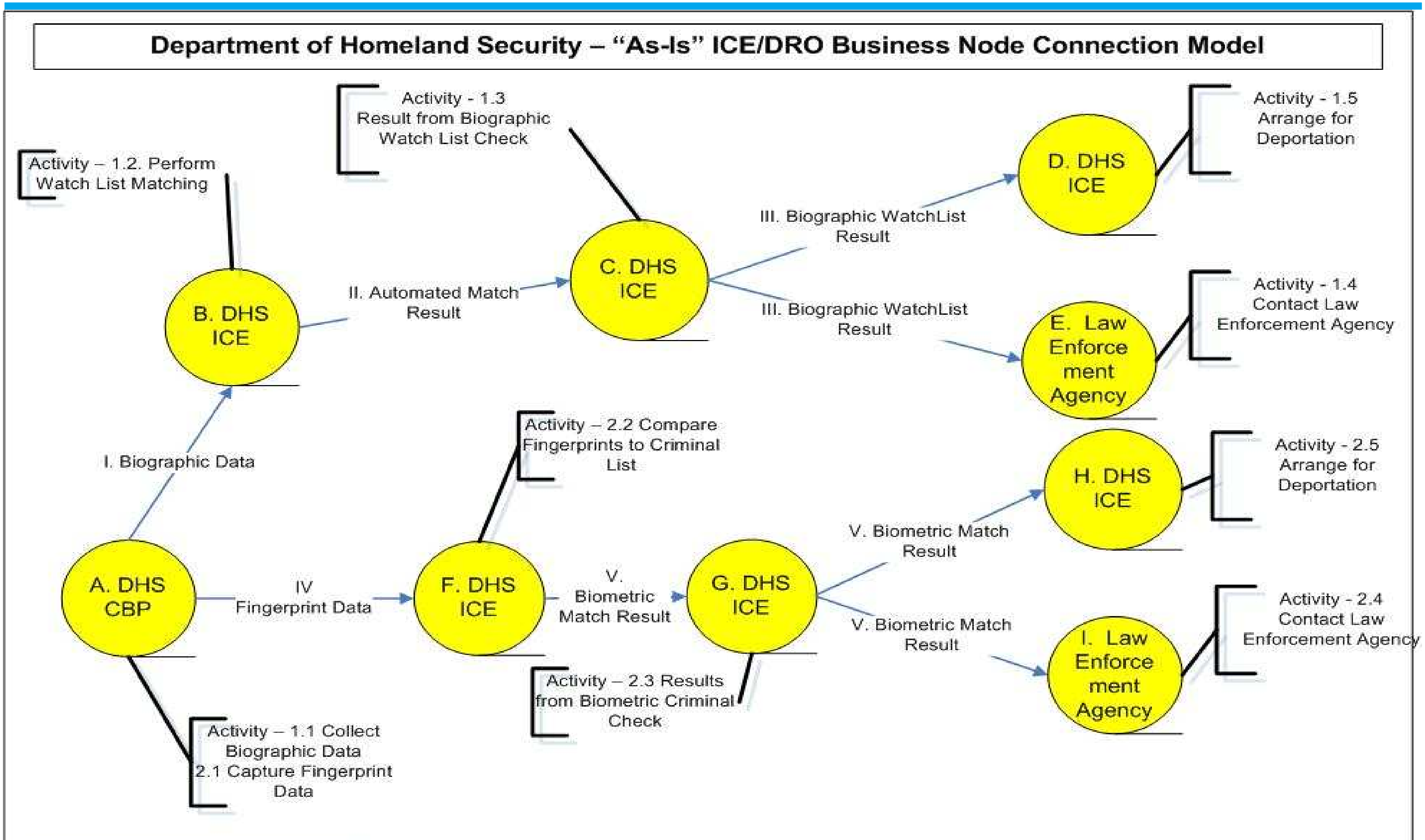
DHS – ICE/DRO



Department of Homeland Security ICE/DRO “As-Is” Activity Model

Immigration and Nationality Act
1.1 Collect Biographic Data
DHS CBP
1.2 Obtain Removal Order
DHS ICE
HSPD-11
1.2 Perform Watch List Matching
DHS ICE
II. Automated Match Result
HSPD-11
1.3 Result from Biographic Watch List Check
DHS ICE
III. Biographic Watchlist Result
Terrorist?
YES
NO
HSPD-11
1. 4 Contact Law Enforcement Agency
DHS ICE
HSPD-11
1.5 Arrange for Deportation
DHS ICE
I. Biographic Data
Immigration and Nationality Act
2.1 Capture Fingerprint Data
DHS CBP
IV. Fingerprint Data
2.2 Compare Fingerprints to Criminal List
DHS ICE
V Biometric Match Result
2.3 Result from Biometric Criminal Check
DHS ICE
V Biometric Match Result
On Criminal List?
YES
NO
2.4 Contact Law Enforcement Agency
DHS ICE
2.5 Arrange for Deportation
DHS ICE

DHS – ICE/DRO



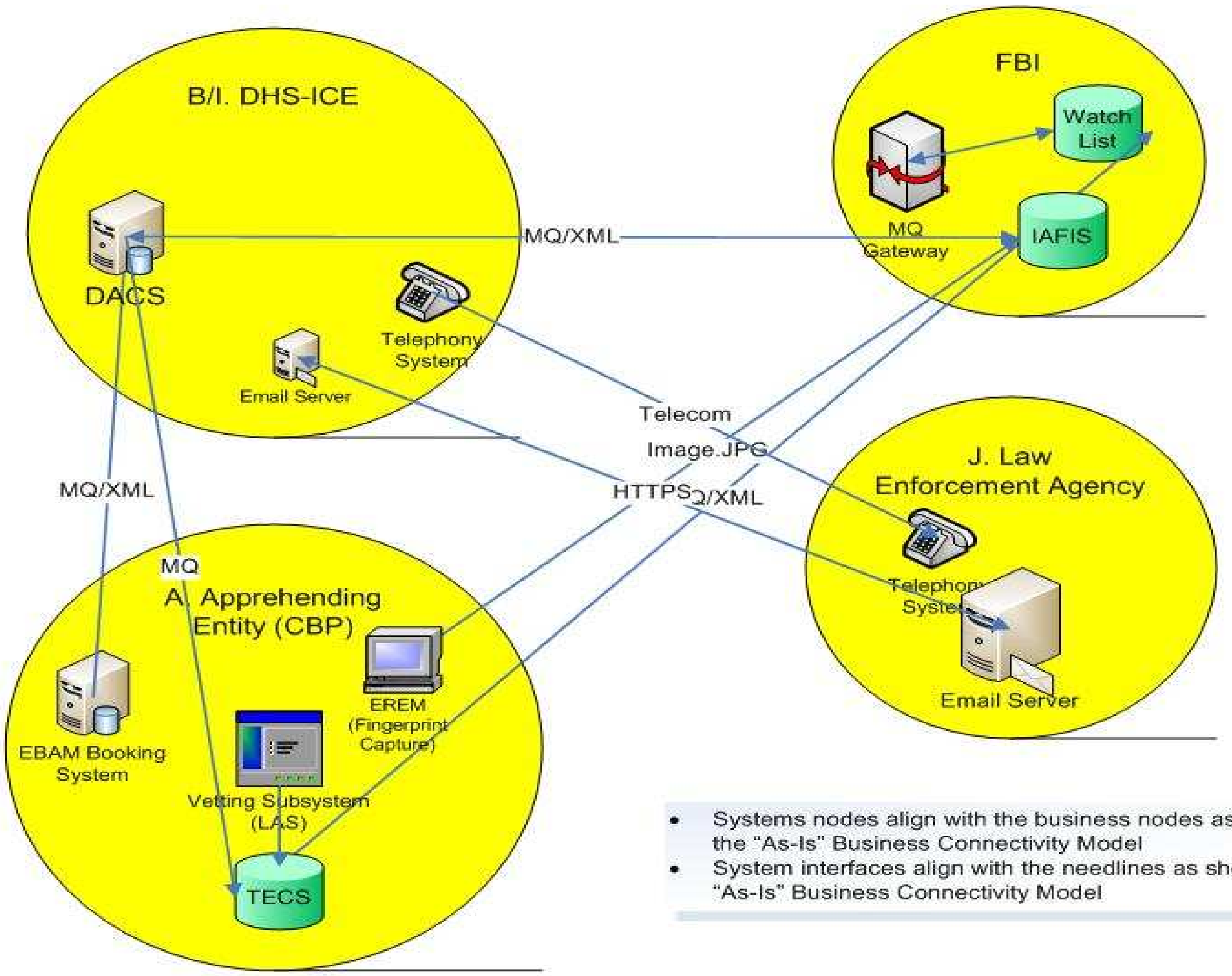
Department of Homeland Security – "As-Is" ICE/DRO Business Node Connection Model

A. DHS CBP
B. DHS ICE
C. DHS ICE
D. DHS ICE
E. Law Enforce ment Agency
F. DHS ICE
G. DHS ICE
H. DHS ICE
I. Law Enforce ment Agency
I. Biographic Data
II. Automated Match Result
III. Biographic WatchList Result
III. Biographic WatchList Result
IV Fingerprint Data
V. Biometric Match Result
V. Biometric Match Result
V. Biometric Match Result
Activity – 1.1 Collect Biographic Data 2.1 Capture Fingerprint Data
Activity – 1.2. Perform Watch List Matching
Activity - 1.3 Result from Biographic Watch List Check
Activity - 1.4 Contact Law Enforcement Agency
Activity - 1.5 Arrange for Deportation
Activity – 2.2 Compare Fingerprints to Criminal List
Activity – 2.3 Results from Biometric Criminal Check
Activity - 2.4 Contact Law Enforcement Agency
Activity - 2.5 Arrange for Deportation

- Activities align with the activities as shown in the "As-Is" Activity Model
- Information provided in the needlines align with the activities as shown in the "As-Is" Activity Model

DHS – ICE/DRO

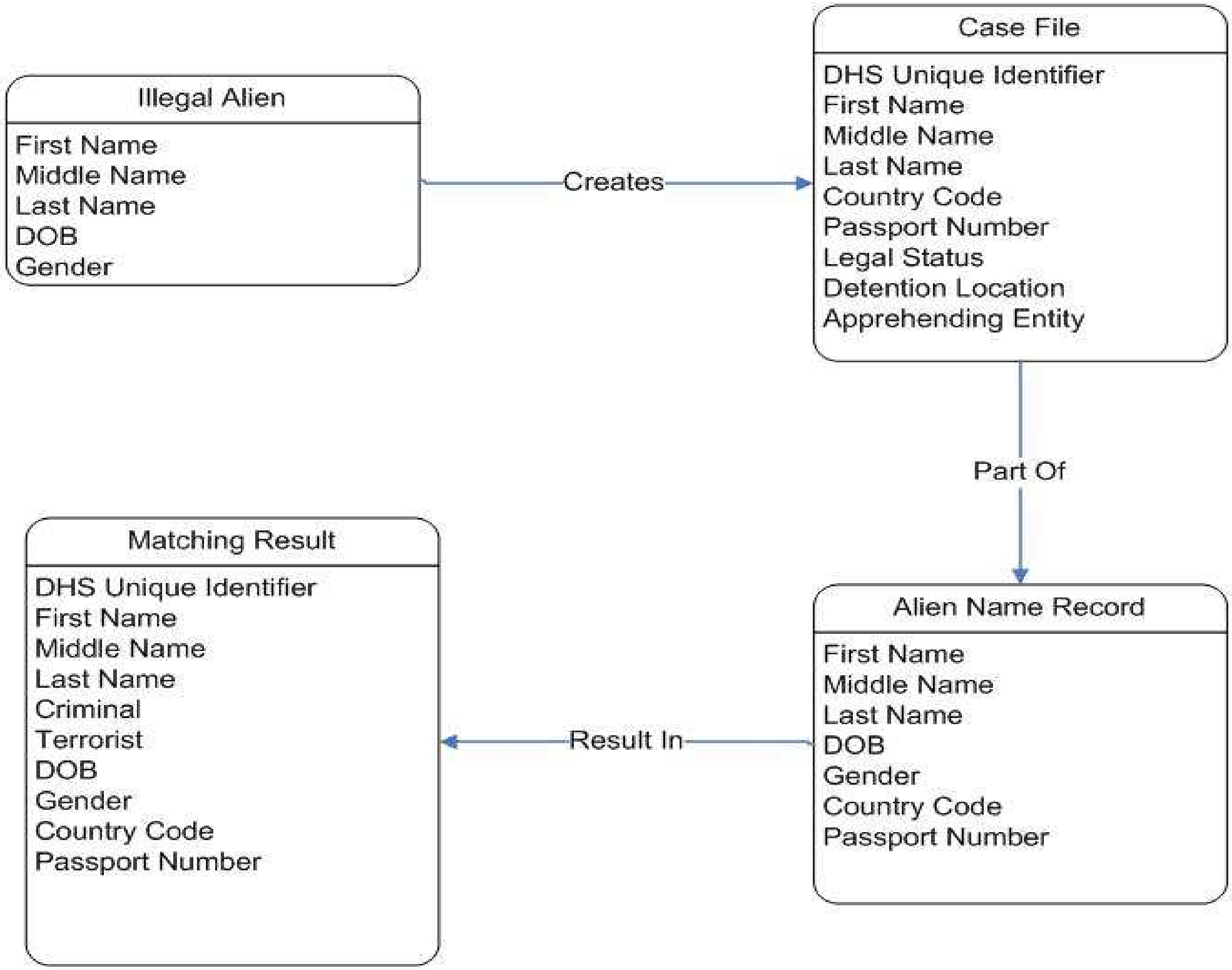
Department of Homeland Security – "As-Is" ICE/DRO Systems Connection Model



- Systems nodes align with the business nodes as shown in the "As-Is" Business Connectivity Model
- System interfaces align with the needlines as shown in the "As-Is" Business Connectivity Model

DHS – ICE/DRO

Department of Homeland Security – "As-Is" ICE/DRO Logical Data Model



Illegal Alien

First Name
Middle Name
Last Name
DOB
Gender

Creates

Case File

DHS Unique Identifier
First Name
Middle Name
Last Name
Country Code
Passport Number
Legal Status
Detention Location
Apprehending Entity

Part Of

Alien Name Record

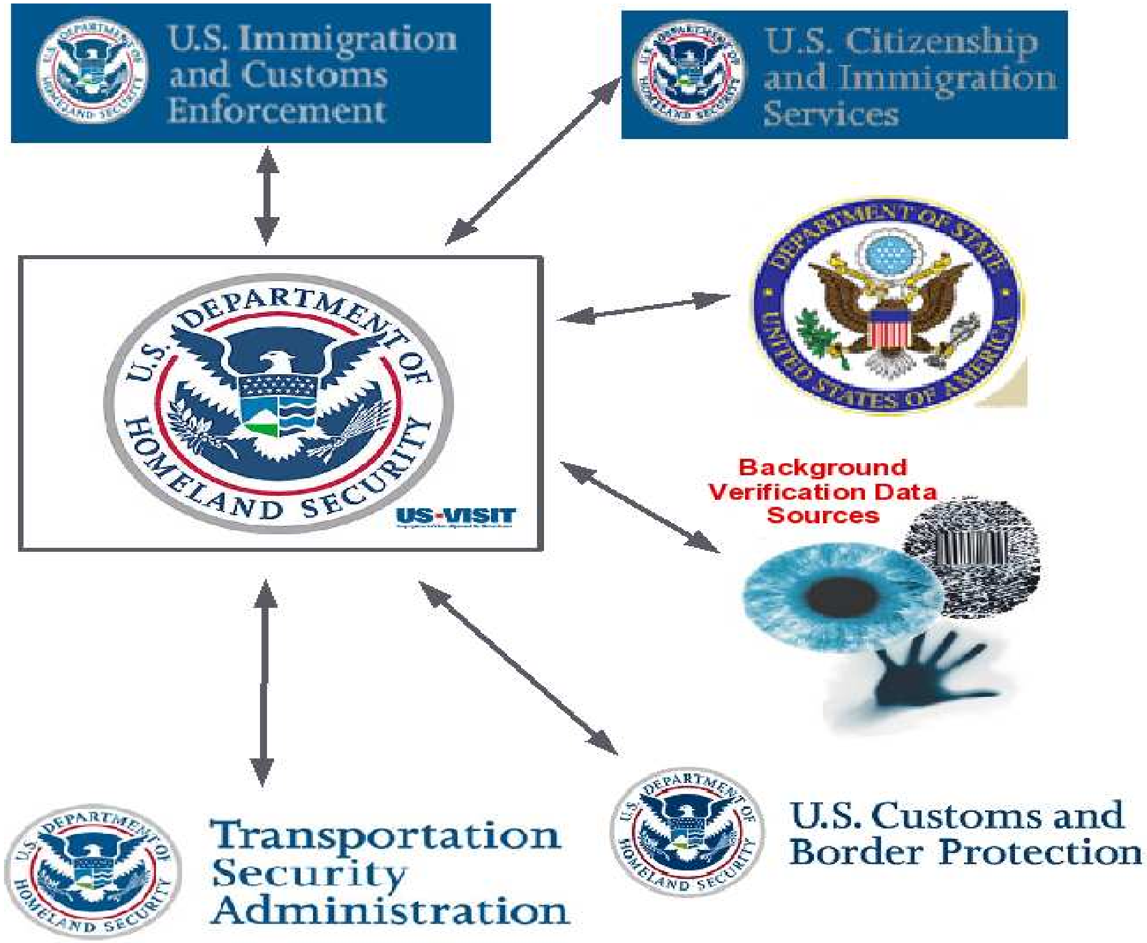
First Name
Middle Name
Last Name
DOB
Gender
Country Code
Passport Number

Result In

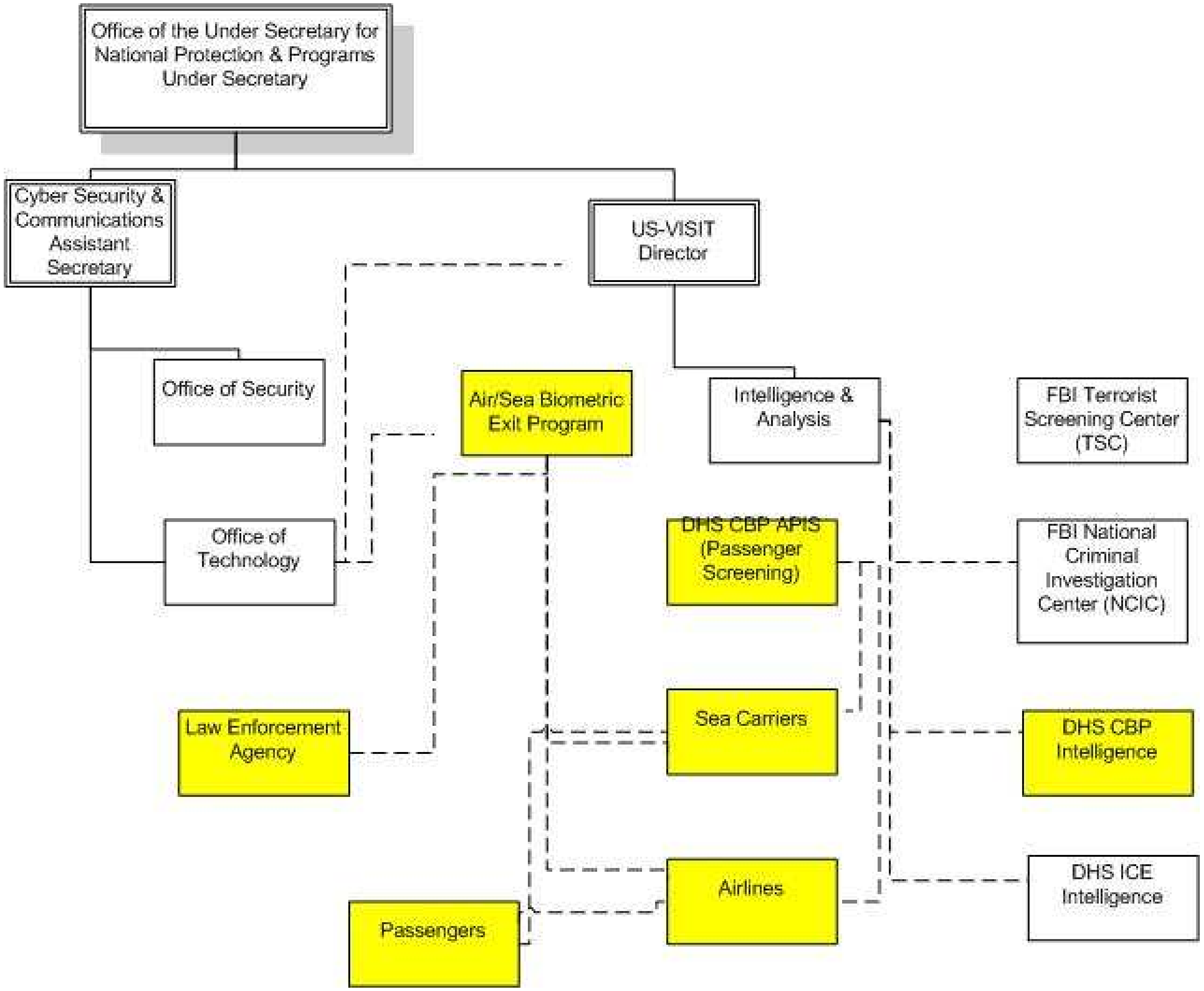
Matching Result

DHS Unique Identifier
First Name
Middle Name
Last Name
Criminal
Terrorist
DOB
Gender
Country Code
Passport Number

DHS – USVISIT

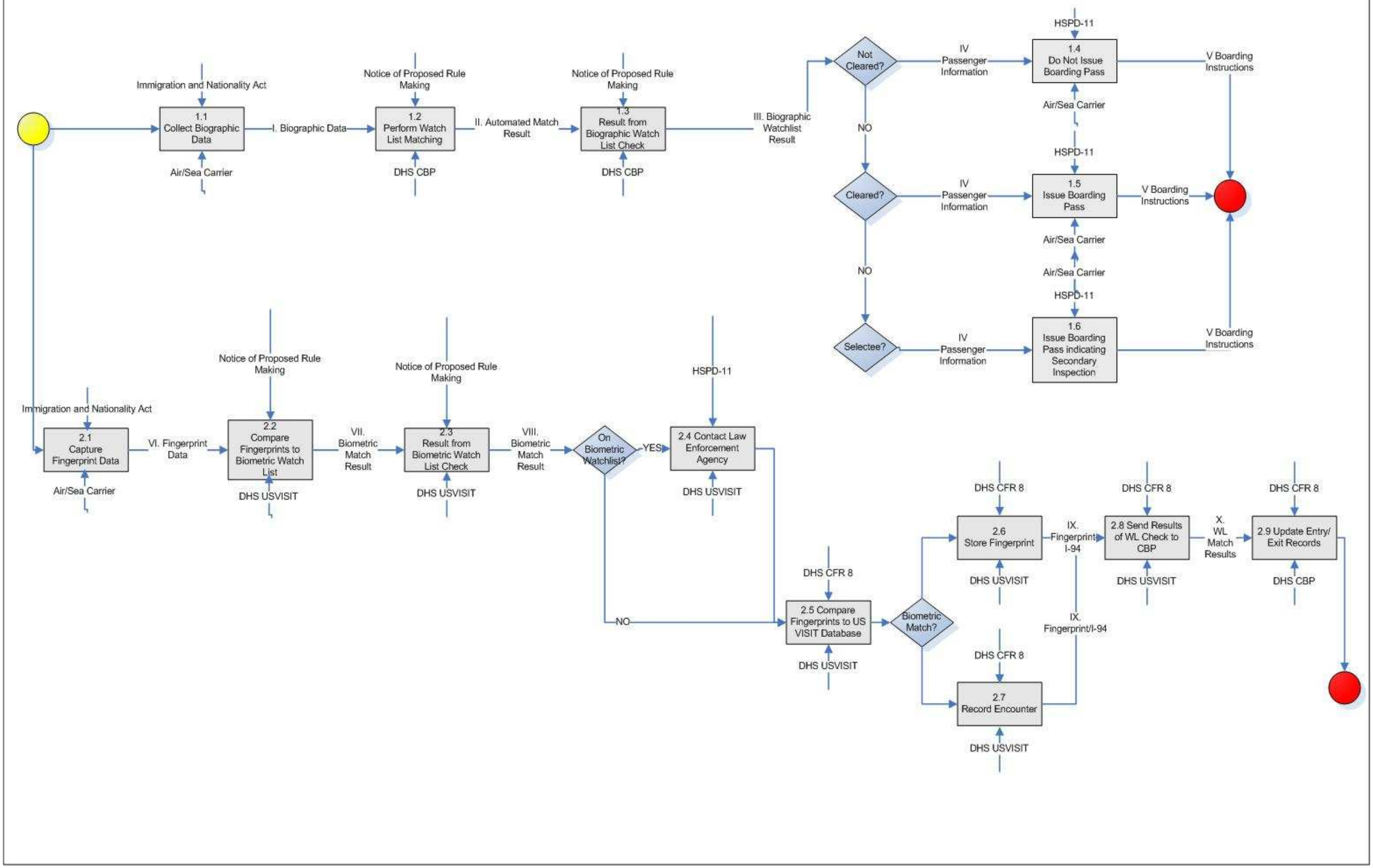

U.S. Immigration and Customs Enforcement
U.S. Citizenship and Immigration Services
U.S. DEPARTMENT OF HOMELAND SECURITY
US-VISIT
DEPARTMENT OF STATE UNITED STATES OF AMERICA
Background Verification Data Sources
Transportation Security Administration
U.S. Customs and Border Protection

DHS – USVISIT


Office of the Under Secretary for National Protection & Programs Under Secretary
Cyber Security & Communications Assistant Secretary
US-VISIT Director
Office of Security
Air/Sea Biometric Exit Program
Intelligence & Analysis
FBI Terrorist Screening Center (TSC)
Office of Technology
DHS CBP APIS (Passenger Screening)
FBI National Criminal Investigation Center (NCIC)
Law Enforcement Agency
Sea Carriers
DHS CBP Intelligence
Airlines
DHS ICE Intelligence
Passengers

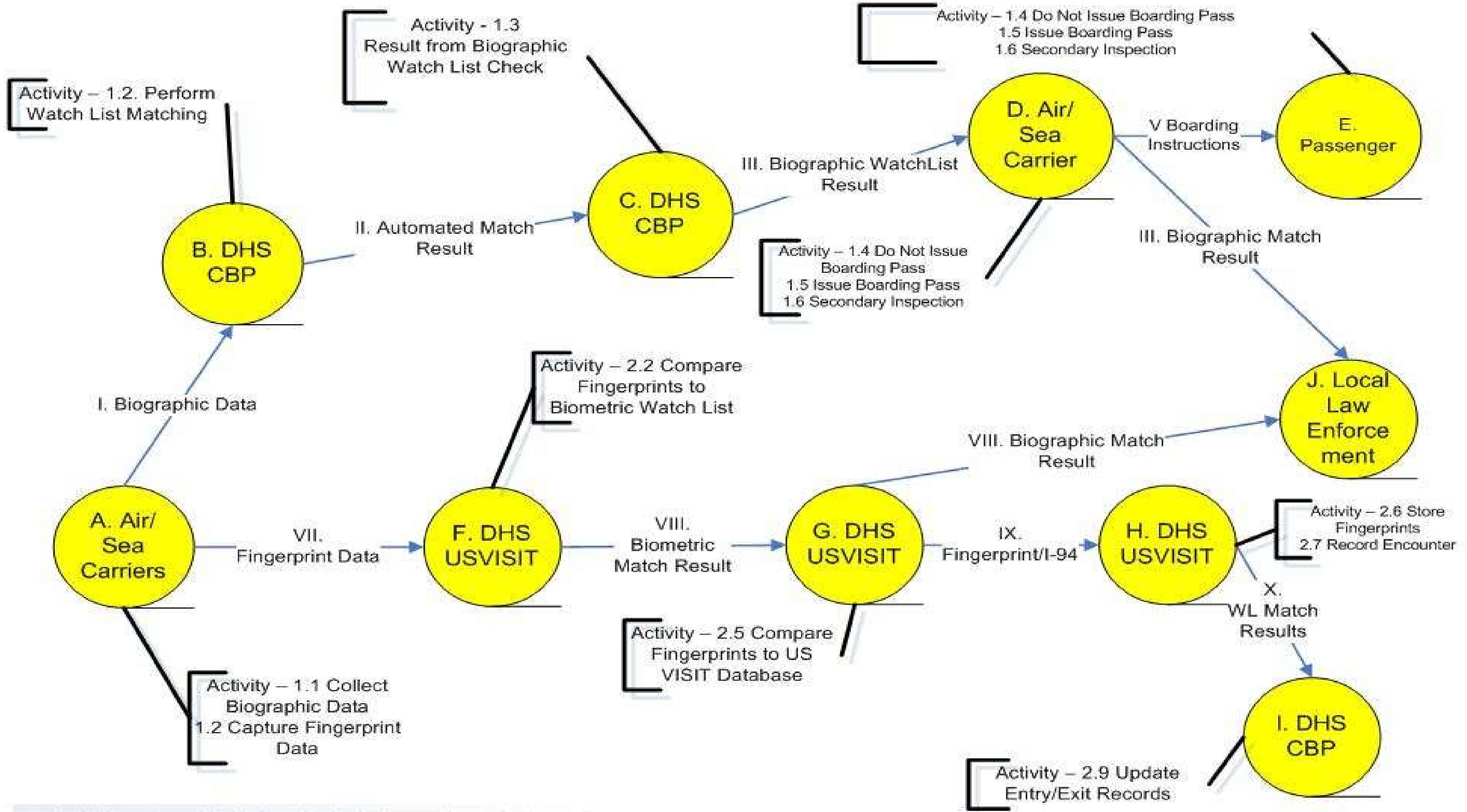
DHS – USVISIT

Figure 6.0 Department of Homeland Security US VISIT Air/Sea Biometric Exit“As-Is” Activity Model


Immigration and Nationality Act
1.1 Collect Biographic Data
Air/Sea Carrier
I. Biographic Data
Notice of Proposed Rule Making
1.2 Perform Watch List Matching
DHS CBP
II. Automated Match Result
Notice of Proposed Rule Making
1.3 Result from Biographic Watch List Check
DHS CBP
III. Biographic Watchlist Result
Not Cleared?
NO
Cleared?
NO
Selectee?
IV Passenger Information
IV Passenger Information
IV Passenger Information
HSPD-11
1.4 Do Not Issue Boarding Pass
Air/Sea Carrier
HSPD-11
1.5 Issue Boarding Pass
Air/Sea Carrier
Air/Sea Carrier
HSPD-11
1.6 Issue Boarding Pass indicating Secondary Inspection
V Boarding Instructions
V Boarding Instructions
V Boarding Instructions
Immigration and Nationality Act
2.1 Capture Fingerprint Data
Air/Sea Carrier
VI. Fingerprint Data
Notice of Proposed Rule Making
2.2 Compare Fingerprints to Biometric Watch List
DHS USVISIT
VII. Biometric Match Result
Notice of Proposed Rule Making
2.3 Result from Biometric Watch List Check
DHS USVISIT
VIII. Biometric Match Result
On Biometric Watchlist?
YES
NO
HSPD-11
2.4 Contact Law Enforcement Agency
DHS USVISIT
DHS CFR 8
2.5 Compare Fingerprints to US VISIT Database
DHS USVISIT
Biometric Match?
DHS CFR 8
2.6 Store Fingerprint
DHS USVISIT
IX. Fingerprint I-94
DHS CFR 8
2.7 Record Encounter
DHS USVISIT
IX. Fingerprint/I-94
DHS CFR 8
2.8 Send Results of WL Check to CBP
DHS USVISIT
X. WL Match Results
DHS CFR 8
2.9 Update Entry/ Exit Records
DHS CBP

DHS – USVISIT

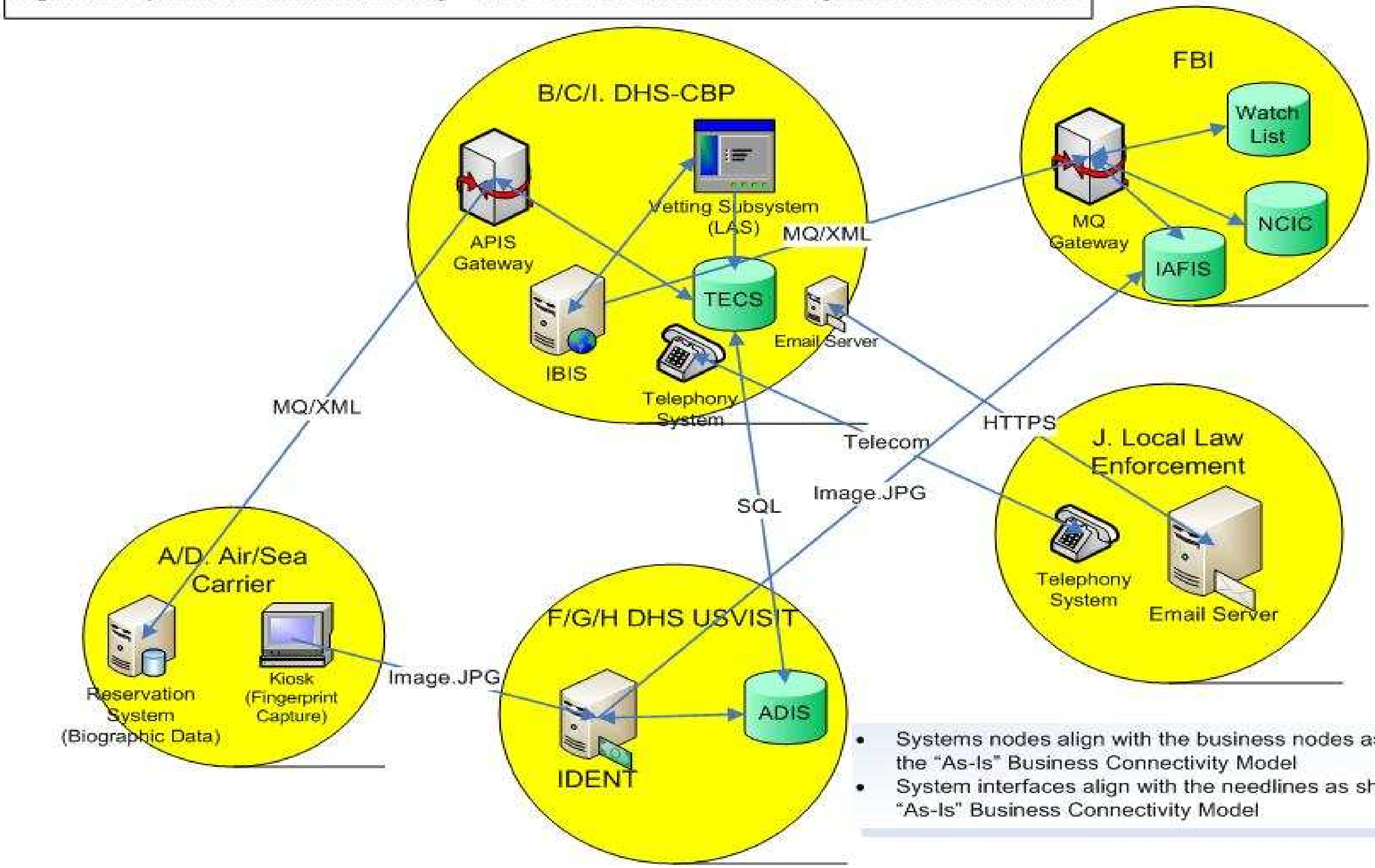
Figure 7.0 Department of Homeland Security – "As-Is" USVISIT Air/Sea Biometric Business Node Connection Model


A. Air/ Sea Carriers
B. DHS CBP
C. DHS CBP
D. Air/ Sea Carrier
E. Passenger
F. DHS USVISIT
G. DHS USVISIT
H. DHS USVISIT
I. DHS CBP
J. Local Law Enforcement
I. Biographic Data
II. Automated Match Result
III. Biographic WatchList Result
V Boarding Instructions
III. Biographic Match Result
VII. Fingerprint Data
VIII. Biometric Match Result
VIII. Biographic Match Result
IX. Fingerprint/I-94
X. WL Match Results
Activity – 1.2. Perform Watch List Matching
Activity - 1.3 Result from Biographic Watch List Check
Activity – 1.4 Do Not Issue Boarding Pass 1.5 Issue Boarding Pass 1.6 Secondary Inspection
Activity – 1.4 Do Not Issue Boarding Pass 1.5 Issue Boarding Pass 1.6 Secondary Inspection
Activity – 2.2 Compare Fingerprints to Biometric Watch List
Activity – 1.1 Collect Biographic Data 1.2 Capture Fingerprint Data
Activity – 2.5 Compare Fingerprints to US VISIT Database
Activity – 2.6 Store Fingerprints 2.7 Record Encounter
Activity – 2.9 Update Entry/Exit Records

- Activities align with the Level I depiction as shown in the "As-Is" Activity Model
- Information provided in the needlines align with the Level I depiction as shown in the "As-Is" Activity Model

DHS – USVISIT

Figure 8.0 Department of Homeland Security – "As-Is" USVISIT Air/Sea Biometric Systems Connection Model



- Systems nodes align with the business nodes as shown in the "As-Is" Business Connectivity Model
- System interfaces align with the needlines as shown in the "As-Is" Business Connectivity Model

DHS – USVISIT

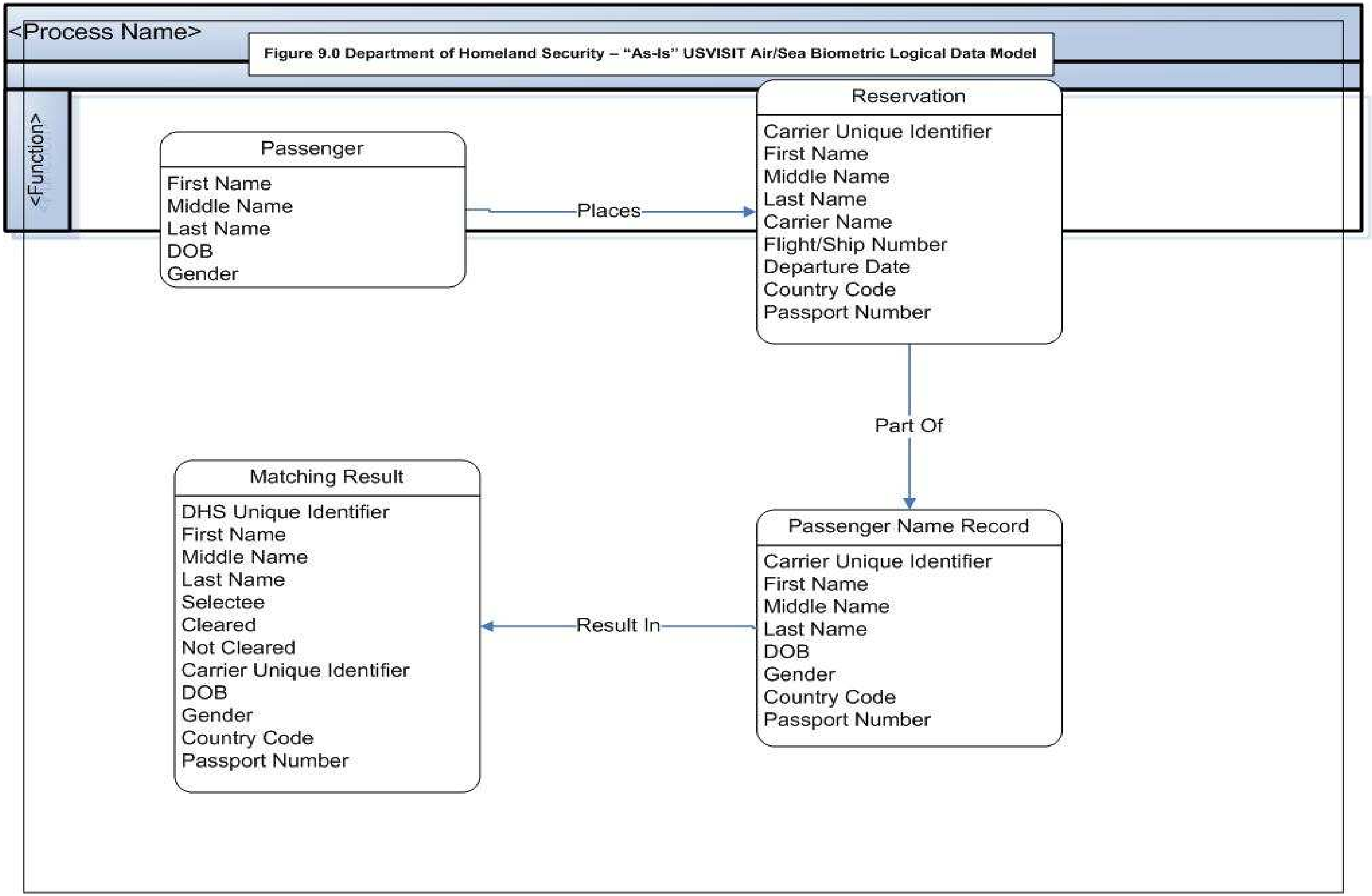
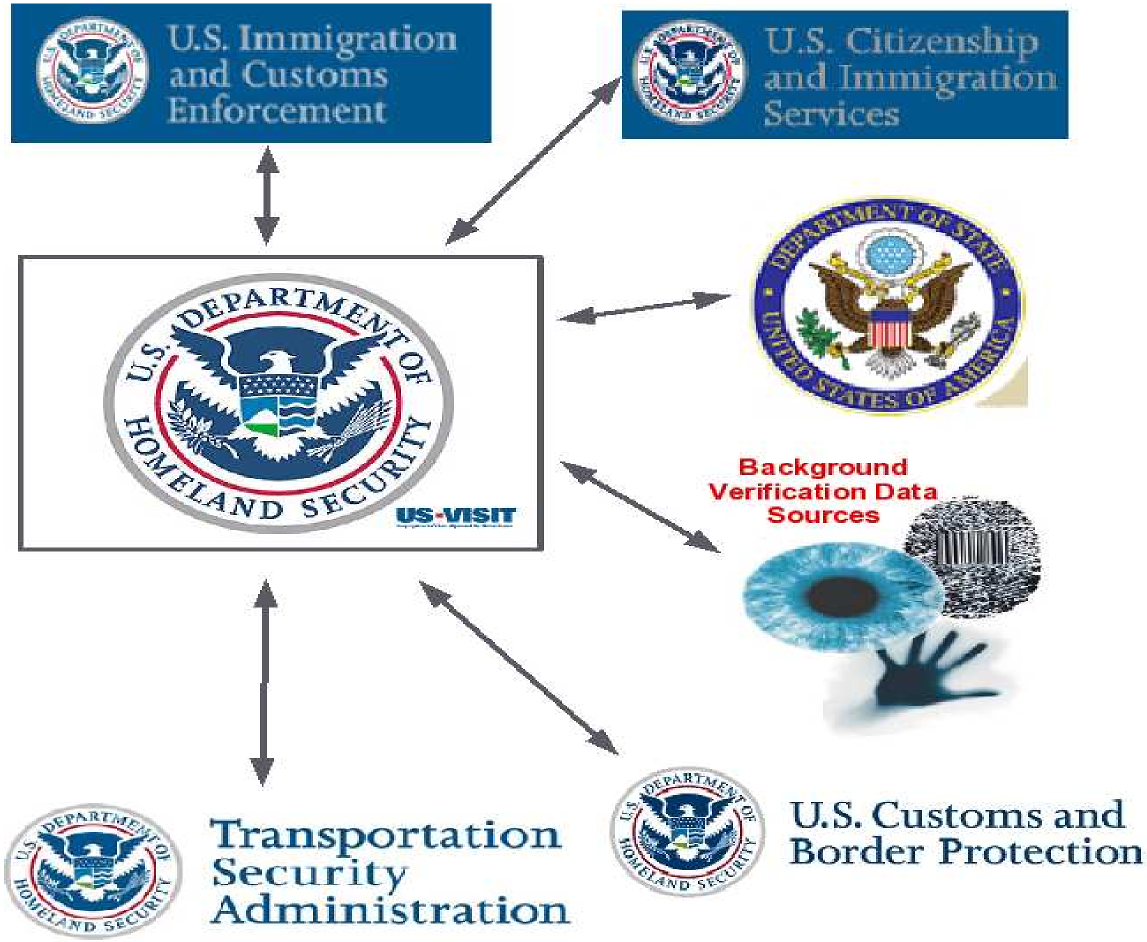


Figure 9.0 Department of Homeland Security – "As-Is" USVISIT Air/Sea Biometric Logical Data Model

DHS – HSPD12


U.S. Immigration and Customs Enforcement
U.S. Citizenship and Immigration Services
DEPARTMENT OF STATE
UNITED STATES OF AMERICA
U.S. DEPARTMENT OF HOMELAND SECURITY
US-VISIT
Background Verification Data Sources
Transportation Security Administration
U.S. Customs and Border Protection

U.S. DEPARTMENT OF HOMELAND SECURITY