U.S. Department of Homeland Security

DHS Biometrics Strategic Framework

2015 – 2025

Version 1.0

June 9, 2015

Prepared by the IBSV Biometrics Sub-Team

Contents

1 INTRODUCTION

1.1 Purpose

The purpose of this document, consistent with the Department of Homeland Security's (DHS) Unity of Effort initiative, is to establish the overarching vision for how enhanced biometrics capabilities will transform DHS mission operations over the next ten years. Unity of Effort as a Department imperative serves to drive advancement of biometric strategies, resource allocations, and capability requirements to meet future challenges through integrated capabilities, services and data sharing in order to operate with increased effectiveness, cohesiveness and efficiency. A unified set of biometric capabilities must support and enable DHS's vision of a homeland that is safe, secure, and resilient against terrorism and other hazards. DHS requires a strategic framework that supports operational efficiency and cost effectiveness for biometrics operations across the Department, such as interoperability and enterprise services for joint mission needs.

A biometric is a measurable physical characteristic or personal behavior trait used to recognize the identity or verify the claimed identity of an individual. The most common biometrics in use in the security market today include fingerprints, facial image, or iris scans. Biometrics technology is a support capability used to assist DHS in attaining its mission goals and objectives. The collection or use of biometric technology is not an end in itself, nor does it replace the underlying missions of DHS and its Operational Components. Whether biometrics are used or not, the missions do not change. This strategic framework identifies common goals and objectives that support multiple missions across DHS.

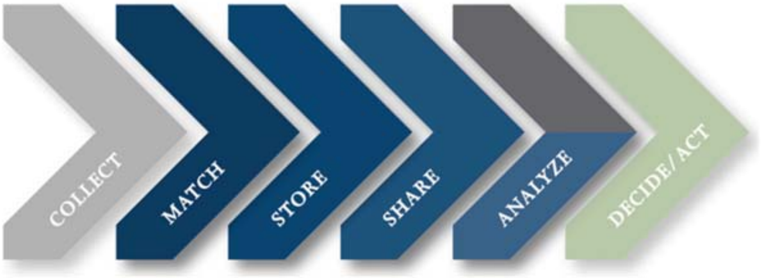
Although DHS has lacked an overarching biometrics strategy to date, activities to advance DHS biometrics capabilities are underway, such as the planning for the re-architecture of the DHS Automated Biometrics Identification System (IDENT), research and development activities within the DHS Science and Technology Directorate (S&T), and various biometrics initiatives being implemented by DHS Operational Components. The DHS Biometrics Strategic framework will be used to identify and align DHS initiatives to meet strategic goals and objectives, as well as identify gaps where action plans must be initiated.

1.2 Context

The use of biometric technology complements associated capabilities, such as biographics and forensics, as an important element of a broader suite of identity-related capabilities. At DHS, establishing, or verifying, an individual's identity through biometrics enables operational front line decisions – whether to determine if services or privileges should be granted, or ascertain if an individual is a threat.

As shown in Figure 1 below, the overall DHS biometric process can be represented as a continuum spanning the collection of biometrics; the matching, storing, and sharing of those biometrics; analysis to confirm biometric match results or review additional associated information; and ultimately, a decision or action taken by a DHS decision maker about an individual.

Figure 1. The DHS Biometric Continuum



The scope of this framework document is the entire DHS Biometric continuum, supporting the Department's five homeland security missions as defined in the 2014 Quadrennial Homeland Security Report and the DHS 2014-2018 Strategic Plan.

1.3 Background

In June 2014, the Secretary of Homeland Security directed the creation of the DHS Joint Requirements Council (JRC) to further the DHS Unity of Effort. The DHS Office of Biometrics and Identity Management (OBIM), DHS Policy Screening and Coordination Office (SCO), DHS Components and other DHS stakeholders have worked collaboratively since the issuance of DHS 2016 Resource Planning Guidance in August 2014 and the establishment of the JRC Information-Based Screening and Vetting (IBSV) Portfolio Team in December 2014 to examine cross-component needs for biometrics capabilities. Although efforts to advance biometrics capabilities across the department are underway, the lack of an integrated biometrics strategy was apparent.

Through the establishment of the JRC IBSV Biometrics Sub Team in late February 2015, biometrics program subject matter experts (SMEs) from each DHS component have been brought together in a forum to share information and identify joint requirements. Chaired by Customs and Border Protection (CBP) and US Citizenship and Immigration Services (USCIS), the Biometrics Sub-Team has been focused to date on sharing information about DHS component plans and needs and validating key foundational documents such as the Joint Biometrics Preliminary Mission Need Statement (P-MNS) and the OBIM Replacement Biometrics System MNS. Through these documents, artifacts and DHS Component needs briefings, the IBSV Biometrics Sub team developed the DHS Biometrics Strategic Framework.

2 CURRENT ENVIRONMENT

2.1 Strategic Trends and Drivers

High level, long term trends with implications that will likely impact and shape DHS biometric applications and other identity technologies may include a diffusion of power among countries, individual empowerment and formation of informal networks connected by current and new technologies, plus global population and demographic shifts. [1]

The DHS 2014 Quadrennial Homeland Security Review (QHSR) further highlights key findings in the strategic environment The QHSR categorizes key prevailing strategic challenges that will drive risk over the next five years:

- An evolving terrorist threat with persistent targets in the transportation sector
- Growing cyber threats that increase risk to critical infrastructure and to the greater U.S. economy
- Biological concerns endure as a top homeland security risk (bioterrorism, pandemics, foreign animal diseases, agricultural concerns)
- Nuclear terrorism through an improvised nuclear device
- Transnational criminal organizations are increasing in strength and capability, driving risk in counterfeit goods, human trafficking, illicit drugs, illegal flows of people and goods
- Natural hazards with increasingly variable consequences
- General factors such as technology and population migrations

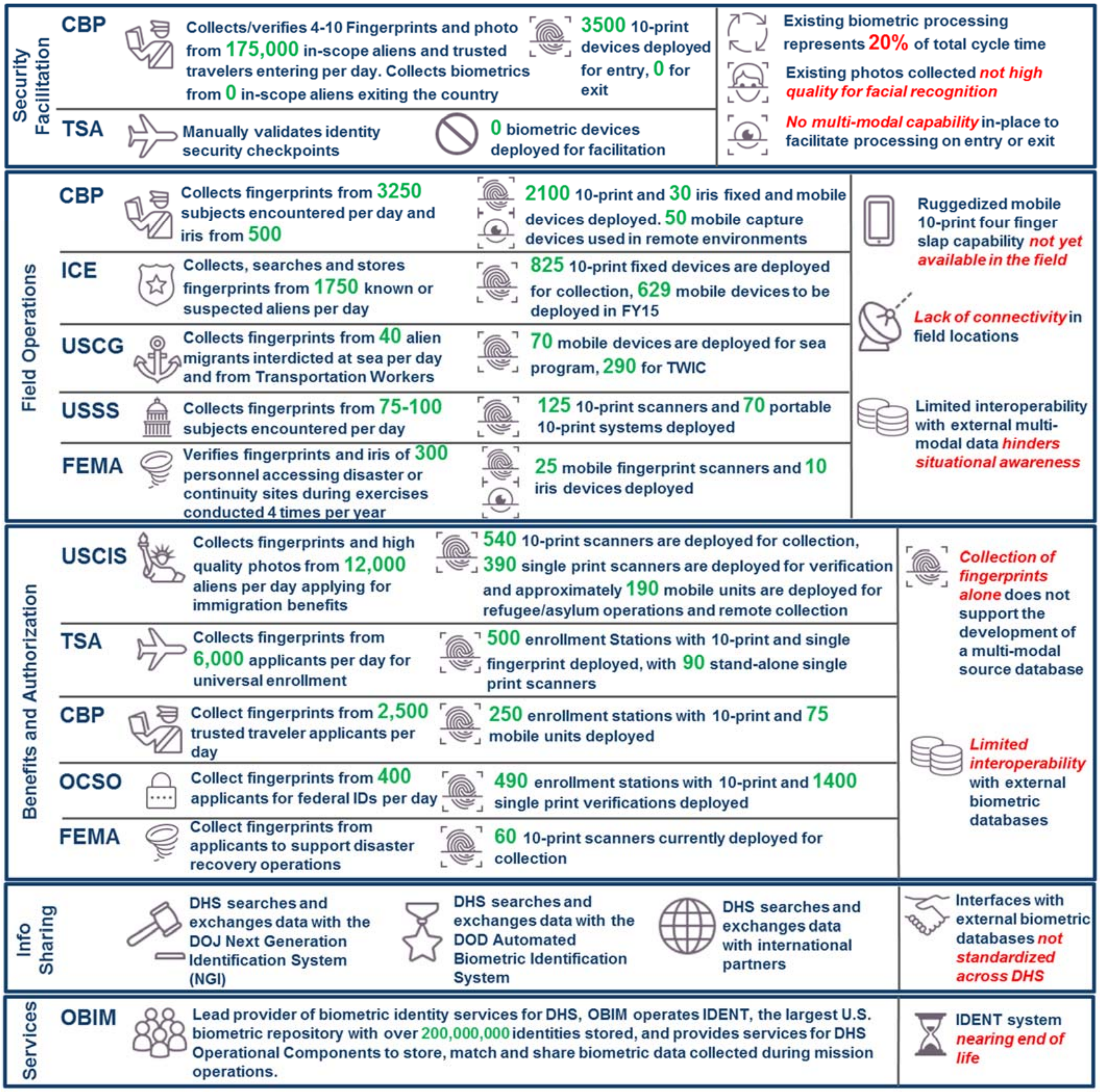
2.2 DHS Biometrics Baseline

The DHS Office of Biometrics and Identity Management (OBIM) operates and maintains the DHS Automated Biometric Identification System (IDENT) and provides identity management services and expertise across DHS. Front-end capabilities (i.e. biometric collection devices, applications, interfaces and supporting infrastructure) are each managed and maintained independently by the components, with limited collaboration. National Security Presidential Directive (NSPD)-59 / Homeland Security Presidential Directive (HSPD)-24 “Biometrics for Identification and Screening to Enhance National Security,” charges federal executive departments and agencies to use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric information. Access to external federal biometric databases however, through bilateral interoperability agreements, is not fully implemented, requiring DHS components to employ mission centric solutions for integrating certain biometric exchanges with the Federal Bureau of Investigation (FBI) and the Department of Defense (DoD). This requires DHS components to work independently with the FBI and DoD to integrate with each biometric system for access to data that assists in identifying and adjudicating subjects. The current IDENT system, although able to store multi-modal biometrics, offers matching capability for fingerprints only, limiting operational

[1] Global Trends 2030: Alternative Worlds, National Intelligence Council, 2012

components' ability to implement the use of alternate biometrics that may better suit operational needs. Current DHS Component systems tend to be encounter-based – instead of person-centric – requiring biometrics collection processes to be repeated, rather than just verified. Connectivity for systems that collect biometrics in the field is inconsistent, often not allowing real-time access to federal biometric databases. Further, existing biometric collection systems in the field are dated, many are at end-of-life, impacting the quality of the biometrics collected, which affects overall performance. Figure 2-1 summarizes biometrics capabilities across DHS today.

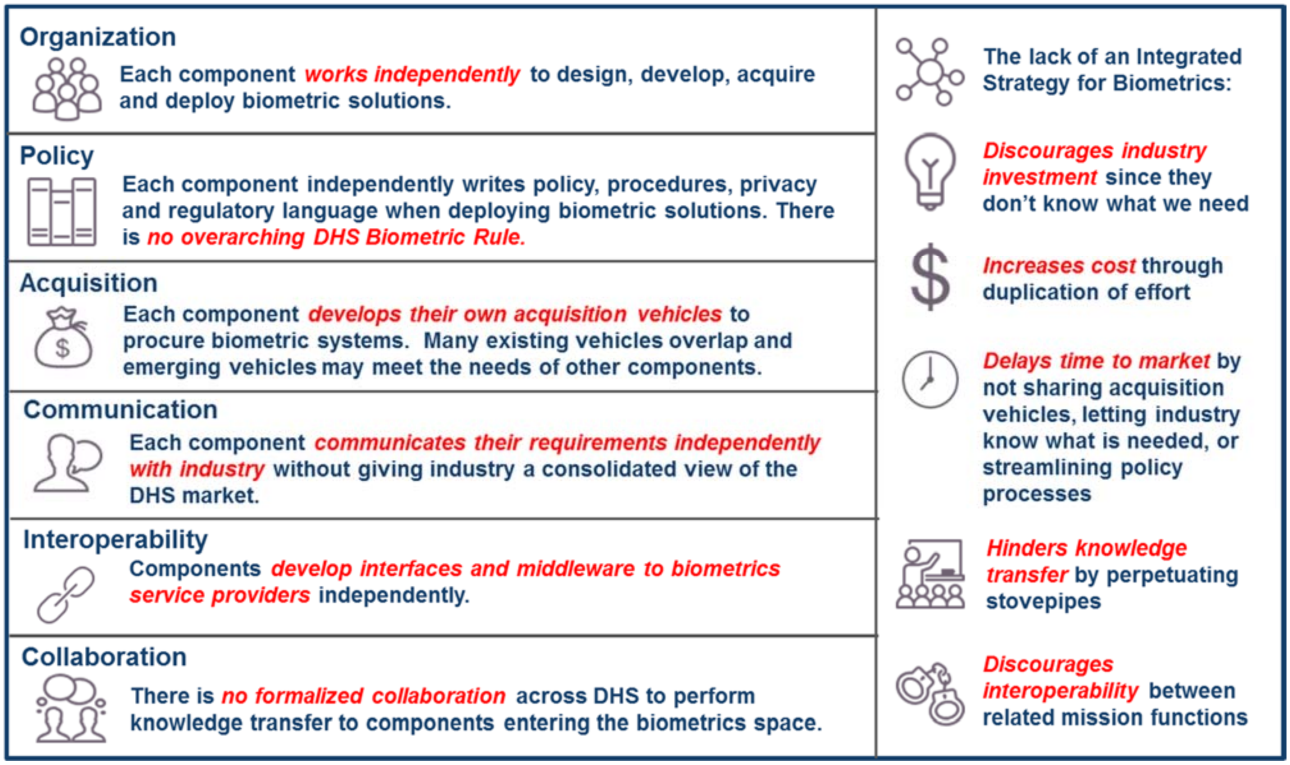
Figure 2-1, Current State Operational Snapshot



Security Facilitation	CBP	Collects/verifies 4-10 Fingerprints and photo from 175,000 in-scope aliens and trusted travelers entering per day. Collects biometrics from 0 in-scope aliens exiting the country	3500 10-print devices deployed for entry, 0 for exit	Existing biometric processing represents 20% of total cycle time Existing photos collected *not high quality for facial recognition* *No multi-modal capability* in-place to facilitate processing on entry or exit
	TSA	Manually validates identity security checkpoints	0 biometric devices deployed for facilitation	
Field Operations	CBP	Collects fingerprints from 3250 subjects encountered per day and iris from 500	2100 10-print and 30 iris fixed and mobile devices deployed. 50 mobile capture devices used in remote environments	Ruggedized mobile 10-print four finger slap capability *not yet available in the field* *Lack of connectivity* in field locations Limited interoperability with external multi-modal data *hinders situational awareness*
	ICE	Collects, searches and stores fingerprints from 1750 known or suspected aliens per day	825 10-print fixed devices are deployed for collection, 629 mobile devices to be deployed in FY15	
	USCG	Collects fingerprints from 40 alien migrants interdicted at sea per day and from Transportation Workers	70 mobile devices are deployed for sea program, 290 for TWIC	
	USSS	Collects fingerprints from 75-100 subjects encountered per day	125 10-print scanners and 70 portable 10-print systems deployed	
	FEMA	Verifies fingerprints and iris of 300 personnel accessing disaster or continuity sites during exercises conducted 4 times per year	25 mobile fingerprint scanners and 10 iris devices deployed	
Benefits and Authorization	USCIS	Collects fingerprints and high quality photos from 12,000 aliens per day applying for immigration benefits	540 10-print scanners are deployed for collection, 390 single print scanners are deployed for verification and approximately 190 mobile units are deployed for refugee/asylum operations and remote collection	*Collection of fingerprints alone* does not support the development of a multi-modal source database *Limited interoperability* with external biometric databases
	TSA	Collects fingerprints from 6,000 applicants per day for universal enrollment	500 enrollment Stations with 10-print and single fingerprint deployed, with 90 stand-alone single print scanners	
	CBP	Collect fingerprints from 2,500 trusted traveler applicants per day	250 enrollment stations with 10-print and 75 mobile units deployed	
	OCSO	Collect fingerprints from 400 applicants for federal IDs per day	490 enrollment stations with 10-print and 1400 single print verifications deployed	
	FEMA	Collect fingerprints from applicants to support disaster recovery operations	60 10-print scanners currently deployed for collection	
Info Sharing		DHS searches and exchanges data with the DOJ Next Generation Identification System (NGI) DHS searches and exchanges data with the DOD Automated Biometric Identification System	DHS searches and exchanges data with international partners	Interfaces with external biometric databases *not standardized across DHS*
Services	OBIM	Lead provider of biometric identity services for DHS, OBIM operates IDENT, the largest U.S. biometric repository with over 200,000,000 identities stored, and provides services for DHS Operational Components to store, match and share biometric data collected during mission operations.		IDENT system *nearing end of life*

Additionally, there are programmatic gaps that limit DHS's ability to enhance biometrics capabilities. Figure 2-2 summarizes the programmatic gaps.

Figure 2-2, Current State Programmatic Snapshot



Organization

Each component *works independently* to design, develop, acquire and deploy biometric solutions.

Policy

Each component independently writes policy, procedures, privacy and regulatory language when deploying biometric solutions. There is *no overarching DHS Biometric Rule.*

Acquisition

Each component *develops their own acquisition vehicles* to procure biometric systems. Many existing vehicles overlap and emerging vehicles may meet the needs of other components.

Communication

Each component *communicates their requirements independently with industry* without giving industry a consolidated view of the DHS market.

Interoperability

Components *develop interfaces and middleware to biometrics service providers* independently.

Collaboration

There is *no formalized collaboration* across DHS to perform knowledge transfer to components entering the biometrics space.

The lack of an Integrated Strategy for Biometrics:

Discourages industry investment since they don't know what we need

Increases cost through duplication of effort

Delays time to market by not sharing acquisition vehicles, letting industry know what is needed, or streamlining policy processes

Hinders knowledge transfer by perpetuating stovepipes

Discourages interoperability between related mission functions

3 Vision, Goals and Objectives for Biometrics within DHS

The vision, goals and objectives for biometrics within the Department must support and enable the core mission areas outlined in the 2014 QHSR and the DHS 2014-2018 Strategic Plan and the foundational principal of maturing and strengthening the homeland security enterprise.[2]

1. Preventing terrorism and enhancing security
2. Securing and managing our borders
3. Enforce and administer our immigration laws
4. Safeguarding and securing cyberspace
5. Strengthen national preparedness and resilience

To support these core mission areas, DHS biometric capabilities must support the individual missions of DHS Components while integrating available data and establishing common means and standards to measure effectiveness of data in order to generate effective solutions. By establishing

[2] The DHS 2014 Quadrennial Homeland Security Review Report describes the Homeland Security Enterprise as "…Federal, State, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of America and the American population." It is also referenced in this manner in the DHS Fiscal Years 2014–2018 Strategic Plan.

a cohesive and integrated strategy for employment of DHS enterprise biometric capabilities that leverage technology advancements, DHS will continue to ensure national security and public safety through leadership in applying the next generation of biometrics capabilities, while transforming operations to be more efficient and effective.

Vision for Biometrics in DHS: Achieve Unity of Effort in addressing biometric capability gaps and advancing biometric uses across DHS to strengthen national security while respecting privacy and civil liberties and transform law enforcement, immigration, security, and disaster recovery operations.

Goal 1: Enhance effectiveness of subject identification

Objective 1.1: Refresh outdated biometric collection systems

Refreshing end-of-life systems to employ current biometric technology that can efficiently collect high quality biometric data across DHS will improve DHS's ability to identify threats or imposters, utilize the biometrics in other field environments, and share more reliable data with other stakeholders. Refreshing technology does not only mean updating collection devices, it may also require investment in application changes, system interface updates, storage and network infrastructure, as the bandwidth requirements could increase with better quality images.

Objective 1.2: Centralize access to federal and international biometric databases

Today, each DHS Operational Component requiring access to other Federal Government biometric databases external to DHS interfaces with those databases directly. For each system, stakeholder coordination, requirements, development and integration is required as a means for multiple systems to receive vital information supporting subject identification. By centralizing access to biometric databases of other Government agencies through the DHS IDENT system, DHS Operational Components will reduce the complexity of existing environments, eliminate the need for duplicative services, and standardize the approach by which DHS interfaces with external partners. Currently, the IDENT Re-architecture plans to implement the centralized approach to external biometric database access. This will also require DHS Operational Components presently interfacing independently with external biometric databases to migrate to a centralized approach.

Objective 1.3: Improve real-time access from field locations

In remote field environments, the ability to access real-time information to verify or identify subjects encountered in remote environments is limited, which can put law enforcement officials at risk if they are unaware of imminent threats. By improving connectivity in field locations, across joint mission areas, such as the United States Border Patrol and U.S. Coast Guard's collection of biometrics from subjects apprehended in remote field environments, DHS's security posture will increase.

Objective 1.4: Expand use of multi-modal biometrics to identify threats

The foundation of identity for both DHS internal and external security systems is fingerprint biometrics. Fingerprints are used to search records of criminal history and to record encounters with subjects seeking admission to the United States or applying for immigration benefits. Other government agencies have experienced significant performance improvements as a result of their investments in alternate biometrics collection such as iris or facial recognition, in addition to fingerprints, of subjects of interest. The use of multi-modal biometrics by DHS during subject encounters will strengthen DHS's ability to detect threats to national security by employing a layered identify verification approach. Additionally, leveraging multi-modal biometric data to assist DHS in vetting candidates applying for internal positions to support DHS's various missions will assist in detecting threats or imposters and preventing inside threats.

Goal 2: Transform identity operations to optimize performance

Objective 2.1: Automate resource intensive identity processes

The highest cost of manned identity solutions within DHS is the recurring human resource cost. The use of multi-modal biometrics to automate identification processes, will transform the way DHS does business. By automating identity verification, resources currently required for these processes can be reallocated to other critical mission areas to enhance national security. Additionally, automation will provide better notification of possible threats and alerts to security personnel, allowing them to focus on the threat and not a system. Automation of resource intensive identity processes can be applied to both external DHS operations as well as internal DHS physical security controls.

Objective 2.2: Implement person-centric biometric processing

DHS systems today are encounter based. Biometric encounters are created when people apply for a benefit, cross a border, are stopped at a checkpoint, apprehended between ports of entry, interdicted in coastal waters, and detained in DHS facilities. Each of these encounters, makes up the history of a person, but by representing the data in an encounter-based fashion, it makes adjudication processes more complicated, and presents challenges in the ability to re-use data for other purposes. Over the next 10 years, DHS will move toward person-centric view capabilities. Person-centric view capability across DHS business processes such as citizenship or enforcement status can improve decision-making. Moreover, by providing multiple uses for a single biometric collection will provide cost savings to the Department and convenience to the individual.

Objective 2.3: Expedite security processes using identity verification capabilities

The ability of DHS to facilitate security processing without impacting national security is critical to the nation's economy. Over the next 10 years, DHS will identify and exploit opportunities to implement identity verification capabilities that will reduce processing time, while maintaining or enhancing security. Use of biometrics rather than credentials or documents to verify identity will reduce vulnerabilities and fraud.

Goal 3: Refine processes and policies to promote innovation

Objective 3.1: Institutionalize joint requirements efforts

Each DHS Operational Component presently plans and supports implementation of needed biometric solutions independently. To date there has been no overarching assessment of biometric capability requirements to identify opportunities for efficiencies. With the creation of the JRC and forums such as the IBSV Biometrics Sub-Team, DHS will strive to implement joint-requirements to more efficiently address overlapping joint mission needs and Departmental oversight requirements, without hindering DHS Operational Component's ability to meet mission needs as they arise.

Objective 3.2: Establish DHS-wide biometrics authorities

One of the major "barriers to entry" and inability for DHS organizations to take on the implementation of biometric solution enhancements is the confusion of current legal authorities. An overarching biometric policy for the Department will provide clear and consistent guidance for DHS operators and oversight authorities on when it is, and is not, appropriate to collect and share biometric data. Such activities could include: a department–level regulation that authorizes all components with identity screening responsibilities to collect multiple modes of biometric identity information with their mission areas; policy guidance on appropriate uses and sharing of biometric data; and leadership prioritization of biometric initiatives.

Objective 3.3: Develop privacy policies and processes

Currently when components implement or update biometrics collections, they must coordinate with the component privacy offices to ensure that the technology sustains and does not erode privacy protections. Typically those processes are performed on a system-by-system basis, according to the specific legal authorities under which the information is collected. While it has taken the initial step of identifying which biometric records have been collected pursuant to the administration of criminal justice, DHS should build on this by developing additional privacy policy to apply to other collections of biometrics to ensure consistency across components and offices in implementing biometric solutions within DHS. By categorizing information according to the purpose for the original collection and sharing it for compatible purposes, DHS will optimize the process of implementing biometrics solutions across DHS, without compromising the privacy protections required by law and DHS privacy and civil liberties policies.

Objective 3.4: Enhance stakeholder communications

There is a need to enhance knowledge management and information sharing across DHS, with other federal and international government agencies, and with industry and academia to ensure more effective communication of DHS requirements. Through the stand-up of the JRC, and specifically the IBSV Biometrics Sub-Team, a forum for communication across DHS stakeholders is now established.

It is critical that DHS enhance communications to promote innovation and better articulate requirements to stakeholders that can offer solutions to operational challenges. Through better knowledge management, industry and academic forums and joint requirements efforts, the communication of needs will enhance DHS's overall capabilities.

Objective 3.5: Implement standardized solutions

Currently, DHS Operational Components implement duplicative services to interface with IDENT. In some cases, duplicative services even exist within individual DHS Operational Components. Over the next ten years, DHS will identify cross-component needs for which the development of standardized, re-usable, enterprise biometrics services can be established to minimize maintenance of duplicative (or near-duplicative) services. Enterprise services will utilize government and industry open standards to allow for further innovation and interoperability. Additionally, biometrics solutions should utilize open standards for collection and storage of biometric data.

Objective 3.6: Establish governance and ensure appropriate oversight

Establishing a governance structure from which biometric portfolio objectives can be prioritized and managed across the department is essential to DHS's ability to implement a joint biometrics strategy. Additionally the role of oversight organizations such as DHS Privacy (PRIV), Civil Rights and Civil Liberties (CRCL) and the Office of General Council (OGC) are critical in DHS's ability to successfully execute the strategy while continuing to protect the rights and privacy of citizens and operate within relevant legal authorities. DHS will ensure the establishment of a governance structure and oversight are applied to strategic efforts ensure protection of DHS and its stakeholders.

4 DHS Strategic Alignment

Figure 4-1 shows how the Biometrics Strategic Framework goals are aligned with the DHS Core Mission Framework Goals and priorities.

	Biometrics Strategic Framework		
DHS Core Missions	**Enhance effectiveness of subject identification**	**Transform identity operations to optimize performance**	**Refine processes and policies to promote innovation**
Preventing Terrorism and Enhancing Security	✓	✓	✓
Securing and Managing our Borders	✓	✓	✓
Enforce and Administer Immigration Laws	✓	✓	✓
Safeguarding and Securing Cyberspace	✓	✓	✓
Strengthen National Preparedness and Resilience	✓	✓	✓

Figure 4-1, DHS Biometrics Strategic Goal Alignment to DHS Core Missions

5 Reference

The DHS Biometrics Strategic Framework was developed with input from a variety previous efforts and guidance across DHS, including:

1. National Security Presidential Directive 59 / Homeland Security Presidential Directive 24: Biometrics for Identification and Screening to Enhance National Security
2. DHS 2014 Quadrennial Homeland Security Review
3. DHS 2014-2018 Strategic Plan
4. DHS CIO / SCO Identity Management and Screening Memorandum (May 2007)
5. DHS CIO / SCO Validation of 2007 Target Architecture Direction Memorandum (Oct. 2010)
6. OBIM Strategic Plan Fiscal Years 2014 – 2018 (May 2013)
7. OBIM Mission Need Statement (Feb. 2014)
8. Independent Program Analysis and Evaluation Screening and Vetting with Biometrics Capability-Based Assessment (April 2014)
9. U.S. Southern Border and Approaches Campaign Plan (Nov. 2014)
10. DHS Joint Biometrics Preliminary Mission Need Statement (Mar. 2015)
11. DHS Joint Biometrics Program Decision Option (Mar. 2015)
12. DHS Component capability briefings (to date) from IBSV Sub-Team Meetings including:
    - CBP
    - USCIS
    - ICE
    - USCG
    - DHS MGMT/OCSO