

**DHS Needs to Update Its
Strategy to Better Manage
Its Biometric Capability
Needs**





OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

September 22, 2023

MEMORANDUM FOR: The Honorable Robert Silvers
Under Secretary
Office of Strategy, Policy, and Plans

Randolph D. Alles
Senior Official Performing the Duties of the Under Secretary
for Management

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

**JOSEPH V
CUFFARI**

Digitally signed by
JOSEPH V CUFFARI
Date: 2023.09.22
09:09:20 -04'00'

SUBJECT: *DHS Needs to Update Its Strategy to Better Manage Its
Biometric Capability Needs*

For your action is our final report, *DHS Needs to Update Its Strategy to Better Manage Its Biometric Capability Needs*. We incorporated the formal comments provided by your office.

The report contains four recommendations aimed at ensuring the Department of Homeland Security's biometric capability needs align with DHS strategic initiatives. DHS concurred with all four recommendations. Based on information provided in response to the draft report, we consider the recommendations open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the Inspector General Act, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over DHS. We will post the report on our website for public dissemination.

Please contact me with questions, or your staff may contact Kristen Bernard, Acting Deputy Inspector General for Audits, at (202) 981-6000.

Attachment



DHS OIG HIGHLIGHTS

DHS Needs to Update Its Strategy to Better Manage Its Biometric Capability Needs

September 22, 2023

Why We Did This Audit

Biometric identity verification and biometric matching are integral to DHS' efforts to protect against terrorism, enforce and administer immigration laws, and secure the border. To achieve its mission, DHS must successfully coordinate biometric activities and technologies with its users. We conducted this audit to determine to what extent DHS has an overall management strategy in place to acquire and deploy a biometric solution that meets Department needs.

What We Recommend

We made four recommendations to ensure biometric capability needs align with DHS strategic initiatives.

For Further Information:

Contact our Office of Public Affairs at (202) 981-6000, or email us at

DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

The Department of Homeland Security does not have an up-to-date strategic plan to manage biometric capabilities across the Department. DHS issued a biometrics strategic framework covering 2015–2025 to address biometric capability gaps and advance biometric use across DHS. Although the Office of Strategy, Policy, and Plans (PLCY) now intends to do so, the office had not updated this strategic framework since its issuance 8 years ago. We found the strategic framework did not accurately reflect the current state of biometrics across the Department, such as the use of facial recognition verification and identification. In addition, PLCY has not implemented department-wide policy for the consistent collection and use of biometric information. Lastly, DHS does not have a transition plan to integrate U.S. Customs and Border Protection's Biometric Entry-Exit system with the Office of Biometric Identity Management's Homeland Advanced Recognition Technology system for biometric matching.

PLCY has taken steps to ensure DHS' biometric capability needs align with department-wide strategic initiatives for biometrics. However, without an updated strategic plan and a department-wide policy for consistent collection and use of biometric information, DHS may not be able to ensure identified programmatic biometric capability needs align with DHS strategic initiatives and may be missing opportunities to enhance biometric practices and policies in support of its mission.

DHS Response

DHS concurred with all four recommendations.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Background

The Department of Homeland Security uses biometric information to positively confirm the claimed identity of an individual, generate an alert if an individual has derogatory information associated with their biometrics, or inform officers if an individual previously claimed a different persona. Biometric information enables national security and public safety decision making by producing accurate, timely, and high-assurance identity information and analysis in the areas of immigration and border management, law enforcement, defense and intelligence, and the provision of benefits and services. Biometrics are unique physical characteristics, such as fingerprints, facial features, and iris patterns. Biometric-associated biographic data includes, among other information, name, date of birth, and country of origin.

DHS has a decentralized oversight structure for biometrics with accountability dispersed among DHS offices. DHS components are responsible for developing and deploying their own biometric capabilities in support of mission objectives. Biometric management and policy activities are assigned across various offices and working groups. In April 2019, the DHS Under Secretary for Management established the Biometric Capabilities Executive Steering Committee as a forum for cross-component collaboration to ensure complementary biometric efforts across the Department. DHS also established the Joint Requirements Council Fingerprint, Face, and Iris Portfolio Team to identify and recommend joint solution approaches and address identified gaps and requirements.

The Office of Biometric Identity Management (OBIM) supplies DHS and its mission partners with the capability for matching, storing, and sharing biometric data.¹ OBIM maintains the largest biometric repository in the U.S. Government. OBIM plans to replace its current legacy system, the Automated Biometric Identification System (IDENT), with the Homeland Advanced Recognition Technology (HART) system, which will serve as the primary DHS system to match, store, and share biometric and associated biographic data for national security, law enforcement, immigration and border management, intelligence, background investigations, and other administrative uses.

The Office of Strategy, Policy, and Plans (PLCY) also plays a key role in the Department's biometrics. In December 2019, the Acting Secretary of Homeland Security issued a delegation of authority to the Under Secretary for PLCY to develop and implement department-wide biometric strategic plans and policies to promote and ensure quality, consistency, and integration for the programs, components, offices, and activities across DHS.² PLCY is also responsible for

¹ OBIM's mission partners include Federal Government agencies, state and local law enforcement, and international partners.

² DHS Delegation Number 23000, *Delegation to the Under Secretary for Strategy, Policy, and Plans*, December 9, 2019.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

negotiating and executing agreements between and among the Department and other Federal agencies and state, local, and tribal governments.

As biometric capabilities are identified, it is important that they complement each other and align strategically, technically, effectively, and operationally with applicable strategic goals and objectives. According to Office of Management and Budget (OMB) Circular No. A-11,³ a strategic plan plays a critical role in communicating a vision for the future to agency managers, employees, delivery partners, suppliers, Congress, and the public. It should be used to inform decision making about the need for major new acquisitions, information technology, and strategic human capital planning. Also, a strategic plan should support planning across organizational operating units and describe how agency components are working toward common results.

We previously reported on U.S. Customs and Border Protection's (CBP) efforts to develop and implement biometric capabilities, including facial recognition technology, to track individuals at ports of entry.⁴ Our audit determined that biometric data collection improved DHS' ability to verify foreign visitor departures at U.S. airports, but guidance was required on department-wide biometric activities to achieve financial, technical, and operational efficiencies. Our previously conducted audits also identified compliance issues related to adequately safeguarding facial recognition data⁵ and proper implementation on DNA collection.⁶ We conducted this audit to determine to what extent DHS has an overall management strategy in place to acquire and deploy a biometric solution that meets Department needs.

Results of Audit

PLCY Did Not Fully Carry Out Its Responsibility to Lead, Conduct, and Coordinate the Implementation of Department-wide Strategies, Policies, and Plans for Biometrics

In December 2019, the Acting Secretary of Homeland Security issued a delegation of authority to the Under Secretary for PLCY to develop and implement department-wide strategic plans and policies to promote and ensure quality, consistency, and integration for the programs, components, offices, and activities across DHS. This includes leading and developing strategies, policies, and plans regarding the collection and use of biometrics. We

³ OMB Circular No. A-11 Section 230 – *Agency Strategic Planning*.

⁴ *Progress Made, But CBP Faces Challenges Implementing a Biometric Capability to Track Air Passengers Nationwide* (OIG-18-80), September 21, 2018.

⁵ *Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot* (OIG-20-71), September 21, 2020.

⁶ *DHS Law Enforcement Components Did Not Consistently Collect DNA From Arrestees* (OIG-21-35), May 17, 2021.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

determined that PLCY did not fully carry out its responsibilities set forth in the delegation.

First, DHS' biometric strategic plan was not up to date. In June 2015, DHS issued the *DHS Biometrics Strategic Framework 2015–2025* (strategic framework) to address biometric capability gaps and advance biometric use across DHS. The purpose of the strategic framework was to establish an overarching vision for how enhanced biometric capabilities would transform DHS mission operations over 10 years. It included goals and objectives to refresh outdated biometric collection systems, centralize access to Federal and international databases, and improve real-time access from field locations. In April 2016, DHS also issued the *Biometrics Roadmap Winter Study* (roadmap), which included specific actions to implement the goals and objectives in the strategic framework.⁷

We reviewed the strategic framework and the roadmap to determine whether the information was relevant and accurately reflected DHS technology advancements and priorities. We found that the strategic framework, which was issued 8 years ago, did not accurately reflect the current state of biometrics across the Department, such as the use of facial recognition verification and identification. The strategic framework did not account for new technological advancements in its goals and objectives. For instance, since the strategic framework was issued, DHS components have increased their use of biometrics beyond finger scans, particularly by using facial recognition. Yet, the strategic framework did not mention these technological advancements or how they should be incorporated into DHS' vision for enhancing biometric capabilities to transform mission operations. Changes in vetting and adopting new uses of biometrics make it critical that the Department continually review its vision to ensure everyone is working toward common goals and objectives.

According to a senior PLCY official, they did not consider an update necessary because they believed the 2015 strategic framework's 10-year outlook was adequate. We disagree with PLCY's approach. According to OMB Circular No. A-11, strategic plans should be developed and updated every 4 years to align resources and guide decision making. Also, because strategic plans are used to align resources and inform agency decision making about the need for new major acquisitions, information technology, strategic human capital planning, and evaluations, it is critical that the information in such plans be relevant and applicable. At the end of our audit, PLCY was updating the strategic framework and planned to publish an implementation plan to help guide the management of biometrics at DHS.

⁷ The *DHS Biometrics Strategic Framework 2015–2025* and *Biometrics Roadmap Winter Study* were issued by the Deputy's Management Action Group Joint Requirements Council Information-Based Screening and Vetting Biometrics Sub-Team.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Second, PLCY did not implement department-wide policy for the consistent collection and use of biometrics, as required by the 2019 delegation of authority. Instead, each component operates under different rules and authorities and independently writes policy and procedures for using biometrics. According to a senior PLCY official, they review all component biometric policies, and develop supplemental policies to address biometric critical areas “on an as needed basis.”

We identified critical policy gaps for the consistent collection and use of biometrics across DHS. For example, DHS does not have clear and consistent guidance on how components should use facial recognition and for what purposes. DHS also does not have department-wide consistent age requirements for collecting biometrics. According to one senior PLCY official, former Secretary John F. Kelly’s 2017 biometrics expansion memorandum serves as an overarching policy for biometrics at DHS.⁸ However, the memorandum does not include specific requirements as a department-wide policy should. For instance, the memorandum allows components to expand the age of the population subject to biometric collection but does not specify the age range. It also encourages increasing the use of multimodal biometric collection techniques (i.e., collecting different types of biometrics) but does not provide specific guidance on how to do this. In fact, the memorandum directs PLCY to work with DHS components to identify opportunities to enhance biometric collection policies and practices. At the time of our audit, PLCY was drafting a policy for facial recognition and a DNA collection policy to address a DHS Office of Inspector General recommendation in a 2021 report.⁹

Without an up-to-date strategic plan and a department-wide policy, DHS may not be able to ensure identified programmatic biometric capability needs align with DHS strategic initiatives and may be missing opportunities to enhance biometric practices and policies in support of its mission.

DHS Does Not Have a Transition Plan to Integrate CBP’s Biometric Entry-Exit System with the Department’s System

In 2013, CBP was mandated to deploy a biometric entry-exit capability to record arrivals to and departures from the United States.¹⁰ Following several

⁸ DHS Secretary Memorandum, *DHS Biometrics Expansion for Improved Identification and Encounter Management*, May 24, 2017.

⁹ *DHS Law Enforcement Components Did Not Consistently Collect DNA from Arrestees*, OIG-21-35, May 17, 2021.

¹⁰ The *Consolidated and Further Continuing Appropriations Act, 2013* transferred United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program responsibilities. As a result, US-VISIT was renamed the Office of Biometric Identity Management and resumed biometric identity services using IDENT; U.S. Immigration and Customs Enforcement became the mission owner for visa overstay analysis activities; and CBP assumed responsibility for entry-exit policy and operations and implementing a biometric exit program.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

years of testing and pilots, CBP deployed facial recognition technology, now known as the Traveler Verification Service, to support comprehensive biometric entry and exit procedures in the air environment. To expedite its deployment, the Biometric Entry-Exit system was temporarily exempt from using OBIM's IDENT and HART systems for biometric storage and matching.¹¹ In June 2017, the DHS Under Secretary for Management directed CBP to work with OBIM to submit a timeline and roadmap, including a transition plan for when CBP's Biometric Entry-Exit system would use HART services for biometric data storage and matching. The Under Secretary also directed CBP to provide results of its coordination with OBIM on the use of both IDENT and HART prior to the next acquisition decision event. The action to work with stakeholders on transition options was later reassigned by the Deputy Under Secretary for Management, as the chair of the Biometric Capabilities Executive Steering Committee (committee), to the Office of the Chief Technology Officer.

We determined that the Department did not develop a roadmap with a formal transition plan for CBP's Biometric Entry-Exit system to use IDENT and HART for biometric data storage and matching. On May 29, 2019, the Office of the Chief Technology Officer presented to the committee a roadmap to integrate the Traveler Verification Service with HART. The roadmap included recommendations to conduct operational integration testing by the end of fiscal year 2020. It also identified steps to conduct a feasibility analysis and to develop integration costs. At the time of our audit, the committee could not provide evidence that the roadmap had been formalized and that the recommendations presented had been implemented.

According to committee personnel, a roadmap was not formalized due to HART's schedule delays in obtaining initial operational capability.¹² The committee plans to proceed with formalizing a roadmap when the HART program office establishes a new date for initial operational capability. We recognize the Department's requirement to expedite a Biometric Entry-Exit capability. However, without a documented transition plan early in an acquisition DHS may not be able to effectively deploy and manage unified biometric capabilities to support its missions.

Recommendations

Recommendation 1: We recommend the Under Secretary for the Office of Strategy, Policy, and Plans update and finalize the DHS biometric strategic plan.

¹¹ Exec. Order No. 13780; 82 Fed. Reg. 13,209, 13,216 (March 6, 2017), directs DHS to expedite implementation of a biometric entry-exit capability.

¹² HART was not yet operational at the time of this audit.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation 2: We recommend the Under Secretary for Management update and finalize the DHS biometrics implementation plan (roadmap) including assigned duties and tasks and metrics to monitor progress in achieving established goals and objectives.

Recommendation 3: We recommend the Under Secretary for the Office of Strategy, Policy, and Plans, in collaboration with key stakeholders, develop and implement a department-wide policy for the collection and use of all biometric modalities.

Recommendation 4: We recommend the Under Secretary for Management, as chair of the Biometric Capabilities Executive Steering Committee, ensure the committee coordinates efforts to develop a transition plan to integrate U.S. Customs and Border Protection's Biometric Entry-Exit system with the Office of Biometric Identity Management's Homeland Advanced Recognition Technology system.

Management Comments and OIG Analysis

DHS concurred with the four recommendations in the report. Appendix A contains a copy of the Department's response in its entirety. DHS also provided technical comments to our draft report, and we incorporated these comments, as appropriate. A summary of the Department's responses to the recommendations and our analysis follows.

DHS Response to Recommendation 1: Concur. PLCY will update the DHS Biometrics Strategic Framework and place it on a 5-year schedule for review and updates. PLCY will issue guidelines and directions addressing the entire biometrics life cycle continuum, with implementation to be further addressed in the DHS Biometric Roadmap as consistent with PLCY authorities. Estimated Completion Date (ECD): February 29, 2024.

OIG Analysis: The Department's corrective action plan is responsive to the recommendation. We consider this recommendation open and resolved until DHS provides an updated DHS Biometrics Strategic Framework.

DHS Response to Recommendation 2: Concur. The Biometric Capabilities Executive Steering Committee, under the direction of the DHS Under Secretary for Management, will task appropriate DHS components and offices to develop component-specific implementation plans in support of the DHS Biometrics Strategic Framework. The Biometric Capabilities Executive Steering Committee will consolidate component plans into a DHS Biometric Roadmap. ECD: February 29, 2024.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

OIG Analysis: The Department’s corrective action plan is responsive to the recommendation. We consider this recommendation open and resolved until DHS provides an updated DHS Biometric Roadmap with assigned duties and tasks and metrics to monitor progress in achieving established goals and objectives.

DHS Response to Recommendation 3: Concur. PLCY, in collaboration with key DHS stakeholders, will consolidate Department policy on the collection and use of biometrics to support the DHS Biometrics Strategic Framework. DHS will integrate all existing DHS biometrics policies into the updated DHS Biometrics Strategic Framework. ECD: February 29, 2024.

OIG Analysis: The Department’s corrective action plan is responsive to the recommendation. We consider this recommendation open and resolved until DHS provides the updated DHS Biometrics Strategic Framework integrating all existing DHS biometrics policies.

DHS Response to Recommendation 4: Concur. The Biometric Capabilities Executive Steering Committee, under the direction of the DHS Under Secretary for Management, will coordinate efforts to develop a plan to transition CBP’s Biometric Entry-Exit system to OBIM’s HART system. A Biometric Capabilities Executive Steering Committee action item will be developed, assigned to the appropriate members, and tracked by the Biometric Capabilities Executive Steering Committee. Further, the timeline and roadmap to integrate CBP’s Biometric Entry-Exit system with HART will depend on HART meeting CBP requirements. The status of this effort and coordination activities will be briefed to the Under Secretary for Management through the Biometric Capabilities Executive Steering Committee’s quarterly meetings. ECD: December 31, 2024.

OIG Analysis: The Department’s corrective action plan is responsive to the recommendation. We consider this recommendation open and resolved until DHS provides a transition plan to integrate CBP’s Biometric Entry-Exit system with OBIM’s HART system.

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

We conducted this audit to determine to what extent DHS has an overall management strategy in place to acquire and deploy a biometric solution that meets Department needs. To accomplish our objective, we interviewed DHS personnel from PLCY, the Science and Technology Directorate, and OBIM.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We researched and analyzed DHS Instruction 102-01-001, *Acquisition Management Instruction*, and DHS Directive 102-01-103, *Systems Engineering Life Cycle*. We also obtained and analyzed the following relevant public laws, directives, and policies:

- *DHS Delegation to the Under Secretary for Strategy, Policy, and Plans*, DHS Delegation Number: 23000, December 2019 and updated January 2022
- *DHS Delegation to the Under Secretary for Management*, DHS Delegation Number: 00002, issued May 2012 and changed October 2019
- *DHS Executive Steering Committee Charter for Biometric Capabilities*, Version 1.1, March 2019
- *National Security Presidential Directive-59 and Homeland Security Presidential Directive-24*, June 2008
- OMB Circular No. A-11 Section 230, *Agency Strategic Planning*, 2021
- *DHS Biometrics Strategic Framework 2015–2025*, Version 1.0, June 2015
- DHS Secretary Memorandum, *DHS Biometrics Expansion for Improved Identification and Encounter Management*, May 2017

To determine whether DHS has a current management strategy, a strategic plan, and a department-wide policy, we interviewed DHS PLCY personnel and reviewed and analyzed OMB Circular No. A-11, Section 230; *DHS Biometrics Strategic Framework 2015–2025*; and *DHS Delegation to the Under Secretary for Strategy, Policy, and Plans*. We also compared and assessed numerous laws, regulations, and authorities for the collection and protection of biometric information, such as Public Law 115-254, Section 1919, *Federal Aviation Administration Reauthorization Act of 2018*, October 2018; *DHS Privacy and Civil Liberties Policy Guidance Memorandum*, June 2009; Public Law 106-215, *Immigration and Naturalization Service Data Management Improvement Act*, June 2000; Public Law 106-396, *Visa Waiver Permanent Program Act*, October 2000; and Public Law 107-56, *PATRIOT Act*, October 2001.

We interviewed DHS personnel from OBIM and the Science and Technology Directorate to determine whether DHS completed the transition plan to integrate biometric systems. We also assessed the Biometric Capabilities Executive Steering Committee’s action items and determined that although the transition plan requirement was reassigned, the transition plan was not formalized nor acted upon.

To determine whether DHS provided adequate oversight of its biometric capabilities, we interviewed PLCY and OBIM personnel. We reviewed and analyzed the *DHS Delegation to the Under Secretary for Strategy, Policy, and Plans* and the Secretary’s 2017 memorandum but did not agree with PLCY’s statement that the Secretary’s 2017 memorandum serves as an overarching policy.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We assessed the internal controls over DHS' strategy to acquire and deploy biometric solutions. Our internal control review was limited to the strategies, oversight, policies and procedures, and defined roles and responsibilities for deployment and use of biometric capabilities in support of DHS' mission objectives. We identified weaknesses with strategic plans, DHS policies, and transition plans, as discussed in the body of the report. Because our internal control review was limited, our assessment may not disclose all internal control deficiencies that may have existed at the time of our audit.

We conducted this performance audit between January 2022 and December 2022 pursuant to the *Inspector General Act of 1978*, 5 U.S.C. §§ 401-424, and in accordance with generally accepted government auditing standards. Those standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DHS OIG's Access to DHS Information

During this audit, DHS provided timely responses to DHS OIG's requests for information and did not delay or deny access to information we requested.

The Office of Audits major contributors to this report are Carolyn Hicks, Director; Paul Exarchos, Audit Manager; Ardeth Savery, Auditor-in-Charge; Michaela Stuart, Auditor; Edgardo Prats-Reyes, Auditor; Lindsey Koch, Communications Analyst; Jason De Los Santos, Counsel; and Maria Holmes, Independent Referencer.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix A
DHS Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

August 24, 2023

MEMORANDUM FOR: Joseph V. Cuffari, PhD
Inspector General

FROM: Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

SUBJECT: Management Response to Draft Report: "DHS Needs to Update Its Strategy to Better Manage its Biometric Capability Needs" (Project No. 22-027-AUD-DHS)

**JIM H
CRUMPACKER**
Digitally signed by JIM H
CRUMPACKER
Date: 2023.08.24 08:25:16
-04'00'

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

DHS leadership is pleased to note OIG’s positive recognition of the steps that the DHS Office of Strategy, Policy, and Plans (PLCY) has taken to ensure DHS’ biometric capability needs align with department-wide strategic initiatives for biometrics. Leadership, however, is concerned that the OIG clearly misunderstand PLCY roles, responsibilities, and authorities as they apply to overseeing DHS people screening and vetting programs by incorrectly concluding that “PLCY did not fully carry out its responsibility to lead, conduct, and coordinate the implementation of department-wide strategy, policy, and plans for biometrics.”

As PLCY explained to OIG throughout this audit, including most recently during the technical comments phase,¹ PLCY does not have authority or the responsibility to “implement” DHS policies. While PLCY has been delegated responsibility to “promote and ensure quality, consistency, and integration” across DHS’ strategies, policies, and plans, PLCY does so to the degree appropriate considering each Component’s unique authorities, roles, responsibilities, and diverse operational requirements and mission environments.

¹ This is a process whereby DHS program officials, subject matter experts, and others provide the OIG written feedback addressing accuracy, sensitivity, context, and editorial issues with draft work products for OIG’s consideration and disposition, as deemed appropriate.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

More specifically, PLCY sets enterprise-level policy requirements that can be applied routinely and broadly (e.g., the PLCY and DHS Chief Information Officer joint requirement for Components to use Automated Biometric Identification System (IDENT) for their biometric storage and matching service’s needs), and that provide overarching guidance to Components and Headquarters (HQ) Offices. These Department-wide policies cannot prescribe how each Component and office will achieve their operational missions, develop business and system requirements, conduct research and development, perform capability testing, begin operational deployment, and conduct evaluation. Instead, each Component and office is responsible for making its own inform decisions on which, if any, biometric modalities to use and what should be the ages of people from whom they are collected.

DHS Components and offices are best able to lead and conduct their biometric recognition planning as part of their mission-based identity screening and vetting requirements under overarching guidance and oversight from the Department. Components and offices must obtain implementation approvals through multiple layers of Component, Departmental, and often Office of Management and Budget review before collecting, storing, matching, sharing, and retaining biometric data. PLCY functions in a coordinating role for these processes and procedures—in conjunction with the DHS Office of Privacy, Office for Civil Rights and Civil Liberties, Office of the General Counsel, Management Directorate (MGMT), Science & Technology Directorate, and the operational Components themselves.

Nonetheless, OIG suggests that PLCY did not impose consistency in the uses of biometric modalities or specific age-based collection requirements on biometrics collections across the Department when it promulgated the Secretary of Homeland Security memorandum, “DHS Biometrics Expansion for Improved Identification and Encounter Management,” dated May 24, 2017. Leadership disagrees with the OIG’s contention that PLCY must prescribe specific biometric modalities and age collection requirements to provide consistency and integration across the Department. The Secretary’s 2017 policy memorandum encourages Components to collect and use additional biometric modalities beyond fingerprints and to remove immigration-related age range barriers to collection. However, the memorandum specified that Components should only do so as operationally required, technically feasible, and in compliance with privacy, civil rights, and civil liberty requirements. This policy reflects an intention to avoid a one-size-fits-all approach and enable individual Components to tailor its application according to their specific mission requirements.

Furthermore, PLCY regularly collaborates with MGMT and other HQ offices to provide enterprise-level direction as needed, such as using IDENT for storage and matching services. as PLCY relies on the individual Components, and often their sub-offices, to determine which technologies best enable them to perform the people screening and vetting required to achieve their operational missions and quickly adapt to changes in the



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

security threat environment. Accordingly, the 2017 memorandum, requires Components to conduct proper due diligence to ensure that any new biometric modalities used, and any changes to age collection requirements are operationally required, technically feasible, and protective of privacy, civil rights, and civil liberties.

DHS remains committed to managing its biometric capability needs through policies and processes that support its critical and ever-evolving missions, primarily through the Biometric Capabilities-Executive Steering Committee (BC-ESC), which serves the Department's coordinating mechanism for strategies and implementation plans related to biometrics.

The draft report contained four recommendations with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual and other issues under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions.

Enclosure



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

**Enclosure: Management Response to Recommendations
Contained in 22-027-AUD-DHS**

OIG recommended that the Under Secretary for the Office of Strategy, Policy, and Plans:

Recommendation 1: Update and finalize the DHS biometric strategic plan.

Response: Concur. PLCY will update the DHS Biometric Strategic Framework and place it on a five-year schedule for review and updates. PLCY will issue guidelines and directions addressing the entire biometrics lifecycle continuum, with implementation to be further addressed in the DHS Biometric Roadmap as consistent with PLCY authorities. Estimated Completion Date (ECD): February 29, 2024.

OIG recommended that the Under Secretary for Management [USM]:

Recommendation 2: Update and finalize the DHS biometrics implementation plan (roadmap) including assigned duties and tasks and metrics to monitor progress in achieving established goals and objectives.

Response: Concur. The BC-ESC, under the direction of the DHS USM, will task appropriate DHS Components and offices to develop Component-specific implementation plans in support of the DHS Biometric Strategic Framework and the BC-ESC, organized under the MGMT Office of Biometric Identity Management (OBIM), will consolidate Component plans into a DHS Biometric Roadmap. The Component implementation plans will be due six months after the DHS Biometric Strategic Framework is completed. The DHS Biometric Roadmap will be completed six months after the Component implementation plans have been provided to the BC-ESC and MGMT-OBIM, where they will be compiled and finalized with Departmental review.

Actions	ECD
DHS Biometric Strategic Framework completion	February 29, 2024
Component Implementation Plans for DHS Biometric Strategic Framework completion	August 30, 2024
DHS Biometric Roadmap completion	February 28, 2025

Overall ECD: February 28, 2025.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation 3: In collaboration with key stakeholders develop and implement department-wide policy for the collection and use of all biometric modalities.

Response: Concur. DHS PLCY, in collaboration with key DHS stakeholders, will consolidate Department policy on the collection and use of biometrics to support the DHS Biometric Strategic Framework. Specifically, DHS will integrate all existing DHS biometrics policies (e.g., key policies from Secretary policies, DHS directives, and DHS agreements) into the updated DHS Biometric Strategic Framework. ECD: February 29, 2024.

OIG recommended that the Under Secretary for Management:

Recommendation 4: As chair of the Biometric Capabilities Executive Steering Committee, ensure the committee coordinates efforts to develop a transition plan to integrate U.S. Customs and Border Protection's biometric entry-exit system with the Office of Biometric Identity Management's Homeland Advanced Recognition Technology [HART] system.

Response: Concur. The BC-ESC, under the direction of the USM, will coordinate efforts to develop a plan to transition U.S. Customs and Border Protection's (CBP) Biometric Entry-Exit (BEE) system to the Office of Biometric Identity Management's HART system. A BC-ESC action item will be developed, tasked to the appropriate members, and tracked by the BC-ESC. Further, the timeline and roadmap to integrate BEE with HART will depend on HART meeting CBP's requirements for BEE. Currently, the ECD for the transition plan is the end of Quarter 1 fiscal year (FY) 2025. This timeframe allows for the rebaselining of the HART Program Initial Operational Capability schedule and influencing the FY 2026 budget, as additional funding will be needed to meet CBP's requirements. The status of this effort and coordination activities will be briefed to the USM through the BC-ESC quarterly meetings. ECD: December 31, 2024



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
CBP Audit Liaison
OBIM Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at:
www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General
Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.



OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" box. If you cannot access our website, call our hotline at (800) 323-8603, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305