OFFICE OF INSPECTOR GENERAL

Homeland Advanced Recognition Technology System Compliance with 28 C.F.R. Part 23

Homeland Security

September 19, 2023

OIG-23-53

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

September 19, 2023

MEMORANDUM FOR: Mason C. Clutter
Chief Privacy Officer
Department of Homeland Security

Shonnie Lyon
Director, Office of Biometric Identity Management

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

GLENN E SKLAR
Digitally signed by GLENN E SKLAR
Date: 2023.09.15 23:37:08 -04'00'

Glenn Sklar
Principal Deputy Inspector General

SUBJECT: *Homeland Advanced Recognition Technology System Compliance with 28 C.F.R. Part 23*

For your action is our final report, *Homeland Advanced Recognition Technology System Compliance with 28 C.F.R. Part 23*. We incorporated the formal comments provided by your office.

The report contains three recommendations the Department of Homeland Security should take to ensure the Homeland Advanced Recognition Technology System's privacy risks are mitigated. DHS concurred with two recommendations and did not concur with one recommendation. Based on information provided in response to the draft report, we consider recommendation 3 open and unresolved. As prescribed by Department of Homeland Security Directive 077-01, *Follow-Up and Resolution for Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for this recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendation will be considered open and unresolved.

Based on information provided in response to the draft report, we consider recommendations 1 and 2 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

Homeland Advanced Recognition Technology System Compliance with 28 C.F.R. Part 23

September 19, 2023

Why We Did This Audit

The Department of Homeland Security Appropriations Bill, 2022 (House Report 117-87) directed the DHS Office of Inspector General to conduct a review of HART technologies, data collection mechanisms, sharing agreements, and privacy protections. As a result, we conducted this audit to determine to what extent OBIM's HART is subject to, and complies with, 28 C.F.R. Part 23. 28 C.F.R. Part 23 provides operating policies to ensure criminal intelligence systems funded under the Crime Control Act are used in conformance with the privacy and constitutional rights of individuals.

What We Recommend

We made three recommendations to ensure HART's privacy risks are mitigated.

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 plan to apply the operating policies of Title 28 of the Code of Federal Regulations (C.F.R.) Part 23, *Criminal Intelligence Systems Operating Policies,* to the Homeland Advanced Recognition Technology System (HART) because it has determined, and we concur, that HART is not a criminal intelligence system, as defined by 28 C.F.R. Part 23. Instead, HART is an identity service provider and data repository that will match, store, and share personally identifiable information. Therefore, HART must operate in accordance with the *Privacy Act of 1974* and the *E-Government Act of 2002.*

Accordingly, the Office of Biometric Identity Management (OBIM) should mitigate all privacy risks associated with how information is characterized, collected, corrected, retained, and shared in HART. However, the DHS Privacy Office did not ensure that DHS systems that supply biometric and biographic data to HART had current Privacy Impact Assessments as required by DHS policy. We determined 2 of 22 systems did not have current privacy compliance documentation. Finally, DHS does not plan to update existing sharing agreements once HART is deployed.

These issues occurred because the DHS Privacy Office responsible for enforcing privacy protections did not provide sufficient oversight of privacy compliance documentation or ensure OBIM implemented all privacy-related recommendations. As a result, DHS cannot ensure HART will protect the privacy of individuals whose information is stored in the system.

DHS Response

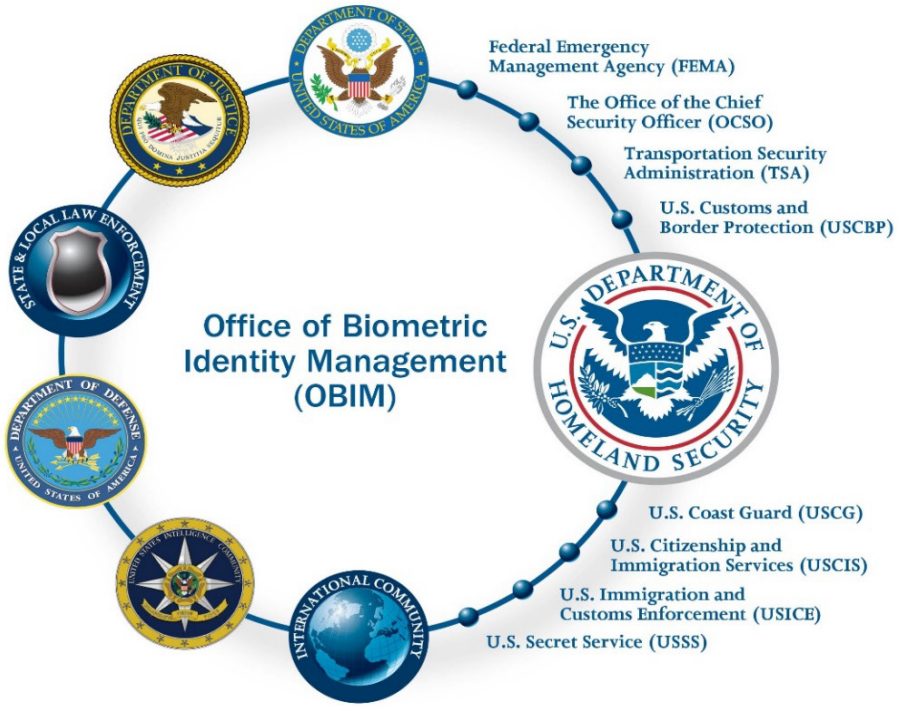
DHS concurred with two recommendations and did not concur with one recommendation.

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 provides biometric identification services through its Office of Biometric Identity Management (OBIM), which provides the capability to match, store, and share biometric data. OBIM operates and maintains the largest biometric repository in the U.S. Government. OBIM shares critical biometric information using advanced data filtering and privacy controls to support the Department and its mission partners. OBIM's mission partners include Federal Government agencies, state and local law enforcement, and international partners (see Figure 1).

Figure 1. OBIM's Mission Partners



Source: OBIM

At the time of our audit, the Automated Biometric Identification System (IDENT) was DHS' system of record for biometric data. DHS plans to replace the legacy IDENT with the Homeland Advanced Recognition Technology (HART) system. HART 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. In 2011, OBIM began a multi-year major acquisition to replace the legacy IDENT system with HART. OBIM is developing HART in two phases: Increment 1 and future capabilities. HART Increment 1 is focused on delivering the core foundational infrastructure and baseline existing functionality of IDENT, and future capabilities will provide added biometric capabilities to meet customer needs, increased interoperability with mission partners, and improved reporting features.

All DHS systems, technology, and programs that collect personally identifiable information (PII) or have a privacy impact are subject to oversight by the Chief Privacy Officer and the requirements of U.S. data privacy and disclosure laws.[1] The DHS Privacy Office is responsible for reviewing and approving all DHS privacy compliance documentation, including:

- *Privacy Threshold Analysis* (PTA): a document used to determine if an information technology system contains PII, whether a Privacy Impact Assessment is required, whether a System of Records Notice is required, and any other privacy requirements.

- *Privacy Impact Assessment* (PIA): a decision tool used by DHS to identify and mitigate privacy risks. A PIA contains information on why the PII is being collected and how the PII will be collected, used, accessed, shared, safeguarded, and stored.

- *System of Records Notice*: a public notice that explains how the information is used, retained, and may be accessed or corrected and whether certain portions of the system are subject to *Privacy Act of 1974*[2] (Privacy Act) exemptions for law enforcement, national security, or other reasons.

- *Periodic review*: Once the PTA, PIA, and System of Records Notice are completed, they are reviewed periodically by the DHS Privacy Office. For systems and programs that require only a PTA and PIA, the process begins again 3 years after the document is complete or when there is an update/change to the system or program, whichever comes first.

[1] PII means any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual. Such information includes a name; social security number; date of birth; and biometric identifiers such as fingerprints, photographs, and iris scans.
[2] *Privacy Act of 1974*, 5 United States Code (U.S.C.) 552a, as amended.

The *Department of Homeland Security Appropriations Bill, 2022,* House Report 117-87 directed the DHS Office of Inspector General to conduct a review of OBIM's HART technologies, data collection mechanisms, sharing agreements, and privacy protections to determine if HART complies with Title 28 of the Code of Federal Regulations (C.F.R.) Part 23, *Criminal Intelligence Systems Operating Policies*.[3] We conducted this audit to determine to what extent OBIM's HART is subject to, and complies with, 28 C.F.R. Part 23.

Results of Audit

DHS Has Determined That 28 C.F.R. Part 23 Operating Policies Do Not Apply to HART But Has Taken Steps to Ensure the System Includes Privacy Protections

The purpose of 28 C.F.R. Part 23 is to ensure all criminal intelligence systems funded under the Crime Control Act[4] are used in conformance with the privacy and constitutional rights of individuals. The regulation is considered the minimum standard for sharing criminal intelligence information for state, local, tribal, and territorial law enforcement agencies across the country. It provides policies to govern criminal intelligence systems for submissions, inquiries, dissemination, reviews and purges, audits and inspections, and security of criminal intelligence information. According to 28 C.F.R. Part 23, a criminal intelligence system is an investigative tool that houses intelligence information related to criminal activity. It includes "the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information." In a 1998 policy clarification, the Department of Justice updated the definition of a criminal intelligence system in 28 C.F.R. Part 23 by excluding identification systems from the regulation.[5]

We concur with DHS' determination that HART is not a criminal intelligence system, as defined by 28 C.F.R. Part 23, and is not funded by the Crime Control Act. We interviewed high-ranking officials from OBIM and the DHS Office of Strategy, Policy, and Plans (PLCY) to determine whether the system will operate under 28 C.F.R. Part 23. Officials from both offices concurred that HART is not a criminal intelligence system, as defined in 28 C.F.R. Part 23, and is not funded by the Crime Control Act. According to OBIM and documents provided, HART is a centralized DHS-wide biometric database that receives both criminal and non-criminal data from mission partners, including DHS components, Federal agencies, international government agencies, and state and local law enforcement agencies.

[3] *Congressional Record*, Vol. 168, No. 42, H2395, March 9, 2022.
[4] *Omnibus Crime Control and Safe Streets Act of 1968*, 42 U.S.C. 3711, et seq., as amended.
[5] Criminal Intelligence Sharing Systems; Policy Clarification, 63 Fed. Reg. 71752 (December 30, 1998) (Clarification to 28 C.F.R. Part 23).

HART is an identity service provider that will store and process biometric data (digital fingerprints, iris scans, facial images) and link the biometrics with biographic information pursuant to the data owner's authorities and policies for use, retention, and sharing of information.[6] The database will contain limited biographic data along with the history of each encounter, including the location and circumstance of each instance resulting in biometric collection needed to place biometric information in the proper context.[7]

OBIM has separate roles and responsibilities from the DHS components and partners who collect biometric data. Primarily, OBIM will not own the biometric or biographic data in HART. Rather, the data providers who collect biometric data will own the data contained in HART and will be able to restrict the maintenance, retention, and sharing of their data with other organizations.[8] OBIM's role is to manage and protect this data, on behalf of its partners, in accordance with legal, policy, and privacy requirements.

Although OBIM will not apply 28 C.F.R. Part 23 operating policies to HART, it will collect, maintain, and share PII in accordance with the Privacy Act and the *E-Government Act of 2002* (E-Government Act).[9] Specifically, the Privacy Act protects individuals by ensuring that personal information collected by Federal agencies is limited to that which is legally authorized and necessary and is maintained in a manner that precludes unwarranted intrusions on individual privacy. The E-Government Act requires agencies to address privacy risks when developing or procuring new or modified technologies to collect, maintain, use, or disseminate PII on or from members of the public.

DHS Needs to Fully Mitigate All Privacy Concerns Before HART Is Deployed

The DHS Privacy Office is responsible for ensuring that all DHS components and mission operations adhere to DHS privacy policies and protections. Specifically, the DHS Chief Privacy Officer is responsible for reviewing and approving all privacy compliance documentation. The E-Government Act requires PIA when developing information technology that collects, maintains, or disseminates PII. A PIA provides an analysis of the privacy considerations posed by a system or program and recommendations to mitigate any impacts on privacy. It informs the public as to what information will be collected; why the information is being collected; how the information will be used, stored, accessed, and protected from unauthorized use or disclosure; and how long the information will be retained. The Chief Privacy Officer elects to conduct a Privacy Compliance Review (PCR) to evaluate how a program office is protecting

[6] If a system user determines a candidate matches a fingerprint (biometric), they might request additional biographical data such as name and date of birth.
[7] HART Increment 1 will not retain DNA.
[8] HART users that do not store biometric information will have search only access.
[9] *E-Government Act of 2002*, Pub. L. No. 107-347, 44 U.S.C. § 3601.

privacy as described in its PIA. A PCR may result in a public report or internal recommendations, depending on the sensitivity of the program under review.

In February 2020, OBIM conducted a PIA of HART Increment 1.[10] In the PIA, OBIM identified 11 privacy risks related to how information is characterized, collected, corrected, retained, and shared in HART. Examples of the privacy risks identified include:

- A risk that data quality will not be maintained because HART users can manually apply derogatory and disposition information. Derogatory information is information that potentially justifies unfavorable suitability, fitness, or security.

- A risk that retaining fingerprint, facial, or iris biometrics for juveniles may result in inaccurate results due to factors including growth and image quality.

- A risk that data owners may not delete their records in a timely manner or in accordance with their respective retention schedule.

- A risk that, when sharing HART data with foreign partners, it is more difficult for DHS to externally impose the same controls that govern the data internally.

The DHS Privacy Office made 13 recommendations in the "Privacy Impact Analysis" section of the PIA to better mitigate the privacy risks. However, we determined the DHS Privacy Office did not provide sufficient oversight to ensure OBIM implemented all privacy-related recommendations. At the time of our audit, nearly 3 years following the assessment, only 1 of the 13 recommendations was resolved and closed. Although the Chief Privacy Officer assigned a PCR team to track the recommendations, the DHS Privacy Office could only provide us with a status of the recommendations as of April 2021. According to a Privacy Office official, the office could not provide DHS OIG with a more current update because the sole member of the PCR team retired in July 2021, and they had not assigned a new team to track the status of recommendations.

According to OBIM, it is in the process of addressing the privacy risks and is working to obtain exemptions for some of the identified risks. However, DHS Instruction 047-01-001*, Privacy Policy and Compliance,* does not specify whether all privacy risks must be mitigated prior to the system going live.

[10] *Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (HART), DHS/OBIM/PIA*, February 24, 2020; https://www.dhs.gov/publication/dhsobimpia-004-homeland-advanced-recognition-technology-system-hart-increment-1.

DHS Did Not Ensure All DHS Systems Sharing Data with HART Had Current PIAs

DHS Instruction 047-01-001 requires information technology systems and programs that use PII or otherwise impact the privacy of individuals to complete a PTA.[11] The PTA helps the Chief Privacy Officer determine if a system or program is privacy sensitive and whether additional privacy compliance documentation, such as a PIA, is needed. The Chief Privacy Officer is supposed to conduct a mandatory review of the PTA every 3 years or when there is an update or change to the system, whichever comes first.

The HART Increment 1 PIA identified 37 DHS systems that will provide biometric and associated biographic data to HART. We assessed 22 of the 37 (59 percent) systems' corresponding PTAs and PIAs and found 2 of 22, did not have current privacy compliance documentation. Specifically, for one system, the DHS Privacy Office did not review and re-certify the PTA after 3 years to validate whether a system change created new privacy risks. For the other system, the DHS Privacy Office determined a new PIA was required. However, at the time of our audit, a PIA had not been completed.

The Office of Strategy, Policy, and Plans Does Not Intend to Update Sharing Agreements

DHS' *Policy Directive 262-15, Privacy and Civil Liberties Policy Guidance Memorandum,* requires that information-sharing activities with external partners that involve PII be formally documented in information sharing and access agreements (ISAA).[12] An ISAA sets the terms for how users can access and use the PII. The Under Secretary for PLCY is the delegated lead for executing sharing agreements, including amendments to such agreements, with Federal, state, local, tribal, foreign governments.[13] Before being finalized, all proposed ISAAs that include sharing of PII must be reviewed by the DHS Privacy Office, the Office for Civil Rights and Civil Liberties, and the Office of the General Counsel. Additionally, the Chief Privacy Officer must approve the finalized ISAAs. As the data steward, OBIM is responsible for ensuring HART data is configured and shared according to the ISAAs.

DHS does not plan to issue new ISAAs for HART. Instead, DHS plans to use the existing ISAAs created for IDENT. According to OBIM officials, they will work with PLCY to review IDENT's existing ISAAs and update them as needed to include references to HART. However, PLCY officials responsible for issuing and amending ISAAs said it was determined that the "technical aspect" of

[11] DHS Directives System Instruction Number 047-01-001, *Privacy Policy and Compliance*, July 25, 2011.
[12] DHS Policy Directive 262-15, *Privacy and Civil Liberties Policy Guidance Memorandum*, June 5, 2009.
[13] DHS Delegation Number 23000, *Delegation to the Under Secretary for Strategy, Policy, and Plans*, Revision Number 01, May 22, 2023.

HART, meaning the users and uses, will not change from IDENT, and therefore would not warrant a change to the ISAAs. As part of our review, we sampled 10 ISAAs with four Federal agencies and found all 10 were either issued under a no-longer-existing program office called the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program or for IDENT.[14] Additionally, three of the ISAAs we reviewed were more than 15 years old.

Although DHS has a requirement to ensure formal sharing agreements are issued when information-sharing activities with external partners involve PII, DHS does not have clear guidance on when to review, update, or issue new ISAAs when upgrading or deploying new technologies. Although the capabilities deployed in HART Increment 1 will not change from IDENT, future enhancements and capabilities may introduce the potential of new data and privacy concerns that may not be covered in these outdated ISAAs.

Recommendations

Recommendation 1: We recommend the DHS Chief Privacy Officer work with the HART program office to monitor and close recommendations made in the HART Increment 1 Privacy Impact Assessment.

Recommendation 2: We recommend the DHS Chief Privacy Officer ensure DHS component systems that use and provide data to HART have current and up-to-date Privacy Impact Assessments.

Recommendation 3: We recommend the DHS Chief Privacy Officer in consultation with the DHS Office of Strategy, Policy, and Plans, issue guidance for when to review, update, or issue new information sharing and access agreements when upgrading or deploying new technologies that collect personally identifiable information.

Management Comments and OIG Analysis

DHS concurred with two recommendations and did not concur with one recommendation. Appendix A contains a copy of the Department's response in its entirety. DHS also provided technical comments to our draft report, and we made changes to incorporate these comments, as appropriate. A summary of the Department's responses to the recommendations and our analysis follows.

DHS Response to Recommendation 1: Concur. The DHS Privacy Office will work with OBIM's Privacy and Policy Branch to monitor and close privacy recommendations identified in the HART Increment 1 PIA. The 13 HART Increment 1 PIA recommendations are a broad mix in the areas of policy and

[14] Transferred United States US-VISIT program responsibilities and identity services using IDENT to OBIM. *Consolidated and Further Continuing Appropriations Act, 2013*, Pub. L. No. 113-6, March 26, 2013.

standards, system requirements, processes, reporting requirements, training, and governance mechanisms. Although the recommendations were made in reference to HART, some of the HART Increment 1 PIA recommendations are policy related and will be addressed by OBIM in coordination with the DHS Privacy Office, PLCY, and DHS components through the Biometric Capabilities Executive Steering Committee. In addition, some of the HART Increment 1 PIA recommendations are mission related and not specific to the HART system itself.

As many of the HART Increment 1 PIA recommendations require coordination across the Department or depend on further policy and technical developments as HART becomes the system of record, the Department will provide the status of the HART Increment 1 PIA recommendations, including which recommendations are closed and an assessment of the recommendations that remain open. Estimated Completion Date (ECD): March 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 documentation showing that recommendations made in the HART Increment 1 PIA are closed.

DHS Response to Recommendation 2: Concur. The DHS Privacy Office will continue to work with the appropriate components and program offices, privacy offices, and other stakeholders to ensure component systems that provide data to HART have current and up-to-date PIAs in accordance with DHS Directive 047-01, *Privacy Policy and Compliance*, and DHS Instruction 047-01-001. The DHS Privacy Office is working with OBIM's Privacy and Policy Branch to better define the landscape of systems providing data and receiving data from HART and will continue to coordinate and collaborate with DHS components and offices to complete the applicable PIAs and PIA updates for the covered systems. ECD: July 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 documentation showing the applicable systems (providing and receiving data from HART) have current and up-to-date PIAs.

DHS Response to Recommendation 3: Non-concur. According to PLCY, administrative changes do not pass the threshold to warrant an update to the ISAA when no functionality changes to data, users, or uses have occurred.

OIG Analysis: We do not consider the Department's actions responsive to this recommendation. DHS does not have clear guidance on when to review, update, or issue new ISAAs when upgrading or deploying new technologies. The recommendation will remain open and unresolved until DHS issues

guidance for when to review, update, or issue new ISAAs when upgrading or deploying new technologies that collect PII.

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 OBIM's HART is subject to, and complies with, 28 C.F.R. Part 23. To accomplish our objective, we obtained and reviewed pertinent Federal, Department, and component regulations, policies, procedures, and guidance relevant to information systems. We interviewed representatives from PLCY; the DHS Privacy Office; and OBIM.

To determine whether HART is a criminal intelligence system, we reviewed 28 C.F.R. Part 23, *Criminal Intelligence Systems Operating Policies,* to identify policies for operating multi-jurisdictional criminal intelligence systems. Additionally, we examined the 1993 revision of 28 C.F.R. Part 23, *Final Revision to the Office of Justice Programs, Criminal Intelligence Systems Operating Policies* (58 Fed. Reg. 48,448), and the 1998 clarification of 28 C.F.R. Part 23*, Criminal Intelligence Sharing Systems; Policy Clarification* (63 Fed. Reg. 71,752). We also met with senior Department officials to determine if OBIM will operate HART in accordance with 28 C.F.R. Part 23 operating policies. To identify the privacy risks related to how data in HART is characterized, collected, corrected, retained, and shared, and whether the risks were mitigated, we reviewed the HART Increment 1 PIA. Additionally, we verified with the DHS Privacy Office whether recommendations made in the HART Increment 1 PIA were implemented. We also reviewed a Notice of Proposed Rulemaking OBIM has proposed to exempt HART from certain provisions of the Privacy Act.

Finally, to assess whether DHS systems that provide biometric and associated biographic data to HART have current PIAs and PTAs, as required by DHS Instruction 047-01-001, we used the HART Increment 1 PIA to identify the DHS systems and their PIAs. We then accessed the PIAs for those identified systems through the DHS Privacy Office website for issued PIAs. We judgmentally selected 21 DHS systems with PIAs older than 3 years. We also selected one DHS system that did not yet issue a PIA. We then requested associated PTAs from the DHS Privacy Office to confirm they were reviewed after 3 years to validate whether a system change created new privacy risks. We eliminated the U.S. Immigration and Customs Enforcement Fugitive Case Management System from our review because it was dispositioned and later consolidated into the Enforcement Alien Removal Module, which is part of ICE's

Enforcement Integrated Database, DHS/ICE/PIA-015 Enforcement Integrated Database.

We assessed internal controls related to how OBIM's HART collects, maintains, and shares PII, in accordance with DHS policies and procedures. Our assessment of DHS policies and procedures would not disclose all material weaknesses in the control structure. Our assessment disclosed that DHS lacked oversight and guidance to ensure HART privacy risks were mitigated and to ensure that data-sharing agreements with partner agencies were reviewed and updated when upgrading or deploying new technologies.

We conducted this performance audit between June 2022 and March 2023 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 that 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 that 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; and Darvy Cruz, Independent Referencer.

Appendix A
DHS Comments to the Draft Report

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

Homeland Security

September 6, 2023

MEMORANDUM FOR: Joseph V. Cuffari, PhD
Inspector General

FROM: Mason C. Clutter
Chief Privacy Officer and Chief FOIA Officer
DHS Privacy Office

MASON C CLUTTER Digitally signed by MASON C CLUTTER Date: 2023.09.06 15:56:02 -04'00'

SUBJECT: Management Response to Draft Report: "Homeland Advanced Recognition Technology System Compliance with 28 C.F.R. Part 23" (Project No. 22-027-AUD-DHS(b))

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

The Department is pleased to note OIG's recognition, and agreement, that Homeland Advanced Recognition Technology (HART) is not a criminal intelligence system, but rather an identity service provider and data repository that will match, store, and share personally identifiable information (PII) once it reaches program initial operational capability (IOC). DHS remains committed to adhering to U.S. privacy laws and DHS privacy policies, applying DHS Fair Information Practice Principles[1] to DHS activities, and treating people and their personal information with respect by ensuring a high standard of privacy protection while executing its mission.

DHS is concerned, however, that the overall conclusion in the OIG's draft report misleads readers into believing that DHS cannot safeguard the privacy of individuals whose information is stored in HART. DHS's Office of Biometric Identity Management (OBIM) completed the appropriate privacy documentation based on plans to reach initial operating capability, and OBIM and PRIV are working to ensure privacy controls are in place to mitigate risks to individuals' PII. It is the Department's priority to fulfill its mission while appropriately safeguarding privacy.

[1] See DHS Privacy Policy Guidance Memorandum 2008-01, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," dated December 29, 2008. https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf

Additionally, the Department stresses that HART has not yet reached program initial operational capability. Accordingly, closing out recommendations is dependent on HART's further technical development. Throughout this process, PRIV and OBIM will continue to coordinate to assess implementation.

The draft report contained three recommendations, two with which DHS concurs (Recommendations 1 and 2) and one with which DHS non-concurs (Recommendation 3). 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. We look forward to working with you again in the future.

Enclosure

Enclosure: Management Response to Recommendations Contained in OIG 22-027-AUD-DHS(b)

OIG recommended that the DHS Chief Privacy Officer:

Recommendation 1: Work with the HART program office to monitor and close recommendations made in the HART Increment 1 Privacy Impact Assessment.

Response: Concur. PRIV will work with OBIM Privacy & Policy Branch (OBIM Privacy) to monitor and close privacy recommendations identified in the HART Increment 1 PIA. The 13 HART Increment 1 PIA recommendations are a broad mix in the areas of policy and standards, system requirements, processes, reporting requirements, training, and governance mechanisms. Since February 2020, OBIM has worked with PRIV to review the recommendations made in the HART Increment 1 PIA and discuss actions currently under way. While the recommendations were made in reference to HART, some of the HART Increment 1 PIA recommendations are policy related and will be addressed by OBIM in coordination with PRIV; the Office of Strategy, Policy, and Plans; and DHS Components through the Biometric Capabilities Executive Steering Committee. In addition, some of the HART Increment 1 PIA recommendations are mission related and not specific to the HART system itself.

As many of the HART Increment 1 PIA recommendations require coordination across the Department or are dependent on further policy and technical development as HART becomes the system of record, an estimated completion date (ECD) cannot be provided at this time. However, by March 29, 2024, or sooner if possible, the Department will provide the status of the HART Increment 1 PIA recommendations. The status will include those recommendations that are closed and an assessment of the open recommendations identified in the HART Increment 1 PIA. It is important to note that OBIM and PRIV will continue to monitor and reassess the appropriateness of the HART Increment 1 PIA recommendations given any changes in Department policy and the evolution of biometrics until the recommendations are closed.

These efforts include the following actions:

Actions	ECD
OBIM Privacy and PRIV review the HART Increment 1 PIA recommendations and establish timelines for closure	March 29, 2024
OBIM Privacy and PRIV close the 13 HART Increment 1 PIA recommendations	TBD

3

OIG recommended that the DHS Chief Privacy Officer and OBIM Privacy & Policy Branch (OBIM Privacy):

Recommendation 2: Ensure DHS component systems' that use and provide data to HART have current and up-to-date Privacy Impact Assessments.

Response: Concur. PRIV will continue to work with the appropriate components and program offices, privacy offices, and other stakeholders to ensure components systems' that provide data to HART have current and up-to-date PIAs in accordance with DHS Directive 047-01, "Privacy Policy and Compliance" (dated July 7, 2011)[2] and DHS Instruction 047-01-001, "Privacy Policy and Compliance" (dated July 25, 2011).[3] PRIV is working with OBIM Privacy to better define the landscape of systems providing data to and receiving data from HART, and will continue to coordinate and collaborate with DHS components and offices to complete the applicable PIAs and PIA updates for the covered systems.

ECD: July 31, 2024.

Recommendation 3: In consultation with the DHS Office of Strategy, Policy, and Plans, issue guidance for when to review, update, or issue new information sharing and access agreements when upgrading or deploying new technologies that collect personally identifiable information.

Response: Non-Concur. As PLCY previously discussed with OIG during its review, it is Policy's practice that administrative changes do not pass the threshold to warrant an update to the ISAA when no functionality changes to data, users, or uses have occurred.

DHS requests thatat OIG consider this recommendation as resolved and closed.

[2] https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-directive-047-01_0.pdf
[3] https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf

4

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

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