United States Government Accountability Office

Report to Congressional Requesters

September 2023

BIOMETRIC IDENTITY SYSTEM

DHS Needs to Address Significant Shortcomings in Program Management and Privacy

GAO-23-105959

GAO Highlights

Highlights of GAO-23-105959, a report to congressional requesters

September 2023

BIOMETRIC IDENTITY SYSTEM

DHS Needs to Address Significant Shortcomings in Program Management and Privacy

Why GAO Did This Study

DHS currently uses an outdated system, implemented over 29 years ago, for providing biometric identity management services (e.g., fingerprint matching). The system stores over 290 million identities. In 2016, DHS initiated a multi-billion dollar program known as HART, which is intended to replace the legacy system. GAO previously reported that due to several challenges, in 2017 the program breached its schedule baseline. In 2019 the program established new cost and schedule commitments with DHS leadership (referred to as a rebaseline). This resulted in delaying the program by 3 years.

GAO was asked to evaluate the HART program. This report's objectives were to (1) determine how the HART program has changed since the 2019 baseline, (2) assess the extent to which the program's cost and schedule estimates followed best practices, and (3) assess the extent to which DHS implemented selected privacy requirements for the program.

GAO reviewed HART planning documentation, evaluated cost and schedule estimates against best practices identified by GAO, and compared privacy documentation to selected Office of Management and Budget privacy requirements. GAO also interviewed appropriate officials.

What GAO Recommends

GAO is making nine recommendations to DHS to follow best practices when preparing HART cost and schedule estimates and implement selected privacy requirements for the system. DHS concurred with the recommendations.

View GAO-23-105959. For more information, contact Marisol Cruz Cain at (202) 512-5017 or cruzcainm@gao.gov.

What GAO Found

Since rebaselining its original cost and schedule commitments in 2019, the Department of Homeland Security's (DHS) Homeland Advanced Recognition Technology (HART) program has further delayed its schedule. Specifically, in 2020 the program declared a second schedule breach and its first cost breach. Accordingly, DHS rebaselined the program again. This extended the schedule for delivering the initial capabilities to replace the legacy system by an additional 33 months beyond the 2019 plan. In addition, the 2022 rebaseline did not include an estimate for completing the program (see table).

Changes in the Homeland Advanced Recognition Technology (HART) Program Schedule from 2019 to 2022

Milestone	Planned completion date[a] (as of May 2019)	Planned completion date[a] (as of May 2022)
Initial operational capability	December 31, 2020	September 30, 2023
Complete full program	June 30, 2024	Not yet planned

Source: GAO analysis of Department of Homeland Security data. | GAO-23-105959

[a]This represents the schedule threshold dates defined in the HART acquisition program baseline.

Regarding costs, the program's 2022 rebaseline increased its estimated costs by $354 million. In April 2023, program officials stated that they needed to rebaseline HART's schedule a third time due to, among other things, higher than expected software defects and performance issues.

The program's 2022 cost and schedule estimates did not fully follow GAO's identified cost and schedule best practices and were, therefore, unreliable. Specifically, the program's cost estimate did not substantially or fully meet the four characteristics of a reliable cost estimate. Moreover, the program's schedule estimate did not substantially or fully meet three of the four characteristics of a reliable schedule estimate. Until these weaknesses are addressed, the HART cost and schedule estimates will continue to be unreliable. In turn, this will impair the ability of senior leadership to make informed decisions regarding the program's future.

DHS fully implemented five of 12 selected Office of Management and Budget privacy requirements. For example, the program addressed the requirement to appropriately encrypt information by demonstrating encryption settings for information at rest and in transit. However, DHS had gaps in the remaining seven requirements. For example, the program's privacy impact assessment, which is intended to analyze how personal information is collected, shared, and managed, was missing key information. Specifically, the assessment was missing information on (1) individuals whose data will be stored in the system and (2) the partners with whom the system will share information. In addition, the program did not have assurances that partners that provide information to the system will appropriately retain and dispose of personally identifiable information. Until DHS addresses these privacy weaknesses, the department lacks assurance that the hundreds of millions individuals' personally identifiable information that will be stored and shared by HART will be appropriately protected.

Contents

Letter		1
	Background	5
	The HART Program Experienced Schedule Delays and Cost Increases since the 2019 Rebaseline	13
	HART Cost and Schedule Estimates Were Unreliable	19
	DHS Did Not Fully Implement a Majority of Selected Privacy Requirements for HART	24
	Conclusions	34
	Recommendations for Executive Action	34
	Agency Comments and Our Evaluation	36
Appendix I	Objectives, Scope, and Methodology	40
Appendix II	Results of GAO's Assessment of the HART Program Cost Estimate Compared with Best Practices	46
Appendix III	Results of GAO's Assessment of the HART Program Schedule Compared with Best Practices	48
Appendix IV	Comments from the Department of Homeland Security	49
Appendix V	GAO Contacts and Staff Acknowledgments	59

Tables

Table 1: Changes in the Homeland Advanced Recognition Technology's (HART) Program Schedule from 2019 to 2022	15
Table 2: Assessment of the Homeland Advanced Recognition Technology (HART) Program Cost Estimate Compared to Characteristics for a Reliable Cost Estimate Using *GAO's Cost Estimating and Assessment Guide*, as of March 2022	20

Table 3: Assessment of the Homeland Advanced Recognition Technology (HART) Program Schedule Compared to Characteristics for a Reliable Schedule Using *GAO's Schedule Assessment Guide*, as of June 2022 23
Table 4: Summary of Department of Homeland Security's (DHS) Implementation of Selected Office of Management and Budget Privacy Requirements for the Homeland Advanced Recognition Technology (HART) Program 25
Table 5: Assessment of the Homeland Advanced Recognition Technology Program's Cost Estimate Compared to Best Practices, as of March 2022 46
Table 6: Assessment of the Homeland Advanced Recognition Technology (HART) Program's Schedule Estimate Compared to Best Practices, as of June 2022 48

Figures

Figure 1: Homeland Advanced Recognition Technology (HART) Key Partners 7
Figure 2: Simplified Planned Process Flow between U.S. Customs and Border Protection and the Homeland Advanced Recognition Technology (HART) System for Biometric Identification and Verification for Air, Land, or Sea Entry 9
Figure 3: Timeline of Homeland Advanced Recognition Technology (HART) Acquisition Program Baselines and Breaches 14
Figure 4: Changes in the Homeland Advanced Recognition Technology (HART) Life Cycle Cost Estimate from May 2019 to May 2022 18

Abbreviations

DHS	Department of Homeland Security
HART	Homeland Advanced Recognition Technology
IDENT	Automated Biometric Identification System
OBIM	Office of Biometric Identity Management
OMB	Office of Management and Budget
PIA	privacy impact assessment
PII	personally identifiable information
SAOP	Senior Agency Official for Privacy

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 12, 2023

The Honorable Gary C. Peters
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Ron Johnson
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

Biometric identity management services, such as fingerprint matching and facial recognition technology, are commonly used across business and government sectors as tools for identifying an individual or verifying an individual's identity. Within the Department of Homeland Security (DHS), the Management Directorate's Office of Biometric Identity Management (OBIM) is the lead entity responsible for providing biometric identity management services.

OBIM's mission is to provide biometric identity services that support national security and public safety decision making for DHS and its partners. OBIM provides services to several DHS components (e.g., U.S. Customs and Border Protection and Federal Emergency Management Agency); as well as the Departments of State, Justice, and Defense; tribal, state, local, and territorial law enforcement; the intelligence community; and international partners.

DHS currently provides biometric identity management services through the Automated Biometric Identification System (IDENT), which became operational over 29 years ago.[1] Among other things, the department uses IDENT to store biographic (e.g., full name, date of birth, and country of origin) and biometric information (e.g., fingerprints, facial features, and iris

[1]IDENT became operational in 1994.

patterns) on U.S. citizens and foreign nationals. It then shares that information with partners to facilitate legitimate travel, trade, and immigration.[2]

However, in 2011 DHS reported that IDENT had significant shortcomings such as system capacity constraints, a lack of ability to handle multiple types of biometric information, and limitations on accuracy and assurance. To mitigate these challenges, DHS initiated the Homeland Advanced Recognition Technology (HART) program in 2016 to replace IDENT and to provide additional capabilities.[3]

The HART system is intended to be a centralized DHS-wide biometric database, which stores and manages over 290 million individuals' personally identifiable information (PII), including biographic and biometric information.[4] HART was originally estimated to cost about $4.2 billion and to be fully implemented by 2021.[5]

In June 2017, the HART program determined it would not be able to meet its initial acquisition program baseline milestones and declared a schedule breach. DHS rebaselined the HART program 2 years later (in May 2019) in response to the breach. However, in June 2021, we reported that the program was significantly behind schedule and had exceeded its most recent cost estimate.[6]

[2]We generally use the term "foreign national" to refer to an "alien," which is defined under U.S. immigration law as any person who is not a U.S. citizen or national. See 8 U.S.C. § 1101(a)(3). In addition, temporary visitors are foreign nationals present in the United States on a temporary basis pursuant to a specific nonimmigrant category (see 8 U.S.C. § 1101(a)(15); 8 C.F.R. § 214.1(a)(1)-(2)), including those who are allowed to seek admission without a visa.

[3]Examples of enhanced functionality include tools to improve human examination of multiple types of biometric information when verifying individuals, a web portal to improve accessibility and provide users with a single web-based point of access to the HART system, and the use of additional types of biometric information such as DNA.

[4]In general, PII is any information that can be used to distinguish or trace an individual's identity, such as name, date or place of birth, and biometric records; or that otherwise can be linked to an individual.

[5]This figure represents the program's life cycle cost estimate established by DHS and OBIM in April 2016. It is presented in base-year 2016 dollars at a 50 percent confidence level and does not include the effects of inflation.

[6]GAO, *Homeland Security: DHS Needs to Fully Implement Key Practices in Acquiring Biometric Identity Management System,* GAO-21-386 (Washington, D.C.: June 8, 2021).

In addition, in 2022, we highlighted that the potential for breaches of biometric information, such as facial images and iris scans, at federal agencies could result in this sensitive information being revealed to unauthorized entities.[7] A breach involving this information may have more serious consequences than the breach of other PII because, unlike conventional identification methods, biometric technologies measure things that are generally distinct to each person and cannot easily be changed.

You asked us to review the HART program. Our specific objectives were to (1) determine how the HART program has changed since the 2019 baseline, (2) assess the extent to which the HART program's cost and schedule estimates followed best practices, and (3) assess the extent to which DHS implemented selected privacy requirements for the HART program.

To address the first objective, we reviewed HART planning documentation to describe the schedule and cost changes that HART has experienced since the 2019 DHS approved baseline. Specifically, we compared the HART schedule and life cycle cost estimates from 2019 to 2022. We also reviewed relevant documentation to describe the status of the program. In addition, we interviewed HART program office officials regarding changes in the program schedule and cost.

To address the second objective, we reviewed and assessed the HART program's cost and schedule estimates from March 2022 and June 2022, respectively. To assess HART's cost estimate, we evaluated documentation against best practices associated with the characteristics of a reliable cost estimate identified in *GAO's Cost Estimating and Assessment Guide*.[8] To assess HART's schedule, we evaluated supporting documentation against best practices associated with the characteristics of a reliable schedule identified in *GAO's Schedule Assessment Guide*.[9]

For both assessments, we also interviewed program officials responsible for developing and managing the program estimates. We provided OBIM and HART program officials with draft versions of our detailed analyses of

[7]GAO, *Facial Recognition Technology: Federal Agencies' Use and Related Privacy Protections,* GAO-22-106100 (Washington, D.C.: June 29, 2022).

[8]GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs,* GAO-20-195G (Washington, D.C.: Mar. 12, 2020).

[9]GAO, *Schedule Assessment Guide: Best Practices for Project Schedules,* GAO-16-89G (Washington, D.C.: Dec. 22, 2015).

the program's cost and schedule estimates to verify that the information on which we based our findings was complete, accurate, and up-to-date.

We determined that the cost and schedule data provided by OBIM was not complete and reliable. We discuss the limitations of these data in the report and we have made appropriate attribution indicating the sources of these data.

To address the third objective, we assessed HART program documents and privacy-related artifacts against selected privacy requirements. Specifically, we selected 12 privacy requirements from Office of Management and Budget (OMB) guidance, including *Managing Information as a Strategic Resource* and *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.[10]

Next, we assessed HART program documentation, including the privacy impact assessment (PIA), system security and privacy plan, records retention schedules, contracts, and information sharing and access agreements inventory and documentation, against the selected requirements. We also interviewed officials from OBIM and other offices within DHS regarding their efforts to implement privacy requirements for HART.

We assessed the reliability of data contained in the system security and privacy plan as well as the information sharing and access agreement inventory by reviewing related documentation and examining these data to identify missing or incorrect information. We followed up with the appropriate officials, as needed. We determined that these data contained in the system security and privacy plan were sufficiently reliable for our reporting objective. We determined that the inventory was not reliable because it was incomplete. We discuss the limitations of these data in the report. A detailed discussion on our objectives, scope, and methodology is provided in appendix I.

We conducted this performance audit from April 2022 to July 2023 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

[10]OMB, Circular A-130*, Managing Information as a Strategic Resource* (Washington, D.C.: July 2016); Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,* (Washington, D.C.: Sept. 26, 2003); and Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a); E-Government Act of 2002, Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921 (2002).

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.

Background

OBIM uses a 29-year-old system known as IDENT to provide DHS and its partners with biometric identity services.[11] The partners use the results from IDENT to perform critical functions, including:

- determining visa issuance and admissibility into the United States;
- establishing eligibility for immigration benefits, including asylum and refugee status;
- determining whether an individual should be granted access to a sensitive facility or sensitive system;
- taking law enforcement actions with potential homeland security implications; and
- verifying the identity of persons associated with matters of national security.

However, in 2011, DHS reported that IDENT had significant shortcomings. Specifically, the department reported that IDENT had:

- significant system capacity constraints,
- a lack of ability to handle multiple types of biometric information,
- the need for improved performance and availability,
- limitations on accuracy and assurance,
- the need for increased interoperability and achievement of cost efficiencies,
- the need for IT security compliance, and
- an inability to meet other current and future mission requirements.

To mitigate these shortcomings, the department initiated the HART program in 2016 to replace IDENT and to provide additional capabilities. At that time, OBIM planned to implement HART in four increments.

[11]IDENT matches, stores, and shares biometric and biographic information that are collected from individuals by partners. OBIM's partners include several DHS components (e.g., U.S. Customs and Border Protection and Federal Emergency Management Agency); as well as the Departments of State, Justice, and Defense; tribal, state, local, and territorial law enforcement; the intelligence community; and international partners.

Increment 1 included the core foundational infrastructure necessary to replace IDENT, operate HART, and to achieve initial operational capability. Once the office completed increment 1, all partners were expected to have migrated from IDENT to HART, thus making HART the system of record. Following this transition, OBIM officials intended to decommission IDENT.

Increments 2 through 4 were intended to deliver additional capabilities, such as using two forms of biometric information to identify and verify an individual (referred to as multimodal fusion);[12] using additional types of biometric information such as DNA, palm, and voice; and performing additional analysis and reporting functions.[13]

HART Is to Store and Share Biometric Information to Identify and Verify Individuals' Identities

Similar to IDENT, HART is intended to match, store, and share biometric and associated biographic information. The partners collect and provide this information in the course of carrying out their missions and submit it to HART. Using HART's biometric identity services, the partners may also submit queries to the system to identify or verify an individual's identity.[14]

OBIM has documented approximately 140 partners that will provide information to HART and/or use the system's biometric identity services.[15] Figure 1 depicts key partners that submit data to HART and/or use the system's biometric identity services.

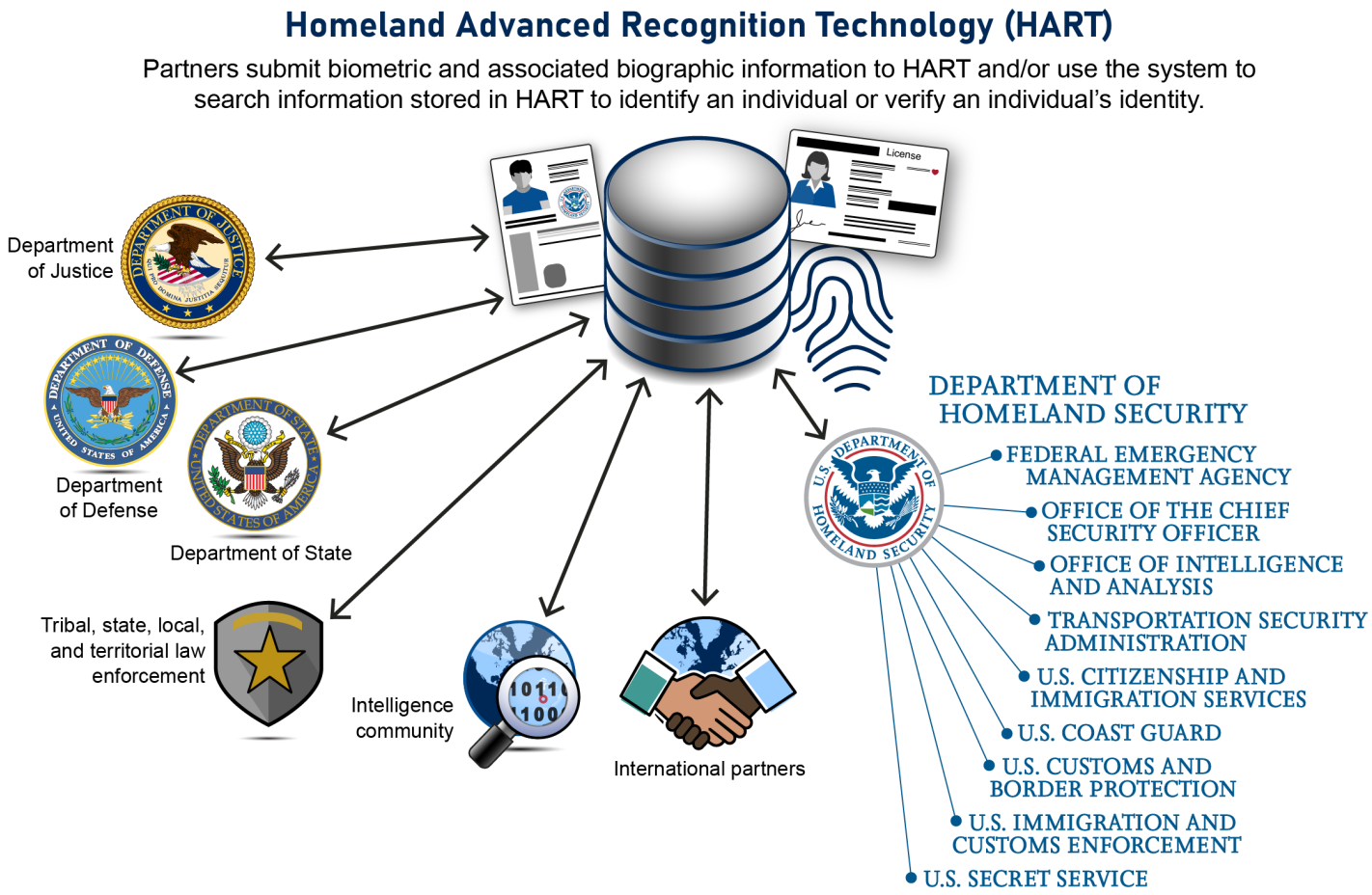
[12]Multimodal fusion is intended to allow for the combining of information from multiple types of biometrics (such as fingerprint and iris pattern) to provide more efficient and accurate identification services and reduce the burden on examiners.

[13]The planned analytic and reporting capabilities are intended to identify trends and patterns, and increase the ability to detect activities requiring immigration or law enforcement action, among other things.

[14]Most partners are considered data providers as well as data users. This means that these partners will submit biometric and biographic information to HART, as well as use the system to search information stored in HART to identify an individual or verify an individual's identity. A small subset of the partners will provide information to HART, but will not query the system. This includes partners that will provide historical information, such as gang affiliations. There are also rare instances where partners will only query the system, but will not provide information to the system. For example, according to OBIM officials, DHS personnel that assist with the Freedom of Information Act requests may search for and extract information to fulfill those requests, but will not provide individuals' information to HART to be stored by the system.

[15]OBIM's documentation identifies partners at the organization, unit, and subunit level. For example, there are seven subunits associated with the Department of State, including one for the Consular Affairs Office's Immigrant Visa Applications and another for Non-Immigrant Visa Applications.

Figure 1: Homeland Advanced Recognition Technology (HART) Key Partners



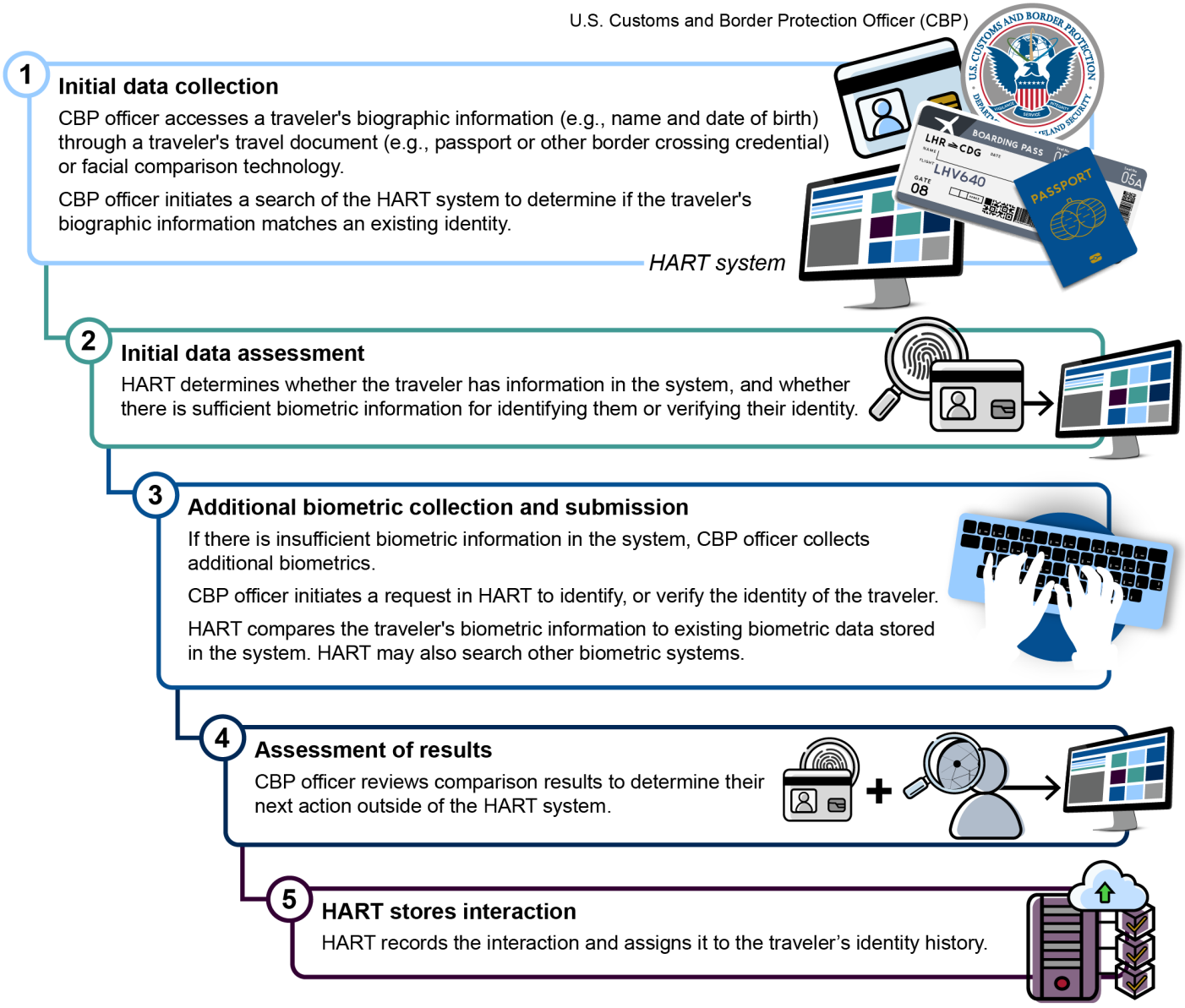
Sources: GAO (analysis of Department of Homeland Security data; icons); agencies (logos). | GAO-23-105959

Similar to their use of IDENT, partners will be expected to use HART for different purposes. For example, among other things, the Department of State is expected to use HART to support biometric identification and verification of international travelers seeking U.S. visas to help determine if visas should be issued. The Transportation Security Administration is expected to rely on the system to retrieve identity information for trusted travelers scheduled to fly within the next 24 hours for use in identity verification at airport security checkpoints. In addition, U.S. Customs and Border Protection is expected to use HART to support biometric identification and verification of in-scope travelers entering and exiting the

U.S. through air, sea, and land ports of entry.[16] Figure 2 describes the planned process flow by which a U.S. Customs and Border Protection officer may use the system.

[16]In-scope international travelers do not include: U.S. citizens; Canadian citizens visiting the United States temporarily for business or pleasure; visitors admitted on a specified visa; children under the age of 14 (unless participating in a trusted traveler program); persons over the age of 79; classes of visitors the Secretary of State and the Secretary of Homeland Security jointly determine shall be exempt; an individual visitor the Secretary of State, the Secretary of Homeland Security, or the Director of the Central Intelligence Agency determines shall be exempt; and Taiwanese officials who hold the specified visas and members of their immediate families who hold these same visas.

Figure 2: Simplified Planned Process Flow between U.S. Customs and Border Protection and the Homeland Advanced Recognition Technology (HART) System for Biometric Identification and Verification for Air, Land, or Sea Entry



Sources: GAO (analysis of agency data; icons); CBP (logo); James Thew/stock.adobe.com; Buffaloboy/stock.adobe.com. | GAO-23-105959

Storing Vast Quantities of PII Poses Privacy Risks

The HART system is expected to store vast quantities of biometric and biographic PII. As of April 2023, OBIM officials stated that IDENT stored more than 290 million separate and distinct identities. In addition, prior to

the Coronavirus Disease pandemic, the IDENT fingerprint gallery was growing at a rate of approximately 2 million fingerprint records each month. OBIM also reported that, on average, the system processed nearly 350,000 transactions daily. The office officials projected that the transaction volumes would return to the pre-pandemic levels and that the number of stored biometrics would continue to increase.

The protection of personal privacy has become a more significant issue in recent years with the increasing amount of data that agencies and other organizations collect, as well as new techniques available for analyzing them. For example, advances in technology, such as new search technology and data analysis software, have made it easier for individuals and organizations to correlate information and track it across large and numerous databases. Recognizing these challenges, we expanded our information security high-risk area in 2015 to include protecting the privacy of PII.[17]

In 2022, we highlighted privacy risks specifically related to facial recognition technology, such as the facial matching capabilities that HART is expected to employ.[18] The potential for data breaches of biometric information such as facial image data sets and iris patterns could result in sensitive information being revealed to unauthorized entities. This is especially concerning because, unlike conventional identification methods, biometric technologies measure things that are generally distinct to each person and cannot easily be changed.

Federal agency collection and use of personal information, including facial images, is governed primarily by the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002.[19] The Privacy Act places limitations on agencies' collection, disclosure, and use of personal

[17]See, most recently GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: Mar. 2, 2021) and *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021).

[18]GAO-22-106100.

[19]5 U.S.C. § 552a; Pub. L. No. 107-347, § 208, 116 Stat. at 2921.

information maintained in systems of records.[20] The E-Government Act requires agencies to conduct, where applicable, a PIA that analyzes how personal information is collected, stored, shared, and managed in a federal system.

In addition, OMB Memorandum M-03-22 provided guidance on implementing the privacy provisions of the E-Government Act.[21] The guidance discusses when agencies should conduct or update a PIA, and what elements are to be included, such as what information is being collected and how it will be used and shared. Further, OMB Circular A-130 outlines some of the general responsibilities for federal agencies managing information resources that involve PII and summarizes the key privacy requirements for managing those resources.[22]

The HART Program Breached Its Initial Baseline and Rebaselined

In April 2016, DHS approved the initial acquisition program baseline for HART. The baseline estimated the total life cycle cost of the new system to be about $4.2 billion.[23] Further, the baseline estimated that initial operational capability would occur in 2018, which would result in the decommissioning of IDENT. The baseline also estimated that full implementation would occur in 2021.

In June 2017, the HART program determined it would not be able to meet its initial acquisition program baseline milestones and declared a schedule breach. According to DHS officials, the breach was due to delays early in the contract award process for increments 1 and 2. In September 2017, 3 months after declaring the schedule breach, DHS awarded a $95 million contract to develop increments 1 and 2.

DHS rebaselined the HART program's cost and schedule estimates 2 years later (in May 2019) in response to the breach. As part of the rebaseline, the department delayed the deployment date for increment 1 by 2 years (from December 2018 to December 2020) and pushed out the

[20]A system of record is defined by the Privacy Act of 1974 as a group of records containing personal information under the control of any agency from which information is retrieved by the name of an individual or by an individual identifier. See 5 U.S.C. § 552a(a)(4), (5).

[21]OMB, Memorandum M-03-22.

[22]OMB, Circular A-130.

[23]This figure represents the program's life cycle cost estimate established by DHS and OBIM in April 2016. It is presented in base-year 2016 dollars at a 50 percent confidence level and does not include the effects of inflation.

program's full deployment date by nearly 3 years (from September 2021 to June 2024).

The rebaselined life cycle cost estimate resulted in a decrease of about $1.4 billion (from $4.2 billion to approximately $2.8 billion).[24] Program officials primarily attributed the cost decrease to a decision to provide storage for HART data using a less expensive cloud-based solution, rather than DHS's data centers.[25] The officials indicated that another reason for the decrease was the removal of technology and refresh upgrades, which were no longer necessary under the cloud approach.

GAO Previously Reported on HART Program Management and DHS Privacy Challenges

GAO previously reported on HART program management and DHS privacy challenges. Specifically, in June 2021, we assessed the extent to which the HART program was adhering to IT acquisition best practices related to risk, contractor, and requirements management, as well as project monitoring and control.[26] We reported that the program had mixed results in implementing the selected IT acquisitions best practices. For example, we reported that a lack of traceability within requirements made it difficult for the program to understand what features had been completed, what work remained, and how to test to ensure features would ultimately meet customers' needs upon integration. We also reported that although the multibillion dollar HART program had suffered continuing delays, the DHS CIO had reported the program as low risk.

We made seven recommendations to improve the success of the program. DHS concurred with all of the recommendations and provided estimated dates for implementing them. As of March 2023, DHS had fully implemented four of our recommendations. However, it has not yet fully implemented the remaining three recommendations related to reviewing contractor deliverables, tracking government labor costs, and monitoring stakeholder involvement.

[24]These figures represent the program's life cycle cost estimate established by DHS and OBIM in April 2016 and May 2019. They are presented in base-year 2016 dollars at a 50 percent confidence level and do not include the effects of inflation.

[25]Cloud computing is a means for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

[26]GAO-21-386.

In addition, in December 2021, we reported on DHS's policies and procedures for protecting PII collected by or shared with its contractors.[27] We made seven recommendations to DHS and its components aimed at improving the oversight of contractors handling PII. For example, we recommended that the DHS Privacy Office provide targeted role-based privacy training to contractors responsible for protecting PII. DHS agreed with the recommendations; however, as of May 2023, the department had not implemented these recommendations.

In September 2022, we reported on privacy program implementation at DHS and other federal agencies.[28] We recommended that DHS fully define and document the role of privacy officials in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages for information systems that involve PII to ensure compliance. We also recommended that the department document a privacy continuous monitoring strategy to ensure that they are effectively monitoring privacy controls on an ongoing basis. DHS agreed with the recommendations; however, as of May 2023, the department had not implemented these recommendations.

The HART Program Experienced Schedule Delays and Cost Increases since the 2019 Rebaseline

Since the first rebaselining in 2019, the program has experienced additional delays in its schedule and increased estimated costs. Specifically, in January 2020, the program declared a second schedule breach—8 months after the initial rebaseline. Moreover, in May 2020, the program also declared its first cost breach.[29]

In May 2022, the program rebaselined its schedule and costs for a second time (2.5 years after declaring the schedule breach).[30] This rebaseline extended the schedule for delivering initial operational capability and prolonged DHS's dependency on IDENT by at least 2

[27]GAO, *DHS Privacy: Selected Component Agencies Generally Provided Oversight of Contractors, but Further Actions Are Needed to Address Gaps,* GAO-22-104144 (Washington, D.C.: Dec. 16, 2021).

[28]GAO, *Privacy: Dedicated Leadership Can Improve Programs and Address Challenges,* GAO-22-105065 (Washington, D.C.: Sept. 22, 2022).

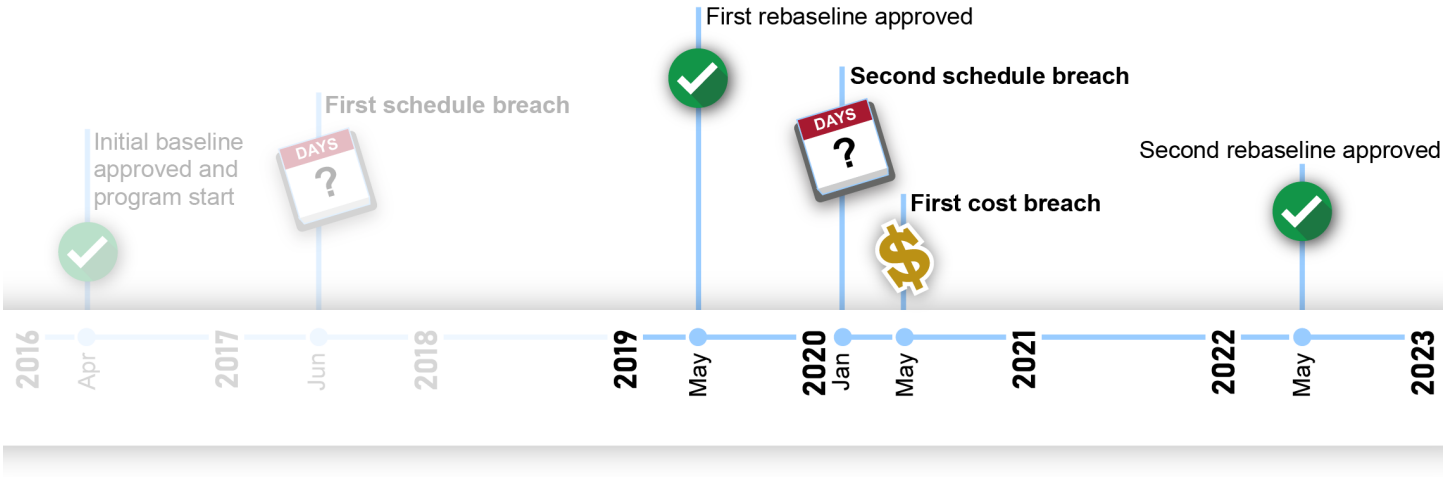
[29]According to the breach remediation plan, the 2020 schedule and cost breaches were due to a variety of factors, including technical challenges related to developing key HART subsystems, disagreements between OBIM and the contractor about the interpretation of certain functional requirements, and the technical approach for customer migration and biometric matching.

[30]According to HART program officials, the DHS Acquisition Review Board met and approved the rebaseline in April 2022. This approval was formally documented in a May 2022 acquisition decision memorandum.

years from the 2019 rebaseline, and at least 4 years from the original 2016 baseline. The HART program also significantly increased its development and operations and maintenance costs in the 2022 rebaselined estimate. Specifically, development costs are estimated to increase by $92 million, and the operations and maintenance costs are estimated to increase by $262 million, for a total increase of $354 million.

Figure 3 shows a timeline of HART's acquisition program baselines and breaches.

Figure 3: Timeline of Homeland Advanced Recognition Technology (HART) Acquisition Program Baselines and Breaches



Source: GAO (analysis of Department of Homeland Security data; icons). | GAO-23-105959

The HART Program Further Delayed the Schedule

The HART program's 2022 rebaseline extended the plan for delivering initial operational capability by at least 2 years from the 2019 rebaselined schedule. In addition, the 2022 rebaseline did not include an estimated time frame for completing the program. Program officials stated that they intend to develop the remainder of the program's schedule when the system is closer to initial operational capability. Table 1 shows the

changes that DHS made to the HART program schedule from 2019 to 2022.[31]

Table 1: Changes in the Homeland Advanced Recognition Technology's (HART) Program Schedule from 2019 to 2022

Milestone	Planned completion date[a] (as of May 2019)	Planned completion date[a] (as of May 2022)	Years/months delayed
Program start	April 25, 2016	April 25, 2016	0
Initial operational capability	December 31, 2020	September 30, 2023	2 years, 9 months
Complete increment 1	December 31, 2020	September 30, 2024	3 years, 9 months
Complete full program	June 30, 2024	Not yet planned	Unknown[b]

Source: GAO analysis of HART 2022 and 2019 acquisition program baselines. | GAO-23-105959

[a]This represents the schedule threshold dates defined in the HART acquisition program baseline.

[b]The 2022 rebaseline did not include an estimate for completing the program. As such, the number of years that this milestone has been delayed is unknown.

The schedule delays reflected in the 2022 rebaseline were due to several factors, such as expanding increment 1 to include, among other things, full performance testing, which was originally planned for completion in increment 2. Other factors for the delay were addressing technical challenges related to some of the key subsystems, such as an overly complex database structure, and changing the technical approach to run HART and legacy system operations in parallel for a longer period of time.

In response to the delays, in September 2021, program officials made a major modification to the primary HART development contract. This modification reallocated all resources to work on increment 1 in order to achieve initial operational capability and suspended all work associated with increment 2. OBIM officials decided to shift the remainder of the

[31]The HART program baseline includes schedule parameters from the master schedule. The schedule parameters establish both objective and threshold dates. Objective dates are the earliest feasible dates, based on acceptable risk that the milestones can occur. Threshold dates represent the latest feasible and acceptable dates the milestones can occur. Exceeding the threshold dates represents a schedule breach and requires a program to develop a breach remediation plan to identify corrective actions and a path forward.

originally planned increment 2 functionality into a later increment, referred to as the future capabilities increment.[32]

As a result, functionality such as the multimodal fusion has been deferred.[33] Specifically, this functionality was intended to be delivered in increment 2 by September 2021. However, since the schedule for future capabilities was not established in the 2022 rebaseline, multimodal fusion has been delayed for an indefinite amount of time.

More recently, since rebaselining in May 2022, the program has encountered additional challenges affecting the schedule. Specifically, in December 2022 program officials reported experiencing higher than expected software defects, security vulnerabilities, and performance issues. For example, in August 2022, program officials began operating HART in parallel with IDENT to test increment 1 in a live environment, which unveiled issues, such as system response times not being met.[34]

Moreover, in April 2023, program officials stated that they plan to again revise their approach for achieving initial operational capability. Officials attributed this decision to the ongoing challenges along with a decrease in fiscal year 2023 appropriations made available for HART.[35] Program officials stated that they are working with DHS leadership to define the path forward and update the schedule. They further stated that it is unlikely that they will achieve initial operational capability by September

[32]In August 2020, the program made a contract modification to address the technical challenges related to the development of increment 1 and decided to combine increments 3 and 4 into a single increment, referred to as future capabilities. In September 2021, the program made another modification to the contract to move increment 2 into the future capabilities increment.

[33]Multimodal fusion is intended to allow for the combining of information from multiple types of biometrics (such as fingerprint and iris pattern) to provide more efficient and accurate identification services and reduce the burden on examiners.

[34]During parallel operations, IDENT remains the official system of record and users continue to receive responses to their queries from IDENT. The queries are passed along to HART where program officials review the responses for consistency with IDENT and against required response times (e.g., retrieving an individual's identity in under 30 seconds).

[35]Joint explanatory statement of conference, 168 Cong. Rec. S7819, S8555 (daily ed. Dec. 20, 2022) (statement of Chair Leahy), specifically referenced in section 4 of the Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, § 4, 136 Stat. 4459 (2022).

2023. As a result, program officials stated that they needed to rebaseline HART's schedule for a third time.

Consequently, each time that the program has deferred initial operational capability, OBIM has needed to extend its support of the legacy system. However, IDENT has significant shortcomings that require DHS to make additional investments in the system to keep it operational much longer than planned. For example, the department plans to spend $155 million in fiscal year 2023 to continue IDENT system operations. As we reported in April 2023, the program has had to seek additional funding and reprioritized activities to address funding gaps.[36]

The HART Program Cost Estimate Increased Development and Operations Costs

HART significantly increased its development and operations and maintenance costs in the 2022 life cycle cost estimate. Specifically, when comparing these costs from the 2019 to 2022 estimates, development costs are estimated to increase by $92 million, and the operations and maintenance costs are estimated to increase by $262 million, for a total increase of $354 million.[37]

Key reasons for these cost increases include additional testing activities, supplementing the prime development contractor with additional engineers, additional software purchases, and updated maintenance projections. The program also incorporated additional costs to account for the ongoing need to satisfy known and unknown requirements when developing future capabilities.

It is important to note that, although the estimated development and operations and maintenance costs increased in the 2022 estimate, the total life cycle cost estimate of $2.63 billion is a decrease of $180 million from the 2019 estimate of $2.81 billion. This decrease was largely due to removing costs that were not specific to the HART program. For example,

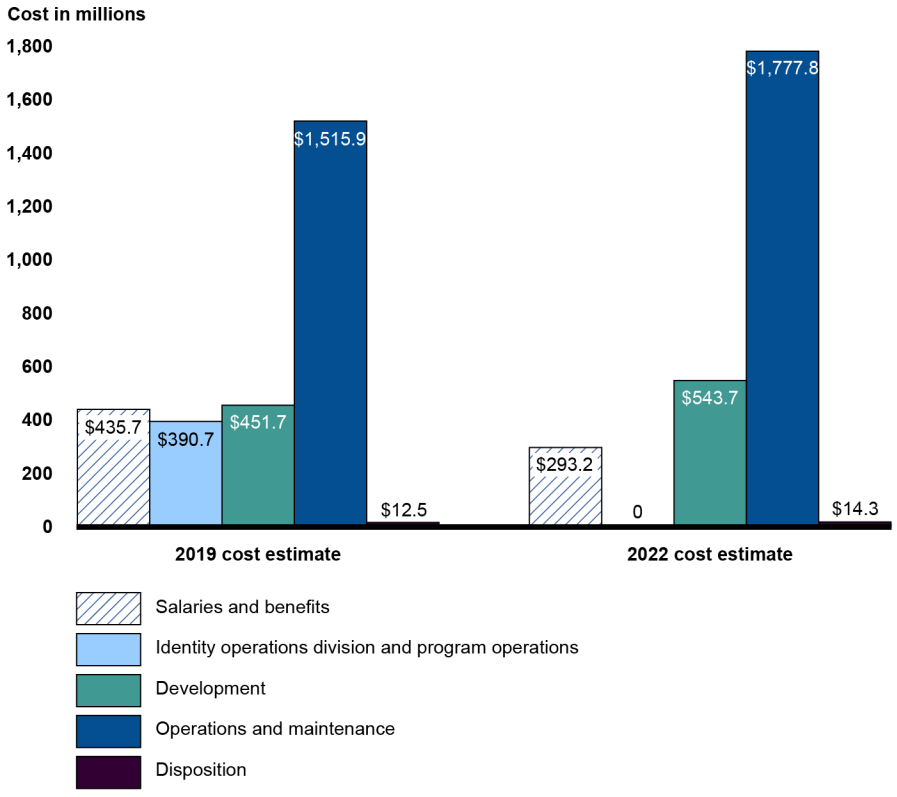
[36]GAO, *DHS Annual Assessment: Major Acquisition Programs Are Generally Meeting Goals, but Cybersecurity Policy Needs Clarification*, GAO-23-106701 (Washington, D.C.: Apr. 20, 2023). We reported that due to schedule delays and having to operate IDENT longer than planned, the program was not fully funded. Program officials said that in fiscal year 2022, the HART shortfall was addressed through reprogramming and the IDENT shortfall was addressed through a technical assistance package. To mitigate shortfalls in fiscal year 2023, program officials were seeking additional funding and reprioritizing activities as needed to align with existing funding, among other things.

[37]These figures are presented in base-year 2016 dollars at a 50 percent confidence level. The base-year is used as a constant dollar reference point to track program cost growth. Expressing an estimate in base-year dollars removes the effects of economic inflation and enables comparing separate estimates, such as the 2019 and 2022 HART cost estimates. All of the cost figures in this report section are represented in base-year dollars.

all costs associated with OBIM's Identity Operations Division and Program Operations, totaling $391 million, were removed from HART's 2022 program estimate. According to program officials, these costs are now captured in a separate OBIM office estimate.

Figure 4 identifies the changes to the HART program's life cycle cost estimate, as of May 2022.

Figure 4: Changes in the Homeland Advanced Recognition Technology (HART) Life Cycle Cost Estimate from May 2019 to May 2022



Source: GAO analysis of Department of Homeland Security data. | GAO-23-105959

Since updating the baseline life cycle cost estimate in May 2022, the program has incurred additional cost increases. Specifically, in August 2022 HART program officials stated that the program expected to reimburse the contractor for additional engineers needed to add capacity to complete development and test work. In addition, the program planned to utilize development teams supplied from another OBIM contract. Although each of these actions will result in added cost to the program

beyond the amount that had been approved in the 2022 life cycle cost estimate, as of February 2023, officials were unable to quantify the additional cost growth. Program officials stated that they will be unable to quantify the cost growth until after agreeing on a new approach for achieving initial operational capability.

HART Cost and Schedule Estimates Were Unreliable

OBIM developed unreliable cost and schedule estimates for the HART program that did not adhere to accepted practices. Specifically, the program's cost estimate did not substantially or fully meet any of the four characteristics of a reliable cost estimate. Moreover, the program's schedule estimate did not substantially or fully meet three of the four characteristics of a reliable schedule estimate.

OBIM's Cost Estimate for the HART Program Was Unreliable

Employing reliable cost estimates is crucial for realistic program planning, budgeting, and management. Cost estimates are necessary for government acquisition programs for many reasons, including to support decisions about funding one program over another, to develop annual budget requests, and to evaluate resource requirements at key decision points. Moreover, having a realistic estimate of projected costs makes for effective resource allocation, and it increases the probability of a program's success. According to the *GAO Cost Estimating and Assessment Guide*, the four characteristics of a high-quality, reliable cost estimate are that it is comprehensive, well-documented, accurate, and credible.

We determined that OBIM's cost estimate for the HART program was unreliable because it did not fully or substantially meet any of the four characteristics of a high-quality, reliable cost estimate. Specifically, the cost estimate partially met all four characteristics of a reliable cost estimate—comprehensive, well-documented, accurate, and credible. Table 2 summarizes our assessment of OBIM'S HART cost estimate compared to these characteristics, as of March 2022. Appendix II provides additional information on our cost assessment.

Table 2: Assessment of the Homeland Advanced Recognition Technology (HART) Program Cost Estimate Compared to Characteristics for a Reliable Cost Estimate Using *GAO's Cost Estimating and Assessment Guide*, as of March 2022

Cost estimating characteristic	GAO assessment
Comprehensive—The estimate should be comprehensive, including identifying all life cycle costs and basing the cost estimate on a technical baseline description that completely defines the program and reflects the current schedule.	**Partially met.** The HART life cycle cost estimate covered government and contractor costs from the beginning of the program's planning activities and was based on a work breakdown structure that included four cost categories. However, the estimate excluded some costs due to a lack of data and uncertain requirements that officials planned to further define as the program approached initial operational capability. For example, while the estimate included costs associated with future capabilities, the program had not defined the actual scope of the future capabilities to inform the associated cost estimates. In addition, the HART Cost Estimating Baseline Document, which served as the technical baseline description for the cost estimate, was outdated and did not reflect programmatic changes since April 2021. For example, the document, which was finalized in April 2021, did not incorporate new work associated with a major contract modification that was awarded in September 2021. Moreover, the assumptions defined in the cost estimate were not used to develop the sensitivity analysis.[a] Without fully accounting for life cycle costs, management will have difficulty successfully planning program resource requirements and making informed decisions. In addition, without analyzing the effects of an invalid assumption on the cost and schedule of a program, cost estimators and management will not have a full understanding of the effects of changing ground rules and assumptions.
Well-documented—The estimate should be well-documented, including showing the source data and the estimating methodology used to derive each element's cost. The estimate should also ensure data in the technical baseline documentation are consistent with data and assumptions in the cost estimate.	**Partially met**. The Office of Biometric Identity Management (OBIM) documented some of the estimating methodologies used to develop the cost estimate. For example, the HART cost estimate documentation stated that officials used methodologies such as parametric modeling (i.e., relying on statistical relationships between historical costs from other comparable programs) and engineering build-ups (i.e., estimating costs at the lowest level). However, there was insufficient detail provided about data sources used to make a judgment on data reliability. For example, while the supporting documentation provided an overall description of data sources used to generate the HART estimate, it did not include a discussion of data reliability. In addition, some of the technical data and assumptions in the cost estimate were inconsistent with the technical baseline documentation. Without fully documenting data sources used to inform the cost estimate, it will be difficult to update the cost estimate and provide a verifiable trace to a new cost baseline as key assumptions change during the course of the program's life. In addition, without ensuring technical data and assumptions are consistent with the technical baseline, the credibility of the cost estimate will suffer.

Cost estimating characteristic	GAO assessment
Accurate—The estimate should be accurate, including estimating each work breakdown structure element using the best methodology, and adjusting for inflation. The estimate should be updated regularly to reflect program changes, document the variances between planned and actual costs, and document lessons learned.	**Partially met**. The cost estimate built up program cost from low-level work breakdown structure elements. In addition, the HART program minimized mistakes by using a software tool to build out the cost estimate. However, large portions of the cost model were based on methodologies that were not fully documented. For example, the estimate relied heavily on subject matter expert opinion, which is a practice that should be limited. The expert opinion method should account for the possibility that bias influenced the result. However, the program did not document taking such steps in its methodology. In addition, the cost estimate did not properly adjust for inflation. For example, the program did not apply inflation to elements representing about 25 percent of the total estimated costs. Moreover, the cost estimate and supporting documentation did not include a discussion of variances between planned and actual costs or lessons learned from elements whose actual costs differed from the estimate. Without fully documenting all elements in the cost model, program management officials and oversight bodies cannot be certain that all cost estimate calculations are accurate and account for all costs. In addition, without properly adjusting for inflation, the HART estimate is at risk of overstating or understating the cost of the program. Lastly, without a documented comparison between the current estimate that is updated with actual costs and the old estimate, cost estimators cannot determine how well they are estimating and how the program is changing over time.
Credible—The estimate should be credible, including developing a sensitivity analysis, a risk and uncertainty analysis,[b] and cross-checks on major cost elements to validate results. The estimate should also be reconciled with an independent cost estimate.[c]	**Partially met**. HART program officials documented the results of a sensitivity analysis, as well as a risk and uncertainty analysis in the cost estimate. However, the risk and uncertainty analysis was applied inconsistently, resulting in an unreliable risk analysis. For example, for the HART capability support cost element, the program applied risk at both the input level (e.g., labor rate) and to the total cost which likely double counted risk. The program also did not demonstrate performing cross-checks of major cost elements to see if results were similar. In addition, the Cost Analysis Division did not generate an independent cost estimate for comparison with the HART program office's cost estimate because the Department of Homeland Security leadership did not require the division to prepare such an estimate. Instead, the division prepared an independent cost assessment, which identified recommendations for the program office to improve its estimate. However, some of the recommendations were not fully addressed. A poorly executed risk and uncertainty analysis gives HART program officials a false sense of security that all risks have been accounted for, which leads to decisions based on bad information. In addition, without employing cross-checks, the estimate will have less credibility because stakeholders will have no assurance that alternative estimating methodologies produce similar results. Moreover, a program estimate that has not been fully reconciled with an independent cost estimate or assessment has an increased risk of proceeding underfunded because it lacks unbiased assessment of whether the estimate can be achieved.

Legend: Met—OBIM provided complete evidence that satisfies the entire criterion; Substantially met—OBIM provided evidence that satisfies a large portion of the criterion; Partially met—OBIM provided evidence that satisfies about one-half of the criterion; Minimally met—OBIM provided evidence that satisfies a small portion of the criterion; Not met—OBIM provided no evidence that satisfies any of the criterion.

Source: GAO analysis of HART program cost estimate and supporting documentation. | GAO-23-105959

[a]A sensitivity analysis identifies a range of possible costs based on varying major assumptions, parameters, and data inputs. The analysis examines the effect of changing one assumption or cost driver at a time while holding all other variables constant.

[b]A risk and uncertainty analysis quantifies the risks and identifies the effects of changing key cost driver assumptions and factors. It uses statistical techniques to predict the probability of successfully executing a program within its budget by capturing the cumulative effect of program risks and uncertainty.

[c]An independent cost assessment is a non-advocate's evaluation of a cost estimate's quality and accuracy, looking at aspects such as the program's technical approach and risk, to ensure that the estimate captures all requirements. It may be used to determine whether the cost estimate reflects the program of record. It is not as formal as an independent cost estimate and does not have to be performed by an organization independent of the acquisition chain of command, although it usually is.

OBIM officials acknowledged that they were not fully or substantially addressing all of the characteristics of a reliable cost estimate. The officials explained that in some cases they were taking the appropriate estimating steps; however, they had not fully documented those steps in order to support the estimate. Officials stated they plan to update documentation supporting the HART life cycle cost estimate. However, they were unable to provide a time frame for completion, as they were in the initial phase of rebaselining the program, which will require the program to revise the cost estimate and associated documentation.

Until OBIM develops an updated cost estimate that fully meets the four characteristics of a reliable cost estimate, the office risks being unable to effectively estimate HART's future funding needs. It also risks using unreliable data to make budgetary decisions to hold the program accountable. As such, it faces an increased likelihood of cost overruns and unmet performance targets for the work associated with the remaining HART capabilities.

OBIM's Schedule Estimate for the HART Program Was Unreliable

The success of a program depends, in part, on having an integrated and reliable master schedule. The schedule provides not only a roadmap for project execution, but also the means by which to gauge progress, identify and resolve potential problems, and promote accountability at all levels of the program. Among other things, scheduling allows program management to decide between possible sequences of activities, determine the flexibility of the schedule according to available resources, predict the consequences of managerial action or inaction on events, and allocate contingency plans to mitigate risks. According to the *GAO Schedule Assessment Guide*, the four characteristics of a high-quality, reliable schedule are that it is comprehensive, well-constructed, credible, and controlled.

We determined that OBIM's schedule for the HART program was unreliable because it substantially met only one of the four characteristics of a reliable schedule estimate—being credible. The schedule partially met the remaining characteristics—being comprehensive, well-constructed, and controlled. Table 3 summarizes our assessment of the HART program's schedule compared to these characteristics, as of June 2022. Appendix III provides additional information on our schedule assessment.

Table 3: Assessment of the Homeland Advanced Recognition Technology (HART) Program Schedule Compared to Characteristics for a Reliable Schedule Using *GAO's Schedule Assessment Guide*, as of June 2022

Schedule estimating characteristic	GAO assessment
Comprehensive—The estimate should be comprehensive, including capturing all activities for managing the entire program and durations of all activities based on a realistic reflection of how long each activity will take. The schedule should also assign resources for the activities and allocate them to determine whether they will be available when needed.	**Partially met.** The HART integrated master schedule included government, contractor, and subcontractor activities through increment 1. Officials also established project activity durations. However, the HART schedule did not include activities beyond increment 1, such as all the development and implementation of work associated with future capabilities. In addition, most activities in the schedule (approximately 98 percent) did not include resource assignments. If the schedule does not fully and accurately reflect the program, it will not be an appropriate basis for analyzing or measuring technical work accomplished and may result in unreliable completion dates, time extension requests, and delays. Moreover, without accurate and complete resource assignments, management's ability to monitor productivity, allocate unused resources, and monitor resource-constrained activities is limited.
Well-constructed—The estimate should be well-constructed, including accommodating a reasonable amount of float, confirming that the critical path is valid and includes all the activities that drive the program's earliest completion date, and sequencing all activities to ensure that each activity includes predecessor and successor logic.	**Partially met.** The schedule accommodated a reasonable amount of time an activity can slip before the program's end date is affected (i.e., float). For example, of the 554 remaining HART tasks set to occur as soon as possible, the majority had a reasonable amount of float of 50 or fewer days. In addition, the critical path for the HART program included activities that drive the program's earliest completion date. However, the critical path we independently calculated within the schedule included three activities that did not appear on the path submitted by program officials. Moreover, the schedule was not properly sequenced. For example, 10 percent of activities were not able to start before a set date, even if their predecessors were complete (i.e., unjustified date constraints). Without a fully defined critical path based upon sound schedule logic, the program may be relying on an unrealistic or overly aggressive plan that cannot predict the impact changes in the program such as delayed activities, scope changes, and the effect of risk events. In addition, date constraints prevent activities from responding dynamically to changes in the program, including actual progress and availability of resources.
Credible—The estimate should be credible, including horizontal and vertical traceability.[a]	**Substantially met.** Program officials reported that they performed a 15-point check on the schedule logic to ensure that the schedule could be horizontally and vertically traced. We tested the horizontal and vertical traceability of the schedule and found the schedule generally responded to our manipulation as expected.
Controlled—The estimate should be controlled, including regularly updating the schedule and using actual progress and logic to realistically forecast dates for program activities. The scheduler should also maintain a baseline schedule to measure and report performance and variances from the plan.	**Partially met.** Program officials stated that the contractor's scheduler meets with government staff responsible for schedule activities to review and update the schedule based on progress. The HART program also compared performance and identified variances from the current schedule. However, updates to the activities in the schedule were not always logical. For example, we found 50 activities completed out of sequence, including two activities starting before their predecessors. Moreover, although program officials stated that they measure performance against the baseline, they did not report trends in performance over time. If changes are not controlled and fully documented, performance cannot be accurately measured against the original plan. Undocumented or unapproved changes will hamper performance measurement and may result in inaccurate variance reporting, inconsistent stakeholder versions of the same plan, and unreliable schedule data.

Legend: Met—The Office of Biometric Identity Management (OBIM) provided complete evidence that satisfies the entire criterion; Substantially met—OBIM provided evidence that satisfies a large portion of the criterion; Partially met—OBIM provided evidence that satisfies about one-half of the criterion;

Minimally met—OBIM provided evidence that satisfies a small portion of the criterion; Not met—OBIM provided no evidence that satisfies any of the criterion.

Source: GAO analysis of HART program schedule and supporting documentation. | GAO-23-105959

[a]Horizontal traceability demonstrates that the overall schedule is rational, has been planned in a logical sequence, accounts for the interdependence of detailed activities and planning packages, and provides a way to evaluate current status. Vertical traceability demonstrates the consistency of dates, status, and scope requirements between different levels of a schedule—summary, intermediate, and detailed.

OBIM officials acknowledged that the HART integrated master schedule did not fully or substantially address all of the characteristics of a reliable schedule. They explained that DHS and OBIM do not require the program to perform some of the best practices that comprise the four characteristics.

Until OBIM revises the HART program's schedule to follow the four characteristics of a reliable schedule, it runs the risk of additional delays as it works to implement the remainder of the program. Further, until OBIM updates the schedule estimate to account for the total time needed to fully implement the remaining effort, department leadership will be limited in its ability to make informed decisions regarding the program's future. Such uncertainty can cause schedule slippages and increased program costs.

DHS Did Not Fully Implement a Majority of Selected Privacy Requirements for HART

OMB established privacy protection requirements for federal agencies to manage federal information resources that involve PII.[38] These requirements include, but are not limited to, following approved records retention schedules, imposing conditions on shared PII, and implementing a risk management framework to manage privacy risks. In addition, OMB established guidance on implementing the privacy provisions of the E-Government Act, including conducting a PIA to analyze how personal information is collected, stored, shared, and managed in a federal system.[39]

Lastly, OMB also issued guidance that outlines the role and designation of agencies' Senior Agency Official for Privacy (SAOP). In particular, it

[38]OMB, Circular A-130.

[39]OMB, Memorandum M-03-22 and Pub. L. No. 107-347, § 208, 116 Stat. at 2921.

describes the position, expertise, and authority the SAOP should have, and it provides details on the official's responsibilities.[40]

DHS did not fully implement a majority of the selected federal privacy requirements to ensure the protection of PII in the HART program. Specifically, of the 12 selected OMB privacy requirements, the department fully implemented five and partially implemented seven. Table 4 describes the selected requirements and provides our assessment of the HART program's implementation of these requirements.

Table 4: Summary of Department of Homeland Security's (DHS) Implementation of Selected Office of Management and Budget Privacy Requirements for the Homeland Advanced Recognition Technology (HART) Program

Privacy requirement	GAO assessment
Review and approve the system security categorization. The Senior Agency Official for Privacy (SAOP), or other delegated officials, shall review and approve the categorization (e.g., low, moderate, or high-impact) of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII).[a]	●
Establish a required security categorization level for shared PII. Agencies that share PII shall require, as appropriate, other agencies and entities with which they share this information, to maintain the PII in a system with a particular categorization level.	●
Incorporate privacy requirements in contracts. Agencies shall ensure contracts incorporate privacy requirements.	●
Encrypt moderate-impact and high-impact information. Agencies shall encrypt all moderate-impact and high-impact information at rest and in transit.[a]	●
Implement a privacy control selection process. Agencies shall employ a process to select and implement from 26 privacy controls that the National Institute of Standards and Technology specified for information systems and programs.[b] Among other things, these privacy controls relate to minimization of PII, responding to a privacy incident, and sharing information with third parties.	●
Conduct a privacy impact assessment (PIA). Agencies shall conduct a PIA to ensure that the handling of PII conforms to applicable privacy requirements. A PIA is intended to identify and evaluate ways to mitigate privacy risks. Among other things, the PIA should describe the intended use of the information being collected, what information will be collected, with whom the information will be shared, and how the information will be secured. In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. The PIA also serves as notice to the public regarding agencies' practices with respect to privacy.	◑

[40]OMB guidance states that at the discretion of the SAOP and consistent with applicable law, other qualified agency personnel may perform privacy functions that are assigned to the SAOP. In all cases, this senior official will retain responsibility and accountability for the agency's privacy program. OMB, Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (Washington, D.C.: Sept. 15, 2016). DHS has designated its Chief Privacy Officer as the SAOP.

Develop a privacy plan and control assessment methodologies. Agencies shall develop and maintain a privacy plan that describes the privacy controls selected for an information system and how the controls have been implemented. In addition, the agency should describe the planned methodologies that will be used to assess whether the privacy controls are implemented correctly and operating as intended.	◑
Assess privacy controls. The SAOP (or other delegated officials) shall conduct and document the results of privacy control assessments prior to the operation of an information system and periodically thereafter to verify their continued effectiveness and to ensure compliance with applicable privacy requirements and manage privacy risks.	◑
Correct privacy-related deficiencies. Agencies shall correct deficiencies that are identified through privacy assessments and use corrective action plans to manage their remediation.	◑
Review the system authorization package. The SAOP (or other delegated officials) shall review authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to ensure compliance with applicable privacy requirements and manage privacy risks. The packages should be reviewed prior to authorizing officials making risk determination and acceptance decisions. At a minimum, the authorization package should include the system security and privacy plan, security and privacy control assessment, and any relevant corrective action plans.	◑
Impose conditions on shared PII through agreements. Agencies shall impose conditions that govern, among other things, use, disclosure, and disposal of shared PII, through written agreements.	◑
Follow records retention schedules. Agencies shall ensure that all records with PII are maintained and disposed of in accordance with applicable schedules that document the period of time that agencies should retain records (called records retention schedules).	◑

Legend: ● = Fully implemented: evidence demonstrated implementation of all aspects of the requirement; ◑ = Partially implemented: evidence demonstrated implementation of some, but not all of the requirement; ○=Not implemented: evidence did not demonstrate implementation of any aspect of the requirement

Source: GAO analysis of HART privacy documents. | GAO-23-105959

[a]The National Institute of Standards and Technology Federal Information Processing Standards Publication 199 dictates that a system's security categorization is expressed as either low, moderate, or high-impact. The categorization is based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. National Institute of Standards and Technology, *Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems* (Gaithersburg, Md.: February 2004).

[b]OMB Circular A-130 describes privacy controls as the administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks. In April 2013, the National Institute of Standards and Technology developed its fourth revision of the Special Publication on Security and Privacy Controls for Federal Information Systems and Organizations, which includes 26 privacy controls for agencies to implement. Although a fifth revision was issued in September 2020, the fourth revision was used as criteria because DHS had not yet implemented the fifth revision. National Institute of Standards and Technology SP 800-53, Revision 4: *Security and Privacy Controls for Federal Information Systems and Organizations* (Gaithersburg, Md.: April 2013, withdrawn Sept. 23, 2021).

The five privacy requirements that the department fully implemented represent important steps toward protecting PII that will be matched, stored, and shared by HART. For example, the Senior Director for Privacy Compliance reviewed and approved the system security categorization of the HART system. In addition, OBIM documented the required security categorization level for entities that HART shares data with in interconnection security agreements. The office also included

privacy requirements in applicable contracts and demonstrated that HART data are encrypted at rest and in transit. Further, the DHS Privacy Office selected and documented the implementation for all 26 privacy controls established by the National Institute of Standards and Technology.

The following summarizes the seven privacy requirements that were partially implemented.

- **Conduct a privacy impact assessment – partially implemented.** DHS Privacy Office officials conducted a PIA of HART and published it in February 2020. Among other things, the PIA described the intended use of the information being collected. For example, the assessment stated that OBIM uses these data to match, store, and share results as permitted to support national security, employment credentialing, law enforcement, immigration, and intelligence. The assessment also analyzed and described how the information will be secured in HART through the use of a robust set of access controls. In addition, Privacy Office officials reviewed the published PIA in December 2021 and determined that no updates were necessary at that time.[41]

  However, although the assessment analyzed and described most types of information that will be stored in the system, it did not describe the categories of individuals' information whose data will be stored in HART. Specifically, the assessment did not disclose whether the system will be collecting and storing foreign nationals' data, U.S. citizens' data, or both. OBIM officials stated that, because the assessment names particular programs which use U.S. citizen data, readers of the PIA should be able to infer that U.S. citizen data will be stored in HART.[42]

  However, this approach puts the onus on the public to know the purpose of the relevant programs and associated systems to understand if U.S. citizen data will be stored in the system. This is important because the statutory privacy rights and protections specified in the Privacy Act of 1974 apply to U.S. citizens and lawful

[41]The DHS Senior Director for Privacy Compliance conducted this review when the department consolidated the HART production and test environments.

[42]Examples of such programs referenced by the PIA include TSA PreCheck, Domestically Filed Intercountry Adoption Applications and Petitions, and Transportation Worker Identification Credential.

permanent residents,[43] whereas they do not always apply to foreign nationals. Officials stated that they will include this information in the next HART PIA. As of May 2023, OBIM officials stated that they were coordinating with the Privacy Office to determine the best time frame for updating the HART PIA, but did not provide an estimated completion date.

In addition, although the HART PIA identified 18 entities that these data will be shared with, the list was incomplete.[44] This is contrary to DHS's PIA guidance, which requires that the assessments identify the names of the federal agencies and foreign governments with which a system shares information. Specifically, the PIA omitted several partners, such as the Office of Personnel Management, Germany, and Croatia.

DHS officials acknowledged that certain partners may not be reflected in the PIA because they were added after the document was published in 2020. Officials stated that they will incorporate new partners into the PIA when it is next updated. However, as previously mentioned, OBIM did not provide an estimated completion date for incorporating the updates.

As such, until the Privacy Office establishes and implements a timeline for incorporating these important updates in the PIA, the public will not be fully aware of whether their information is stored in HART and with whom their information is shared.

- **Develop a privacy plan and control assessment methodologies – partially implemented.** The HART system security plan includes a privacy plan. This privacy plan describes the 26 privacy controls and 63 associated sub-elements. The plan also discusses how the controls will be implemented. For example, to implement a control related to privacy awareness and training, the HART plan states that employees handling sensitive PII should receive role-based training.

  Regarding assessment methodologies, the DHS Privacy Office documented methods for a limited portion of the controls. Specifically, for eight of the 63 privacy control sub-elements, the office documented the steps the office planned to take to determine whether the control

[43]5 U.S.C. § 552a.

[44]These 18 entities include DHS component users, such as the U.S. Customs and Border Protection and the Transportation Security Administration, as well as agencies such as the Department of Justice and Department of State.

was implemented correctly or operating as intended. For example, to assess implementation of a control related to privacy requirements for contractors and service providers, the office documented that it plans to review and approve sections of the contracts to ensure all privacy language is included.

However, contrary to OMB's guidance, the Privacy Office did not clearly describe planned methodologies for assessing the implementation for each of the remaining 55 privacy control sub-elements. Privacy Office officials stated that they did not believe describing planned assessment methods was necessary.

Without documented assessment methods for each control, there is a lack of transparency regarding what steps the office took (or plans to take) to determine whether a control was (or will be) implemented correctly. Further, without documented methods, the process will not be repeatable for new staff who may be responsible for future assessments of the privacy controls. Until the Privacy Office ensures that detailed methodologies are defined for the HART program, the department risks assessing privacy controls incorrectly or having controls that do not work as intended.

- **Assess privacy controls – partially implemented.** Delegated privacy office officials conducted an initial assessment of the privacy controls for the HART system. Privacy Office officials stated that they assessed the controls through their review and approval of privacy compliance documentation, including the PIA, privacy threshold analysis, and system of records notices. Following the approval of the PIA in February 2020, the office documented the results of its assessment of the controls as implemented. In addition, Privacy Office officials stated that they reassessed the implementation of the privacy controls when the office reviewed and updated the privacy threshold analysis in December 2021.

  In addition to taking these actions, DHS also planned to assess the continued effectiveness of the privacy controls by initiating a privacy compliance review within 1 year of completing the PIA (by February 2021). However, as of May 2023, the privacy office had not completed this privacy compliance review and it was 2 years overdue. Privacy Office officials stated that they had initiated the compliance review, but paused it due to difficulty filling a vacancy gap in the Director of Oversight position whose responsibility was to conduct the review. As of May 2023, the position remained vacant, but DHS was actively conducting an applicant screening process.

Nevertheless, until the office prioritizes developing and implementing a timeline for completing the planned privacy compliance review, DHS will not have taken the steps necessary to help ensure that the program's privacy controls are effective.

- **Correct privacy-related deficiencies – partially implemented.** The DHS Privacy Office identified 13 deficiencies and made recommendations to OBIM to remediate them in a February 2020 PIA. OBIM officials reported completed or planned actions for addressing six of the 13 deficiencies. For example, the Privacy Office identified that OBIM did not regularly confirm that the information that HART shares is consistent with the data provider's requirements. In response, OBIM reported that the office plans to conduct periodic reviews to ensure that any new or existing information sharing rules are consistent with the data provider's requirements.

  However, as of May 2023, OBIM has not demonstrated that it had addressed or established corrective action plans to address the remaining seven deficiencies. Privacy Office officials stated that they are not actively monitoring the status of these deficiencies due to staff vacancies. Nevertheless, without ensuring that OBIM has fully addressed the remaining seven privacy deficiencies or has corrective action plans in place to do so, OBIM is in jeopardy of leaving some privacy risks unaddressed.

- **Review the system authorization package – partially implemented.** The DHS Privacy Office reviewed some of the documents comprising the HART authorization package, including the December 2021 privacy threshold analysis and the February 2020 PIA. However, the office did not review other parts of the package, such as the security control assessment.

  Privacy Office officials stated that they reviewed only those artifacts that are applicable to privacy and that they are not required to review the other artifacts, such as the security control assessment. However, this is contrary to OMB's guidance, which states that the SAOP (or other delegated official) has a responsibility for reviewing the authorization package for information systems to ensure that privacy risks are managed prior to system authorization.[45] In addition, these other documents within the package that privacy officials did not

[45]OMB Circular A-130 defines the authorization package as including the system security and privacy plan, security and privacy control assessment, and any relevant corrective action plans.

review address security controls that are of particular importance to protecting PII (e.g., remote access, authentication, and encryption).[46]

Finally, in September 2022, we recommended that DHS fully define and document the role of the SAOP or other designated privacy official in reviewing authorization packages.[47] However, as previously mentioned, as of May 2023, the department had not taken steps to implement this recommendation. Until the appropriate privacy official reviews all documentation associated with the HART authorization package, the system will lack sufficient oversight for all controls related to privacy. Privacy officials may also fail to identify potential privacy risks or deficiencies.

- **Impose conditions on shared PII through agreements – partially implemented.** OBIM and its predecessor established information sharing and access agreements with entities which the IDENT system (and HART once deployed) shares PII.[48] OBIM officials stated that these agreements contain conditions for shared PII. However, the information sharing and access agreements we reviewed did not consistently address seven key conditions for protecting PII (i.e., use, disclosure, retention and disposal, correction and redress, data sensitivity, authority for sharing, and privacy).

  Specifically, OBIM provided two lists that collectively identified 111 agreements. Of the 18 selected agreements we reviewed, only six contained all seven conditions. The remaining 12 agreements did not consistently address each of the conditions. For example, three

[46]DHS established guidance that identifies specific National Institute of Standards and Technology security controls that should be implemented for privacy sensitive systems that permit remote access to PII, such as HART. For example, the guidance requires all privacy sensitive systems to implement security controls related to remote access and authenticator management to ensure that remote access to PII is appropriately protected. The guidance also requires that the SAOP approves cases where these required security controls cannot be implemented. DHS, *4300A Sensitive Systems Handbook, Attachment S, Compliance Framework for Remote Access to and Extracts from Privacy Sensitive Systems, Version 11.0* (Washington, D.C.: Aug. 5, 2014).

[47]GAO, *Privacy: Dedicated Leadership Can Improve Programs and Address Challenges*, GAO-22-105065 (Washington, D.C.: Sept. 22, 2022).

[48]OBIM was formerly known as the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program. US-VISIT was established in 2003 to provide U.S. visa-issuing posts and ports of entry with the biometric technology that enabled the U.S. government to establish and verify identities. In 2013, pursuant to the Consolidated and Further Continuing Appropriations Act, 2013, Pub. L. No. 113-6, 127 Stat. 198, 356 (2013) Congress replaced funding for US-VISIT's biometric identity management functions with funding for the newly created OBIM.

agreements did not address the condition related to the use of PII, and three agreements did not address the condition related to the disposal of PII.

The missing conditions were due, in part, to the age of certain agreements. Specifically, over half of the agreements were established before 2010 when DHS issued guidance on the required contents and conditions that should be included in the information sharing and access agreements. Officials from OBIM and the DHS Office of Strategy, Policy, and Plans recognized that these agreements may not always include all of the required conditions in the guidance.[49] In February 2023, the policy officials stated that the Office of the Chief Information Officer is working on updating the information sharing and access agreement guidance, and once updated the policy officials will begin work on updating the agreements to be consistent with the new guidance.

As of May 2023, the department expected to complete a draft of the revised information sharing and access agreement guidance by September 2023 and publish a final version by January 2024. If DHS updates each of the information sharing and access agreements that were missing the required conditions, as planned, it will provide the department with greater assurance that HART partners are consistently applying appropriate privacy conditions for shared PII.

In addition to missing conditions for protecting PII in the agreements, OBIM does not maintain a reliable inventory of these agreements. Specifically, while a key characteristic of data reliability includes completeness, OBIM's lists identifying 111 information sharing and access agreements were incomplete. The lists did not clearly identify agreements for each of OBIM's approximately 140 partners. For example, according to the lists, the Office of Personnel Management and the Department of Justice's Bureau of Prisons do not appear to have agreements with OBIM.

OBIM officials stated that the reason that some partners do not appear to be covered by a sharing agreement is because some agreements cover multiple partners. For example, officials stated that the Office of Personnel Management's and the Bureau of Prisons' information sharing with HART is covered by an agreement between

[49]With regard to information sharing and access agreements, DHS Office of Strategy, Policy, and Plans officials have stated that their office supports DHS components with their data sharing requirements and leads the coordination, drafting, and updating of department-level sharing arrangements where multiple components are responsible parties.

DHS, the Departments of State and Justice, and OBIM. However, there is no traceability that shows that this agreement covers the bureau and the office. In addition, OBIM's lists did not specify this arrangement for either of these partners. As such, the lists lack critical information to ensure that OBIM has a complete inventory of agreements that cover all partners.

In February 2023, officials from the Office of the Chief Information Officer stated that they developed an inventory system for sharing agreements, which is available for DHS components to access. In May 2023, DHS officials stated that OBIM was reviewing the technical capabilities of the system to determine if it would meet the office's needs for maintaining HART's agreements. However, they did not provide a timeline for determining next steps. Until OBIM establishes and implements a timeline for maintaining a reliable inventory of information sharing and access agreements for HART, the office will be limited in its ability to ensure that appropriate conditions are imposed on partners to protect PII.

- **Follow records retention schedules – partially implemented.** OBIM issued guidance that all partners that provide data are responsible for the retention and disposal of the records that they provide to HART in accordance with their retention schedules. Specifically, these data providers must use HART services to delete records in the system.[50]

  HART records containing PII are subject to varying retention periods depending on the data providers' retention schedules. For example, U.S. Citizenship and Immigration Services data entered into HART regarding adoption application processing should be disposed of after 50 years.

  However, OBIM does not take steps to verify that data providers appropriately dispose of records containing PII in HART. While OBIM officials stated that the office has the ability to create reports to assist partners in determining adherence to the records retention schedule, it does not require its partners to request such reports from OBIM on a recurring basis to ensure that PII is appropriately disposed of from the system. OBIM officials also stated partners have not requested such reports for this use.

[50]Using the HART service known as "delete encounter," data providers can submit a request for the system to delete their records in accordance with the applicable retention schedule. The data providers may also send OBIM a list of records for the office to delete.

Given the large number of partners that provide data to HART (approximately 140), and varying retention periods for the vast quantity of PII stored in the system, there is a risk that the partners will not appropriately dispose of PII. As such, until OBIM establishes and maintains a process for ensuring that these partners have used HART services to appropriately delete PII from the system, the office risks retaining PII in the system longer than the scheduled retention period, which could potentially compromise individuals' privacy.

Conclusions

DHS's reliance on the 29-year-old biometric identity management system to support national security, law enforcement, and immigration decisions, emphasizes the critical need for OBIM to avoid further delays, cost overruns, and performance issues. However, the program's repeated cost and schedule baseline breaches since 2017 have prolonged DHS's and its partners' dependency on IDENT for at least 4 years beyond the original plan. In addition, HART's development and operations costs have grown by at least $354 million.

OBIM's schedule and cost shortcomings for HART reflect its lack of alignment with important cost and schedule estimation best practices. Specifically, OBIM's lack of reliable cost and schedule estimates increases the risk that management will not have the information necessary for effective decision-making. Further, until the significant weaknesses in the cost and schedule estimates are addressed the office risks further cost overruns and schedule delays. These risks are especially concerning as the program is in its seventh year and has yet to achieve initial operational capability.

While HART promises to deliver benefits, deploying the modernized system will increase privacy risks as OBIM plans to store additional kinds of biometrics (e.g., DNA) and anticipates continued growth in users and identities stored in HART. DHS has taken important steps to fully implement five of the 12 selected privacy requirements; however, the gaps in the remaining seven requirements reduce HART's ability to appropriately protect individuals' PII. As such, until OBIM addresses weaknesses in HART privacy protections, such as the missing information in the PIA and the lack of assurances in partners' adherence to records retention schedules, the office may develop a system that puts individuals' PII at increased risk for compromise.

Recommendations for Executive Action

We are making nine recommendations to DHS:

The Secretary of DHS should direct the OBIM Director to update the cost estimate for the HART program to account for all costs and incorporate

the best practices called for in the GAO *Cost Estimating and Assessment Guide*. (Recommendation 1)

The Secretary of DHS should direct the OBIM Director to revise the schedule estimate for the HART program that incorporates the best practices called for in the GAO *Schedule Assessment Guide*. (Recommendation 2)

The Secretary of DHS should direct the OBIM Director to coordinate with the Privacy Office to establish and implement a timeline for updating the HART PIA to fully describe the categories of individuals whose data will be stored in HART and the partners with whom the system shares information. (Recommendation 3)

The Secretary of DHS should direct the Privacy Office to describe planned methodologies for determining that all privacy controls are implemented correctly and operating as intended for future control assessments of the HART program. (Recommendation 4)

The Secretary of DHS should direct the Privacy Office to develop a timeline for completing the planned HART privacy compliance review. (Recommendation 5)

The Secretary of DHS should direct the OBIM Director to coordinate with the Privacy Office to establish and implement plans for correcting seven remaining privacy deficiencies identified in the HART PIA. (Recommendation 6)

The Secretary of DHS should direct the Privacy Office to ensure the complete HART authorization package is reviewed by the office prior to future system authorizations. (Recommendation 7)

The Secretary of DHS should direct the OBIM Director to establish and implement a timeline for maintaining a reliable inventory of information sharing and access agreements with partners that share data with HART. (Recommendation 8)

The Secretary of DHS should direct the OBIM Director to establish and maintain a process for ensuring that partners that provide data to HART have used the system's services to help to appropriately dispose of PII from the system, in accordance with applicable records retention schedules. (Recommendation 9)

Agency Comments and Our Evaluation

We provided a draft of this report to DHS for review and comment. The department provided written comments, which are reprinted in appendix IV. In its comments, DHS concurred with all nine of our recommendations and provided estimated completion dates for implementing four of them.

DHS also provided additional considerations related to recommendations 1, 2, and 4. Specifically, regarding recommendations 1 and 2, the department stated that it has made some improvements related to cost and schedule estimation that we did not reflect in the report. For example, DHS stated that in January 2023 OBIM initiated improvements to its application of risk and updated supporting documentation to include actual source data when actuals are updated in the estimate. In addition, among other things, the department stated that in December 2022, it updated the HART schedule to clearly distinguish tasks assigned to federal employees and contractors.

We did not reassess the cost and schedule estimates based on these reported improvements because the updates had not been approved by DHS leadership. Instead, we reviewed the June 2022 program schedule because it served as the basis for the HART program's most recent acquisition program baseline, which was reviewed and approved by DHS leadership. We will reassess the reliability of the program's cost and schedule estimates, including the actions taken to address our recommendations, once the program establishes its new baseline and the estimates receive approval from DHS leadership.

In addition, while DHS concurred with recommendation 1, the department indicated that it disagrees with our ratings for three of the 18 best practices within of our cost assessment. Specifically, DHS stated that these three practices should have been rated as "substantially met" instead of "partially met." However, we maintain that the assessments are accurate for each of the three following areas.

- The department stated the best practice of "documented all cost-influencing ground rules and assumptions" within the cost estimating characteristic of "comprehensive" has been substantially met. Specifically, DHS stated that the cost estimate inputs had risk assumptions aligned to the ground rules and that the estimate was used to run a sensitivity analysis.

  However, we found that while OBIM did have risk assumptions for cost elements in the estimate, instead of using these assumptions to develop a sensitivity analysis as described in the GAO Cost Guide, it

used a predetermined sensitivity range of possible costs without considering the unique risk assumptions of each cost element. As a result, management lacked insights into the linkage between the technical baseline parameters, assumptions, and cost model inputs that informed the sensitivity analysis. This inhibits management's ability to make well-founded decisions.

- The department also stated the best practice of "adjusted for inflation" within the cost estimating characteristic of "accurate" has been substantially met. Specifically, the department stated that the HART program did not use standard inflation on some cost elements due to the existence of negotiated costs or where inflation was already incorporated into the cost for that item. DHS stated that this was done to avoid applying an inflation factor twice.

  However, as previously discussed with OBIM officials, cost estimates should be prepared in base-year dollars to eliminate the distortion that would otherwise be caused by overall price-level changes. This requires the transformation of historical or actual cost data into base-year dollars. If data are not properly normalized, the data set may be inconsistent with other data used in the estimate and the effects of external inputs may not be removed.

- DHS stated the best practice of "updated regularly to reflect program changes and actual costs" within the cost estimating characteristic of "accurate" has been substantially met. DHS stated that it entered actual costs into the estimate as they become available. In prior discussions, OBIM stated that it intended to update its documentation to identify sunk costs when updating the estimate. We agree that this would be an acceptable approach when DHS prepares the revised cost estimate to support a new program baseline.

  In additional comments on our cost estimate analysis, the department stated that the DHS Cost Analysis Division developed an Independent Cost Assessment and it does not intend to conduct an Independent Cost Estimate of the HART program. As we discussed with DHS officials, conducting an Independent Cost Assessment would have been considered an acceptable alternative to an Independent Cost Estimate if we had found that the issues in the assessment were fully addressed. However, OBIM did not demonstrate that it had fully addressed the issues related to risks and subjectivity, or implemented the associated recommendations.

  With regard to recommendation 2, while DHS concurred with the recommendation, it disagreed with our rating for one of the 10 best practices within our schedule assessment. Specifically, the

department stated the best practice “confirmed that the critical path is valid and included all activities that drive the program’s earliest completion date” within the schedule estimating characteristic of “well-constructed,” has been substantially met. The department stated that OBIM’s schedule update process accounts for differences in calculating the critical path and attested that there was not an issue with the critical path provided to us.

However, as discussed with DHS, our analysis showed that there were additional problems with the critical path. Specifically, there were lags and constraints on tasks on the critical path and it was unclear if the critical path contained level of effort tasks. Unless the schedule is fully horizontally traceable, the effects of delayed activities on successor activities cannot be determined. Further, level of effort activities should not drive the schedule.

In additional comments on recommendation 2, DHS stated that the HART program is meeting the intent of the assigning resources scheduling best practice through its Agile processes. The department added that this process provides the program manager greater insight into resource allocations and issues as the lower level requirements are tracked. For these reasons, DHS did not add resource-loading into the HART schedule.

However, we found that while the program had listed a government point of contact for some tasks in the schedule, this was not the person or people actually responsible for conducting the work for each of the tasks. In addition, the program did not demonstrate assigning and monitoring resources through its Agile processes. Resources must be considered in the creation of a schedule because their availability directly affects an activity’s duration. Further, if the schedule does not have resource assignments, management’s ability to monitor productivity, allocate idle resources, monitor resource-constrained activities, and level resources across activities is severely limited.

Lastly, with regard to recommendation 4, while DHS stated that it concurs with the recommendation, it requested that we consider the recommendation resolved. Specifically, the department stated that the Privacy Office described planned privacy control assessment methodologies. DHS noted that the implementation statements for each privacy control in the HART System Privacy Plan described how a control was implemented or assessed.

However, we disagree that the office took steps to clearly document its planned methodologies for determining if they were implemented

correctly or operating as intended. Specifically, 87 percent (i.e., 55 of the 63) of the privacy control sub-elements did not have documented planned methodologies prior to being assessed. Documenting methodologies for assessing privacy controls is essential to ensure that DHS can determine if these controls were properly implemented for HART.

In addition to the aforementioned comments, we received technical comments from DHS, the Transportation Security Administration, U.S. Customs and Border Protection, and OBIM officials, which we incorporated, as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Homeland Security, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-5017 or cruzcainm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.

Marisol Cruz Cain
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) determine how the Homeland Advanced Recognition Technology (HART) program has changed since the 2019 baseline, (2) assess the extent to which the HART program's cost and schedule estimates followed best practices, and (3) assess the extent to which the Department of Homeland Security (DHS) implemented selected privacy requirements for the HART program.

To address the first objective, we reviewed HART planning documentation, such as schedule and cost estimates and the associated acquisition program baselines, to describe the schedule and cost changes that HART experienced since 2019. Specifically, we compared the schedule estimates supporting the 2019 and 2022 acquisition program baselines. To identify changes in cost, we compared the HART life cycle cost estimates supporting the May 2019 and May 2022 acquisition program baselines. In addition, we reviewed relevant documentation, such as monthly oversight meeting minutes, to describe changes to the program since the May 2022 baseline. Lastly, we interviewed HART program office officials regarding changes in the program schedule and cost.

To address the second objective, we reviewed the HART program's cost and schedule estimates dated March 2022 and June 2022, respectively, and related documents describing HART's cost and schedule estimation practices.[1]

- To assess HART's cost estimate, we evaluated documentation supporting the estimate, such as the cost estimating baseline document, which defined the program's technical approach, and the program's risk register, which informed the risk and uncertainty analysis. We assessed this documentation against best practices identified in *GAO's Cost Estimating and Assessment Guide*.[2] These best practices map to the four characteristics of a high-quality, reliable cost estimate—comprehensive, well-documented, accurate, and credible. To understand HART's methodology, data, and approach, we interviewed relevant program officials, including the HART

[1]In response to our request for the baseline integrated master schedule, the Office of Biometric Identity Management (OBIM) provided a schedule dated June 2022, a month after establishing the May 2022 acquisition program baseline.

[2]GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs,* GAO-20-195G (Washington, D.C.: Mar. 12, 2020).

program manager and government cost lead for the Office of Biometric Identity Management (OBIM).

- To assess HART's schedule, we evaluated supporting documentation, such as the integrated master schedule, schedule risk analysis, and a schedule management plan. We assessed the schedule documentation against best practices identified in *GAO's Schedule Assessment Guide*.[3] These best practices map to the four characteristics of a high-quality, reliable schedule estimate—comprehensive, well-constructed, credible, and controlled. We also interviewed program officials responsible for developing and managing the program schedule, including OBIM's schedule management lead, to understand their practices for creating and maintaining the schedule.

For our assessments of the HART program's cost and schedule estimates, we assessed each best practice as follows:

- Met—OBIM provided complete evidence that satisfies the entire criterion.
- Substantially met—OBIM provided evidence that satisfies a large portion of the criterion.
- Partially met—OBIM provided evidence that satisfies about one-half of the criterion.
- Minimally met—OBIM provided evidence that satisfies a small portion of the criterion.
- Not met—OBIM provided no evidence that satisfies any of the criterion.

Then, to determine the overall assessment for each of the four characteristics, we assigned each best practice assessment a score based on a 5-point scale: not met = 1, minimally met = 2, partially met = 3, substantially met = 4, and met = 5. We calculated the average of the individual best practice assessment scores to determine the overall assessment rating for each of the four characteristics as follows: not met = 1.0 to 1.4, minimally met = 1.5 to 2.4, partially met = 2.5 to 3.4, substantially met = 3.5 to 4.4, and met = 4.5 to 5.0.

[3]GAO, *GAO Schedule Assessment Guide: Best Practices for Project Schedules,* GAO-16-89G (Washington, D.C.: Dec. 22, 2015).

Finally, we provided OBIM and HART program officials with draft versions of our detailed analyses of the program's cost and schedule so that they could verify the information on which we based our findings.

We determined that the cost and schedule data provided by OBIM was not complete and reliable. We discuss the limitations of these data in the report and we have made appropriate attribution indicating the sources of these data.

To address the third objective, we identified privacy requirements based on a review and analysis of federal laws, policy, and guidance. Specifically, we reviewed the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002,[4] as well as the Office of Management and Budget's (OMB) Circular A-130 *Managing Information as a Strategic Resource,* which included requirements for federal agencies to implement specific requirements for managing personally identifiable information (PII). We also reviewed Memorandum M-03-22*, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,* related to conducting a privacy impact assessment (PIA).[5]

Next, we selected requirements by first analyzing nine areas of requirements included in OMB A-130 appendix II.[6] The nine areas are comprised of 68 requirements. From these nine areas, we selected four areas that, based on our professional judgement, we determined contained requirements that could be applied to individual information systems such as HART (as opposed to agency-wide privacy activities).

[4]Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a) and E-Government Act of 2002, Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921 (2002).

[5]OMB, Circular A-130, *Managing Information as a Strategic Resource* (Washington, D.C.: July 2016) and Memorandum M-03-22*, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Washington, D.C.: Sept. 26, 2003).

[6]OMB A-130 Appendix II includes 11 areas: (1) Fair Information Practice Principles, (2) Senior Agency Official for Privacy, (3) Agency Privacy Program, (4) Considerations for Managing PII, (5) Budget and Acquisition, (6) Contractors and Third Parties, (7) Privacy Impact Assessments, (8) Workforce Management, (9) Training and Accountability, (10) Incident Response, and (11) Risk Management Framework. We excluded two of these areas from consideration when selecting requirements. Specifically, we did not consider the Fair Information Practice Principles area because it is not an OMB requirement and we did not consider the Senior Agency Official for Privacy area because it was duplicative of requirements in the Agency Privacy Program area.

Those areas were: (1) considerations for managing PII, (2) contractors and third parties, (3) conducting a PIA, and (4) risk management framework.[7] Collectively, these four areas included a total of 27 requirements.

From these 27 requirements, we excluded 15 that, based on our professional judgement, were not applicable to individual information systems. We also excluded requirements that overlapped with other selected requirements or with our prior reporting on contractor oversight at DHS.[8] This resulted in 12 remaining requirements that we assessed HART against:

1. Review and approve the system security categorization.
2. Establish a required security categorization level for shared PII.
3. Incorporate privacy requirements in contracts.
4. Encrypt moderate-impact and high-impact information.
5. Implement a privacy control selection process.
6. Conduct a PIA.
7. Develop a privacy plan and control assessment methodologies.
8. Assess privacy controls.
9. Correct privacy-related deficiencies.
10. Review the system authorization package.
11. Impose conditions on shared PII through agreements.
12. Follow records retention schedules.

To determine the extent to which the HART program had implemented the selected requirements, we obtained and assessed HART program documents and privacy-related artifacts against each of the selected privacy requirements. In particular, we analyzed, among other things,

[7]National Institute of Standards and Technology developed the risk management framework to address broad information-security and risk-management activities to be followed in developing information systems, including categorizing the system's impact level; selecting, implementing, and assessing security controls; authorizing the system to operate; and monitoring the efficacy of controls on an ongoing basis. OMB's Circular A-130 requires agencies to use this framework to manage privacy risks.

[8]GAO, *DHS Privacy: Selected Component Agencies Generally Provided Oversight of Contractors, but Further Actions Are Needed to Address Gaps*, GAO-22-104144 (Washington, D.C.: Dec. 16, 2021).

OBIM biometric guidelines, biometric records retention schedules, HART support contracts, information sharing and access agreements inventory and documentation, the PIA, and the system security and privacy plan.

In addition, we interviewed knowledgeable DHS officials regarding their efforts to implement privacy requirements for the system. Specifically, we interviewed officials from the HART program; OBIM; the DHS Privacy Office; the DHS Office of Strategy, Policy, and Plans; and the DHS Office of the Chief Information Officer.

We assessed the HART program's implementation of the 12 selected requirements as:

- fully implemented, if available evidence demonstrated implementation of all aspects of the requirement;
- partially implemented, if available evidence demonstrated implementation of some, but not all of the requirement, or;
- not implemented; if available evidence did not demonstrate implementation of any aspect of the requirement.

To assess the reliability of data contained in the system security and privacy plan, we (1) reviewed related documentation such as the user guide for the system in which DHS maintains system security and privacy plans; (2) examined these data for obvious outliers, incomplete entries, or unusual entries; and (3) interviewed knowledgeable program officials about the reliability of these data provided. We determined that these data were sufficiently reliable for the purposes of our reporting objective.

Moreover, to assess the reliability of the inventory of information sharing and access agreements provided by OBIM officials, we (1) reviewed related documentation and assessed the inventory for consistency with existing agency records; (2) examined these data for obvious outliers, incomplete entries, or unusual entries; and (3) interviewed knowledgeable program officials about the reliability of these data provided. We determined that the inventory was not reliable because it was incomplete. We discuss the related limitations in the report.

To determine whether the program had incorporated conditions for shared PII into the sharing agreements with partners, we first asked HART program officials to provide us with a list of information sharing and access agreements that pertain to data stored and shared by the system. The program provided us with two lists that collectively included 111 agreements. We selected the 37 agreements with domestic entities (e.g.,

the Department of State and Department of Defense) and excluded 74 agreements with international entities (e.g., United Kingdom, Canada, and Australia). We further narrowed the list of domestic agreements by excluding 11 agreements that duplicated across both lists, three agreements that were addendums to other full agreements, one agreement that was superseded by another agreement, one agreement that was internal to DHS, and three agreements that were listed but not provided. As a result, we selected a total of 18 agreements to review.

We also interviewed knowledgeable officials from DHS regarding their processes for developing and inventorying information sharing and access agreements. Specifically, we interviewed officials from OBIM; the DHS Office of Strategy, Policy, and Plans; and the DHS Office of the Chief Information Officer.

Lastly, we assessed the relevance of standards for internal controls for the audit. We determined that the control environment, risk assessment, control activities, information and communication, and monitoring components of internal controls were significant to our second and third objectives. Of specific relevance were internal control principles that emphasize that management should, among other things, use quality information to achieve the entity's objectives, and identify, analyze, and respond to significant changes that could impact the internal control system.

We conducted this performance audit from April 2022 to July 2023 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.

Appendix II: Results of GAO's Assessment of the HART Program Cost Estimate Compared with Best Practices

According to the *GAO Cost Estimating and Assessment Guide*,[1] the four characteristics of a high-quality, reliable cost estimate are comprehensive, well-documented, accurate, and credible. The following table provides our assessment of the HART program's cost estimate compared to these characteristics and the associated best practices, as of March 2022.

Table 5: Assessment of the Homeland Advanced Recognition Technology Program's Cost Estimate Compared to Best Practices, as of March 2022

Cost estimating characteristic	Overall assessment	Best practice	Individual assessment
Comprehensive	Partially met	Included all life cycle costs	Partially met
		Based on a technical baseline description that completely defines the program, reflects the current schedule, and is technically reasonable	Partially met
		Based on a work breakdown structure that divides work into smaller elements at an appropriate level of detail	Substantially met
		Documented all cost-influencing ground rules and assumptions.	Partially met
Well-documented	Partially met	Documented the source, reliability of data, and the estimating methodology used to derive each element's cost	Partially met
		Easily replicated and understandable	Partially met
		Provided consistency between data, assumptions, and technical baseline description	Partially met
		Reviewed and accepted by management	Substantially met
Accurate	Partially met	Estimated for each work breakdown structure element using the best methodology from data collected	Partially met
		Adjusted for inflation	Partially met
		Contained few, if any, minor mistakes	Substantially met
		Updated regularly to reflect program changes and actual costs	Partially met
		Documented variances between planned and actual costs and lessons learned	Minimally met
		Based on historical data	Partially met
Credible	Partially met	Included a sensitivity analysis that identified a range of possible costs based on varying inputs	Partially met
		Included a risk and uncertainty analysis that identified the effects of changing key cost drivers	Partially met
		Employed cross-checks on major cost elements to validate results	Minimally met
		Compared to an independent cost estimate conducted by an outside group to determine whether other estimates produce similar results	Partially met

Legend: Met— The Office of Biometric Identity Management (OBIM) provided complete evidence that satisfies the entire criterion; Substantially met—OBIM provided evidence that satisfies a large portion of the criterion; Partially met—OBIM provided evidence that satisfies about one-half of the criterion;

[1]GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs,* GAO-20-195G (Washington, D.C.: Mar. 12, 2020).

Minimally met—OBIM provided evidence that satisfies a small portion of the criterion; Not met—OBIM provided no evidence that satisfies any of the criterion.

Source: GAO analysis of HART program cost estimate and supporting documentation. | GAO-23-105959

Appendix III: Results of GAO's Assessment of the HART Program Schedule Compared with Best Practices

According to the *GAO Schedule Assessment Guide*,[1] the four characteristics of a high-quality, reliable schedule are that it is comprehensive, well-constructed, credible, and controlled. The following provides our assessment of the HART program's schedule estimate compared to these characteristics and the associated best practices, as of June 2022.

Table 6: Assessment of the Homeland Advanced Recognition Technology (HART) Program's Schedule Estimate Compared to Best Practices, as of June 2022

Schedule estimating characteristic	Overall assessment	Best practice	GAO assessment
Comprehensive	Partially met	Captured all activities for managing the entire program	Partially met
		Assigned resources (e.g., labor and materials) needed to complete the activities to determine whether they will be available when needed	Minimally met
		Established the duration of all activities based on a realistic reflection of how long each activity will take	Substantially met
Well-constructed	Partially met	Sequenced all activities to ensure that they include predecessor and successor logic	Partially met
		Confirmed that the critical path is valid and included all activities that drive the program's earliest completion date	Partially met
		Accommodated a reasonable amount of total float (time an activity can slip before the program's end date is affected)	Substantially met
Credible	Substantially met	Verified that the schedule can be traced horizontally and vertically[a]	Substantially met
		Prioritized risks and identified necessary schedule contingency based on a robust schedule risk analysis	Partially met
Controlled	Partially met	Updated regularly using actual progress and logic to realistically forecast dates for program activities	Partially met
		Maintained a baseline schedule to measure, monitor and report actual performance and variances from the plan	Partially met

Legend: Met— The Office of Biometric Identity Management (OBIM) provided complete evidence that satisfies the entire criterion; Substantially met—OBIM provided evidence that satisfies a large portion of the criterion; Partially met—OBIM provided evidence that satisfies about one-half of the criterion; Minimally met—OBIM provided evidence that satisfies a small portion of the criterion; Not met—OBIM provided no evidence that satisfies any of the criterion.

Source: GAO analysis of HART program schedule and supporting documentation. | GAO-23-105959

[a]Horizontal traceability demonstrates that the overall schedule is rational, has been planned in a logical sequence, accounts for the interdependence of detailed activities and planning packages, and provides a way to evaluate current status. Vertical traceability demonstrates the consistency of dates, status, and scope requirements between different levels of a schedule—summary, intermediate, and detailed.

[1]GAO, *Schedule Assessment Guide: Best Practices for Project Schedules,* GAO-16-89G (Washington, D.C.: Dec. 22, 2015).

Appendix IV: Comments from the Department of Homeland Security

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

Homeland Security

August 4, 2023

Marisol Cruz Cain
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-23-105959, "BIOMETRIC IDENTITY SYSTEM: DHS Needs to Address Significant Shortcomings in Program Management and Privacy"

Dear Ms. Cruz Cain:

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

DHS leadership is pleased to note GAO's recognition of the Department fully implementing five Office of Management and Budget privacy requirements. Implementing these requirements represents important steps towards protecting the personally identifiable information (PII) that will be matched, stored, and shared by Homeland Advanced Recognition Technology (HART).

As the Department's enterprise service provider of biometric identity services, the Management Directorate's (MGMT) Office of Biometric Identity Management (OBIM) considers the privacy of individuals' PII, and the security of the information in its data stores, to be the foundational elements of all developmental and operational activities. DHS's commitment to privacy and security is reflected in the legacy Automated Biometric Identification System (IDENT), and has been methodically integrated into HART as DHS develops and delivers this modernized system. Furthermore, Privacy Impact Assessments[1,2] are in place and approved by the Department for the IDENT and

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

[2] DHS/OBIM/PIA-001 (DHS/NPPD/PIA-002), "Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)," dated December 7, 2012; https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system

HART systems, and these systems are also subject to review of system security controls such as privacy controls, to achieve and maintain an approved authority to operate. These best practices safeguard the data OBIM uses for critical mission needs.

OBIM has already taken many steps to improve its program management of HART. As part of a contract modification awarded October 31, 2022, for example, OBIM government staff assumed the role of Lead Integrator of HART development, and subsequently reviewed and updated development and testing processes, took control and re-prioritized work, and modified the developer's scope to transition the work to other OBIM contractors under OBIM Government oversight to improve efficiencies. Since April 2023, OBIM also made significant changes regarding its executive level governance, to include: (1) initiating the restructuring of the OBIM Executive Steering Committee to provide more effective governance; (2) assigning an Executive level Program Manager; and (3) appointing the DHS Chief Information Officer as the HART Lead Technical Authority to help drive technical decisions throughout the Systems Engineering Lifecycle process.

The program continues to make improvements to its processes and documentation, such as the HART Life Cycle Cost Estimate (LCCE) and Integrated Master Schedule (IMS), to support decision-making. Further, DHS has made progress on addressing recommendations made by GAO in a previous report focused on HART.[3] Of the seven recommendations issued in the previous report, GAO considers four closed as implemented,[4] and the Department continues to work with GAO on implementing and closing the remaining open recommendations.

In the time since GAO conducted their Cost and Schedule Analysis for this engagement, improvements have also been made to the HART LCCE and HART IMS that are not reflected in the GAO's draft report. For example, for the HART LCCE, OBIM initiated improvements to its application of risk and improved documentation (i.e., updating actual source name and date in the LCCE when actuals are updated in the estimate) in January 2023. For the HART IMS, tasks were aligned to the OBIM Schedule Work Breakdown Structure in November 2022, and the HART IMS was updated to more clearly define whether tasks are assigned to federal employees or contractors in December 2022.

Further, in the draft report's assessment of OBIM's use of cost and schedule estimation best practices, GAO defines: (1) "partially met" as OBIM providing evidence that satisfies about one-half of the best practice criterion; and (2) "substantially met" as OBIM providing evidence that satisfies a large portion of the best practice criterion. DHS disagrees with GAO's assessment on four of the best practices, and describes below rationale to warrant a "substantially met" assessment for each.

[3] GAO-21-386, "HOMELAND SECURITY: DHS Needs to Fully Implement Key Practices in Acquiring Biometric Identity Management System," dated June 8, 2021; https://www.gao.gov/assets/gao-21-386.pdf
[4] https://www.gao.gov/products/gao-21-386

1. The cost estimation best practice of "Comprehensive" "Documented all cost-influencing ground rules and assumptions" has been substantially met, as OBIM reviewed the GAO Cost Estimating Guide with regards to the sensitivity analysis, and the methodology used meets the intent of the guidance. Specifically, the estimate variable inputs have risk assumptions aligned to the overarching ground rules and assumptions in the LCCE. These risk assumptions are used to calculate the point estimate for those variable inputs. This point estimate is then used to run the sensitivity analysis. OBIM discussed the Department's methodology for this best practice with GAO during a call in May 2023.

2. The cost estimation best practice of "Accurate" "Adjusted for inflation" has been substantially met. The HART program does not use standard inflation on work breakdown structure items where no inflation is required, due to the existence of negotiated costs or where inflation is already incorporated into the number for that work breakdown structure item. This is done to avoid applying an inflation factor twice. OBIM discussed the Department's methodology for this best practice with GAO during a call in May 2023.

3. The cost estimation best practice of "Accurate" "Updated regularly to reflect program changes and actual costs" has been substantially met. Actual costs are entered directly into the cost estimate line items, thereby superseding the estimated data. The estimated data from contracts is kept in the model for historical purposes. OBIM discussed the Department's methodology for this best practice with GAO during a call in May 2023.

4. The schedule estimation best practice of "Well-constructed" "Confirmed that the critical path is valid and included all activities that drive the program's earliest completion date" has been substantially met. As part of the formal status/review cycle of the schedule, the program makes updates to the schedule starting at a defined status date in each period, and updates are made to the schedule based on all changes up to that date. The three critical path tasks in question had changes that were past the defined status date. As such, notes were put in the schedule for the next update cycle. These notes would be used to incorporate the change into the following week's update. This was explained in our Schedule Analysis comments provided to GAO in December 2022. The update process is the reason for the difference in calculating the critical path, not an issue with the critical path the program has calculated, and this was explained in our Schedule Analysis comments provided to GAO in December 2022. These efforts provided evidence that satisfies a large portion of the criterion of this best practice.

DHS remains committed to improving its program management and oversight of the HART program, as well as ensuring that OBIM continues to identify and address any

privacy risks in its systems as the Department works to achieve HART Program Initial Operational Capability.

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

Sincerely,

JEFFREY M BOBICH Digitally signed by JEFFREY M BOBICH Date: 2023.08.04 14:54:25 -04'00'

Jeffrey M. Bobich
Acting Chief Financial Officer
Office of the Chief Financial Officer

Enclosure

4

Enclosure: Management Response to Recommendations Contained in GAO-23-105959

GAO recommended that the Secretary of Homeland Security direct the OBIM Director to:

Recommendation 1: Update the cost estimate for the HART program to account for all costs and incorporate the best practices called for in the GAO Cost Estimating and Assessment Guide.

Response: Concur. MGMT OBIM will update the HART Cost Estimating Baseline Document (CEBD) and HART LCCE to align with GAO's best practices, as appropriate. However, regarding the best practice of performing an independent cost estimate (ICE), it is important to clarify that the Cost Analysis Division (CAD) and the HART program office work closely together in the development of the program's LCCE during the program's annual updates to their LCCE, and CAD routinely conducts independent cost assessments (ICAs) on the program's cost estimate. The result of CAD's ICA provides the DHS Chief Financial Officer and Under Secretary for Management assurance that the LCCE is reliable and suitable for making critical acquisition decisions. Further, the goal of an ICE is to reach the same conclusion of high-quality cost estimating results and to provide decision makers with the same great insight that the Department is meeting with ICAs. Accordingly, the best practice of conducting an ICE would be a significant increase in CAD's efforts to produce similar results to those that CAD currently provides with less effort. For these reasons, OBIM will not conduct an ICE of the HART program.

As HART is currently in the initial rebaseline planning process, an estimated completion date (ECD) for the HART Increment 1 Rebaseline CEBD and HART Increment 1 Rebaseline LCCE cannot be provided at this time because they are contingent on available funding. However, DHS will be able to provide an ECD for the HART Increment 1 Rebaseline CEBD and HART Increment 1 Rebaseline LCCE after the HART Increment 1 Rebaseline Remediation Plan is completed in September 2023. With regards to Future Capabilities, the program is currently focused on Increment 1 development and delivery. Future Capabilities planning, to include updates to the HART CEBD and the HART LCCE, will be completed after HART Program Initial Operational Capability (IOC). These efforts include the following actions:

Actions	Estimated Completion Date (ECD)
HART Increment 1 Rebaseline Remediation Plan completion	September 29, 2023
HART Increment 1 Rebaseline CEBD update	TBD
HART Increment 1 Rebaseline LCCE completion	TBD
HART Future Capabilities CEBD update	TBD
HART Future Capabilities LCCE Completion	TBD

Overall ECD: TBD.

Recommendation 2: Revise the schedule estimate for the HART program that incorporates the best practices called for in the GAO Schedule Assessment Guide.

Response: Concur. OBIM will update the HART IMS to align to GAO's best practices, as appropriate. However, OBIM is already meeting the intent of the best practice of assigning resources (e.g., labor and materials) needed to complete the activities to determine whether they will be available when needed through the program's current processes. While all work breakdown structure areas in the HART IMS were resource assigned, the HART IMS was not resource-loaded. Rather, OBIM conducts resource demand management through OBIM's agile processes within a system called JIRA, in which the low-level requirements/stories are managed instead of the HART IMS (which captures higher-level epics and releases). OBIM's current agile processes control contractor and federal resource allocations, ensuring both are not overallocated. This process provides the program manager greater insight into resource allocations and issues as the lower-level requirements are tracked in JIRA. For these reasons, the Department will not add resource-loading into the HART IMS.

As HART is currently in the initial rebaseline planning process, an ECD for the HART Increment 1 Rebaseline IMS revision cannot be provided at this time because they are contingent on available funding. DHS will be able to provide an ECD for the HART Increment 1 Rebaseline IMS after the HART Increment 1 Rebaseline Remediation Plan is completed in September 2023. With regards to Future Capabilities, the program is currently focused on Increment 1 development and delivery. Future Capabilities planning, to include a revision to the HART IMS, will be completed after HART Program IOC. These efforts include the following actions:

Actions	ECD
HART Increment 1 Rebaseline Remediation Plan completion	September 29, 2023
HART Increment 1 Rebaseline IMS Revision completion	TBD
HART Future Capabilities IMS Revision completion	TBD

Overall ECD: TBD.

Recommendation 3: Coordinate with the Privacy Office to establish and implement a timeline for updating the HART PIA [privacy impact assessment] to fully describe the categories of individuals whose data will be stored in HART and the partners with whom the system shares information.

Response: Concur. OBIM Privacy will work with the DHS Privacy Office to highlight the identification of categories of individuals whose PII is stored in HART, and the partners with whom the system shares information, in the next HART PIA update.

ECD: July 31, 2024.

GAO recommended that the Secretary of Homeland Security direct the Privacy Office to:

Recommendation 4: Describe planned methodologies for determining that all privacy controls are implemented correctly and operating as intended for future control assessments of the HART program.

Response: Concur. Throughout GAO's work on this audit, the DHS Privacy Office described planned methodologies for determining that all privacy controls are implemented correctly and operating as intended for the HART program. Specifically, privacy controls are assessed through the entire privacy compliance documentation process, to include development of a Privacy Threshold Analysis (PTA), PIA, System of Records Notice (SORN), Privacy Act Statements, etc., as well as DHS privacy policies. Further, the implementation of the privacy controls is assessed during the privacy compliance documentation process.

The actual implementation of a Privacy Control as a specific process happens as a system is being built out/developed. The system/program, for example, builds in an auditing tool or a training program, while the PTA, PIA, and/or SORN are designed specifically to elicit responses from programs to assess whether the Privacy Control implemented/built into/added to a system is satisfactory. The PTA, PIA, and/or SORN documents that tool/program, and the Privacy Office assesses whether that Privacy Control's implementation is satisfactory. Because

the Privacy Controls either pass or fail, they are deemed satisfactory during the assessment of the PTA, PIA, or SORN. Further, the "Implementation Statement" section for each Privacy Control in the HART System Privacy Plan describes how the control is implemented/assessed (i.e., passes).

The following documentation was provided to GAO on October 25, 2022, as evidence of these processes:

- DHS Directive 047-01 "Privacy Policy and Compliance" dated July 7, 2011;[5]
- Instruction 047-01-001, "Privacy Policy and Compliance, dated July 25, 2011;"[6]
- Several internal documents providing information on a crosswalk of Privacy Controls, a system security and privacy plan, and system screenshots.

DHS requests that GAO consider this recommendation resolved and closed, as implemented.

Recommendation 5: Develop a timeline for completing the planned HART privacy compliance review.

Response: Concur. The Chief Privacy Officer selected a new Privacy Oversight Director, who will enter on duty in September 2023, and will be responsible for completing Privacy Compliance Reviews (PCR). However, the DHS Privacy Office initial timeline for conducting a HART PCR was predicated on HART being fully implemented (HART Program IOC). Therefore, the DHS Privacy Office is unable to provide a timeline for completing the review until the HART Program IOC. These efforts include the following actions:

Actions	ECD
DHS Privacy Oversight Director entering on duty	September 29, 2023
HART Privacy Compliance Review timeline completed	TBD, one year after HART Program IOC

Overall ECD: TBD.

GAO recommended that the Secretary of Homeland Security direct the OBIM Director to:

Recommendation 6: Coordinate with the Privacy Office to establish and implement plans for correcting seven remaining privacy deficiencies identified in the HART PIA.

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

8

Response: Concur. OBIM Privacy will work with the DHS Privacy Office to plan, monitor, and address the seven remaining privacy recommendations identified in the HART PIA. Specifically, OBIM Privacy and the DHS Privacy Office will address corrective actions to close out the privacy recommendations once the DHS Privacy Office's Privacy Oversight Director enters on duty in September 2023. As the hiring process is not complete, a final timeline for this effort cannot be provided at this time. These efforts include the following actions:

Actions	ECD
DHS Privacy Oversight Director hired	September 29, 2023
OBIM and DHS Privacy Office review seven remaining privacy recommendations and establish timelines for correcting deficiencies	March 29, 2024
OBIM establishes and implements plans for correcting deficiencies for the seven remaining privacy recommendations	TBD per guidance from the DHS Privacy Oversight Director

Overall ECD: TBD.

GAO recommended that the Secretary of Homeland Security direct the Privacy Office to:

Recommendation 7: Ensure the complete HART authorization package is reviewed by the office prior to future system authorizations.

Response: Concur. The DHS Privacy Office will review the entire HART authorization package prior to the next "authority to operate" update. Specifically, the DHS Privacy Office will work with OBIM Privacy and the DHS Office of the Chief Information Officer/Office of the Chief Information Security Officer to ensure the HART authorization package is appropriately reviewed. The ECD is dependent on the HART authorization package moving forward as currently scheduled.

ECD: June 28, 2024.

GAO recommended that the Secretary of Homeland Security direct the OBIM Director to:

Recommendation 8: Establish and implement a timeline for maintaining a reliable inventory of information sharing and access agreements with partners that share data with HART.

Response: Concur. OBIM Privacy will revise its inventory listing of information sharing and access agreements with partners that share data with HART to ensure

the inventory provides reliable information on what Departmental agreements align to which partners, and whether these partners are current or planned users of HART. In addition, OBIM will maintain an inventory of agreements related to HART, and will establish a timeline for review and updates to the inventory listing and inventory on a consistent basis.

ECD: July 31, 2024.

Recommendation 9: Establish and maintain a process for ensuring that partners that provide data to HART have used the system's services to help to appropriately dispose of PII from the system, in accordance with applicable retention schedules.

Response: Concur. OBIM will establish and maintain a process for ensuring that partners that provide data to HART are using HART services to remove PII from the system in accordance with their National Archives and Records Administration-approved records schedules. This process will strengthen Government, mission-partner, and public trust by defining, managing, and remediating potential over-retention of PII in HART.

ECD: September 30, 2024.

10

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contact

Marisol Cruz Cain, (202) 512-5017, cruzcainm@gao.gov

Staff Acknowledgments

In addition to the contacts listed above, the following staff made significant contributions to this report: Shannin O'Neill (assistant director), Hannah Brookhart (analyst in charge), Mathew Bader, Christopher Businsky, Emile Ettedgui, Rebecca Eyler, Yvette Gutierrez, Franklin Jackson, William Laing, Jennifer Leotta, Lee McCracken, Nolan Roosa, Lucas Scharf, Andrew Stavisky, Adam Vodraska, and Andrew Weiss.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548

Please Print on Recycled Paper.