June 2021

HOMELAND SECURITY

DHS Needs to Fully Implement Key Practices in Acquiring Biometric Identity Management System

GAO@100

A Century of Non-Partisan Fact-Based Work

GAO@100
Highlights

HOMELAND SECURITY

DHS Needs to Fully Implement Key Practices in Acquiring Biometric Identity Management System

Why GAO Did This Study

DHS currently uses an outdated system, implemented over 27 years ago, for providing biometric identity management services (i.e., fingerprint matching and facial recognition technology services), known as the Automated Biometric Identification System, or IDENT. In 2016, DHS initiated a multi-billion dollar program known as HART, which is intended to replace the existing system.

GAO was asked to evaluate the HART program. Its specific objectives, among others, were to (1) determine the status of the program, (2) assess the extent to which the DHS CIO was accurately reporting risk and meeting applicable oversight requirements, and (3) assess the extent to which the program was identifying and managing its risks.

To accomplish these objectives, GAO identified the program's schedule and cost estimates, assessed the CIO's risk ratings and HART oversight documentation and related evidence against OMB guidance, and compared the program's risk management practices to best practices that are essential to identifying and mitigating potential problems. In addition, GAO interviewed appropriate officials.

What GAO Recommends

GAO is making seven recommendations, including that DHS update its policy to reflect the current IT program assessment process, and fully implement the risk management best practice related to monitoring the status of risks and mitigation plans. DHS concurred with all of the recommendations and provided estimated dates for implementing them.

What GAO Found

The Department of Homeland Security (DHS) initially expected to implement the entire Homeland Advanced Recognition Technology (HART) by 2021; however, no segments of the program have been deployed to date. Currently estimated to cost $4.3 billion in total, DHS plans to deploy increment 1 of the program in December 2021 and expects to implement later increments in 2022 and 2024. Increment 1 is expected to replace the functionality of the existing system.

Although the multi-billion dollar HART program had suffered continuing delays, until the end of last year, the DHS Chief Information Officer (CIO) had reported the program as low risk on the IT Dashboard, a website showing, among other things, the performance and risks of agency information technology (IT) investments. In May 2020, the Office of the CIO began developing a new assessment process which led to the CIO accurately elevating HART's rating from low to high risk and reporting this rating to the IT Dashboard in November 2020. In addition, consistent with OMB guidance, the CIO fulfilled applicable oversight requirements for high-risk IT programs by, among other things, conducting a review of the program known as a TechStat review. While the CIO complied with applicable oversight requirements in conducting the TechStat review, GAO noted that DHS's associated policy was outdated. Specifically, the 2017 policy does not reflect the revised process DHS started using in 2020. As such, until the guidance is updated, other departmental IT programs deemed high risk would likely not be readily aware of the specific process requirements.

Concurrent with the CIO's actions to conduct oversight, HART program management has also acted to implement important risk management practices. Specifically, GAO found that HART had fully implemented four of seven risk management best practices and partially implemented the remaining three (see table). For example, as of February 2021, the program had identified 49 active risks, including 15 related to cost and schedule and 17 related to technical issues. While DHS has plans under way to fully implement two of the partially implemented practices, until it fully implements the remaining practice its efforts to effectively monitor the status of risks and mitigation plans may be hampered.

Summary of the Homeland Advanced Recognition Technology Program's Implementation of the Seven Risk Management Practices

Practice	GAO assessment
1. Determine risk sources and categories	●
2. Define parameters to analyze and categorize risks	●
3. Establish and maintain a risk management strategy	◑
4. Identify and document risks	●
5. Evaluate and categorize each identified risk using defined risk categories and parameters, and determine its relative priority	●
6. Develop a risk mitigation plan in accordance with the risk management strategy	◑
7. Monitor the status of each risk periodically and implement the risk mitigation plan as appropriate	◑

Legend: ● = Fully implemented ◑ = Partially implemented ○ = Not implemented
Source: GAO analysis of agency data. | GAO-21-386

United States Government Accountability Office

Contents

Figures

GAO@100

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
A Century of Non-Partisan Fact-Based Work

441 G St. N.W.
Washington, DC 20548

June 8, 2021

The Honorable Gary C. Peters
Chairman
The Honorable Rob Portman
Ranking Member
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
Chairman
Committee on Homeland Security
House of Representatives

Biometric identity management services, such as fingerprint matching and facial recognition technology services, are commonly used across business and government sectors as a tool for identifying and verifying customers or persons of interest. 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 enable national security and public safety decision making for DHS and its partner agencies—DHS components; as well as the Departments of State, Justice, and Defense; state, local, tribal, and territorial law enforcement; the intelligence community; and foreign country partners.[1] Such information enables the partner agencies to make national security,

---

[1]DHS's 14 components include: U.S. Citizenship and Immigration Services, U.S. Coast Guard, U.S. Customs and Border Protection, Cybersecurity and Infrastructure Security Agency, Federal Emergency Management Agency, Federal Law Enforcement Training Center, U.S. Immigration and Customs Enforcement, U.S. Secret Service, Transportation Security Administration, Management Directorate, Science and Technology Directorate, Countering Weapons of Mass Destruction Office, Office of Intelligence and Analysis, and Office of Operations Coordination.

GAO-21-386 Biometric Modernization Program

law enforcement, immigration, intelligence, and other public safety decisions.

DHS currently provides biometric identity management services through the Automated Biometric Identification System, or IDENT. Among other things, the department uses IDENT to store biometric data (e.g., digital fingerprints and iris scans) on foreign nationals and share it with U.S. government and foreign partners to facilitate legitimate travel, trade, and immigration.[2] However, in 2011 DHS reported that IDENT, which became operational in 1994, had significant shortcomings such as system capacity constraints, a lack of ability to handle multiple types of biometric data, and limitations on accuracy and assurance. In 2018, we reported that IDENT may not be able to fully support requirements related to other DHS programs that seek to match biometric data against the department's biometric data repositories.[3]

To mitigate these challenges, DHS initiated the Homeland Advanced Recognition Technology (HART) program in 2016. The HART system is intended to be a centralized DHS-wide biometric database that replaces and enhances the functionality provided by IDENT. The new system is also expected to provide additional biometric services, as well as a web portal and new tools for analysis and reporting. HART was originally estimated to cost about $5.8 billion and to be fully implemented by 2021.[4]

In response to your request to review HART, our specific objectives were to (1) determine the status of the HART program, (2) assess the accuracy of the DHS Chief Information Officer's (CIO) risk ratings for the HART program reported on the IT Dashboard and whether the CIO met

---

[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]GAO, *Homeland Security Acquisitions: Leveraging Programs' Results Could Further DHS's Progress to Improve Portfolio Management,* GAO-18-339SP (Washington, D.C.: May 17, 2018).

[4]The $5.8 billion figure that DHS and OBIM established for HART represents the program's cost threshold in its initial April 2016 acquisition program baseline. This figure represents the total lifecycle cost estimate in then-year dollars, which includes the effects of inflation.

TechStat review requirements,[5] (3) assess the extent to which the HART program was identifying and managing its risks, and (4) assess the extent to which the HART program was implementing selected information technology (IT) acquisition best practices.

To address our first objective, we obtained and reviewed data related to HART's initial, rebaselined, and current cost and schedule estimates. We also reviewed artifacts from the HART program's status reviews, such as monthly briefings to the DHS Deputy Under Secretary for Management and weekly minutes from project team meetings. We also reviewed HART remediation plans. In addition, we interviewed knowledgeable officials from the DHS Office of the Chief Information Officer (OCIO), OBIM, and HART.

To address the second objective, we obtained and reviewed OCIO's internal program health assessments and associated risk ratings for HART, and analyzed the assessments and ratings against evidence related to program performance that we obtained while addressing the first objective. We used this information to determine if the OCIO health assessment ratings were consistent with the program's actual risks. We also compared the OCIO health assessment ratings to the CIO evaluations reported on the IT Dashboard to determine whether the ratings on the Dashboard were current and reflected the risk level associated with HART, as required by the Federal Information Technology Acquisition Reform Act (FITARA)[6] and associated Office of Management and Budget (OMB) implementation guidance.

Further, we obtained and analyzed the department's oversight review documentation for HART to determine if the CIO met the five TechStat review requirements that we identified in FITARA, associated OMB

---

[5]The Federal IT Dashboard is an Office of Management and Budget website that reports performance and supporting data for major IT investments (see itdashboard.gov). A major IT investment means a system or an acquisition requires special management attention because it has significant importance to the mission or function of the government; significant program or policy implications; high executive visibility; high development, operating, or maintenance costs; an unusual funding mechanism; or is defined as major by the agency's capital planning and investment control process. A TechStat review is an evaluation of high-risk IT investments to determine whether to terminate or turn around investments that are in danger of failing or are not producing results.

[6]*Federal Information Technology Acquisition Reform provisions of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015*, Pub. L. No. 113-291, div. A, title VIII, subtitle D, 128 Stat. 3292, 3438-3450 (Dec. 19, 2014).

implementation guidance, and the department's policy.[7] In addition, we interviewed appropriate officials from the OCIO, including the department's CIO, to obtain further information about the HART risk ratings on the IT Dashboard and the use of the office's existing oversight processes to address the requirements associated with a TechStat review.

To address the third objective, we obtained the program's risk management artifacts and compared them to the seven risk management practices identified in the Software Engineering Institute's Capability Maturity Model® Integration for Acquisition.[8] These practices included, among other things, establishing and maintaining a risk management strategy, identifying and documenting risks, and developing a risk mitigation plan.

We assessed the HART program's implementation of the seven risk management practices as:

- fully implemented, if available evidence demonstrated all aspects of the practice;

- partially implemented, if available evidence demonstrated some, but not all, aspects of the practice; and

- not implemented, if available evidence did not demonstrate any aspect of the practice.

We also interviewed appropriate program officials, including the HART program manager and HART risk manager, to obtain additional information about the program's risks and risk management practices. In addition, we interviewed two HART stakeholder groups. The first group was the OBIM Executive Stakeholders Board, which included members from the Departments of Defense, Justice, and State. The second group was HART's Integrated Project Team, which included members from OBIM that were outside of the HART program office and other DHS components, such as the Science and Technology Directorate. We selected these stakeholder groups because they collectively provided representation from key stakeholders associated with the HART program.

---

[7]DHS Directive 102-03, *TechStat Accountability Sessions* (Washington, D.C.: May 17, 2017).

[8]Software Engineering Institute, *Capability Maturity Model® Integration for Acquisition*, Version 1.3 (November 2010).

We obtained their perspectives on the key risks facing the program and the extent to which those risks were being addressed.[9]

To address the fourth objective, we first analyzed the 22 process areas within Capability Maturity Model® Integration for Acquisition and identified those areas which were relevant for assessing the HART program. From the list of the 22 areas, we selected those process areas associated with maturity level two. Maturity level two establishes the foundation for effective acquisition practices.[10]

To narrow our list further, we excluded process areas that were not associated with the project processes category.[11] For the six areas that remained, we then selected the areas that, based on our professional judgment, were the logical choices for selection given where the HART program was in its system development lifecycle (i.e., post-contract award and in the system development phase). The selected areas were (1) agreement management, (2) project monitoring and control, and (3) requirements management. Collectively, these three process areas contained 20 practices.

From these 20 practices, we selected 14 that, based on our professional judgment, were more important aspects to review given where the program was in its system development lifecycle. In addition, we excluded

---

[9]DHS's Office of Program Accountability and Risk Management—DHS's main body for acquisition oversight—developed department-wide risk management processes that acquisition programs are required to follow. For our review, we assessed the HART program against key industry best practices for risk management outlined in the Capability Maturity Model® Integration for Acquisition guide.

[10]Capability Maturity Model® Integration for Acquisition aligns each of its process areas to a maturity level. Maturity levels are a means of improving the processes corresponding to a given set of process areas (i.e., maturity level). The five maturity levels are designated by the numbers 1 through 5: Initial (1), Managed (2), Defined (3), Quantitatively Managed (4), and Optimizing (5).

[11]The 22 process areas in Capability Maturity Model® Integration for Acquisition are associated with one of the following four categories: Project Processes (11), Organizational Processes (3), Support Processes (4), and High Maturity Processes (4). The process areas associated with the Project Processes category contain practices that address acquirer activities related to establishing, executing, and ensuring the transition of an acquisition project. We excluded the remaining process areas associated with the other three categories because those areas included processes and practices that can be applied more generally to the organization.

practices within a process area if another process area also identified a similar practice.[12]

We compared the program's contract management, program management, and requirements management artifacts to the 14 selected practices. We also interviewed program officials, including the HART program manager and HART requirements manager, to (1) obtain an understanding of the processes in place to manage the program and (2) discuss the program's efforts to implement the selected practices.

We assessed the HART program's implementation of the 14 IT acquisitions practices as:

- fully implemented, if available evidence demonstrated all aspects of the practice;

- partially implemented, if available evidence demonstrated some, but not all, aspects of the practice; and

- not implemented, if available evidence did not demonstrate any aspect of the practice.

Further, to assess whether the HART program had implemented the contract management practice of managing contractor invoices, we first asked the HART program officials to provide us with a list of invoices that the system development contractor had submitted between May 2019 and August 2020. This resulted in 33 invoices. Of these 33 invoices, we selected the seven most recent invoices associated with specific contract line item numbers. We selected one additional invoice which was the most recent invoice generally associated with the cost-plus-fixed-fee portion of the development contract.[13] This resulted in a total of eight selected invoices for our review. We reviewed the selected invoices to determine whether the HART program office and contracting officials reviewed and approved these invoices.

We assessed the reliability of the cost, risk, and requirements-related data that were provided by the HART program officials by (1) analyzing related documentation and assessing the data against existing agency

---

[12]One of the 14 selected practices is a combination of three individual practices. We combined these practices into one practice because of the overlapping nature of the three practices.

[13]A cost-plus-fixed-fee contract provides for payment to the contractor of a negotiated fee that is fixed at the inception of the contract.

records to identify consistency in the information; (2) examining the data for obvious outliers, incomplete entries, or unusual entries; and (3) interviewing knowledgeable program officials about the reliability of the data provided. We determined that the data used to support the findings in this report were sufficiently reliable for the purposes of our reporting objectives, with the exception of the agency-reported HART spending data. Specifically, we determined that the spending data provided by the HART program officials were not reliable and we discuss the limitations of these data in the report. We have also made appropriate attribution indicating the sources of the provided data. A detailed discussion of our objectives, scope, and methodology can be found in appendix I.

We conducted this performance audit from January 2020 to June 2021 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.

Background

OBIM's mission is to provide DHS and its partner agencies with biometric identity services that enable them to make national security and public safety decisions. To do so, OBIM uses the IDENT system, which became operational 27 years ago (in 1994).

IDENT is the central DHS-wide system that stores and processes biometric data that are collected from individuals by partner agencies and links the biometric data with biographic information (i.e., name and date of birth). The partner agencies 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 identify of persons associated with matters of national security.

As of April 2021, OBIM reported that IDENT stored more than 268 million separate and distinct identities. Prior to the Coronavirus Disease 2019 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 agency projected that the transaction volumes would return to the pre-pandemic levels and that the number of stored biometrics would continue to increase.

DHS Established the HART Program to Address Shortcomings with IDENT

In 2011, DHS reported that IDENT had several significant shortcomings. Specifically, the department reported that IDENT had:

- significant system capacity constraints,

- a lack of ability to handle multiple types of biometric data,

- 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 address these shortcomings, the department began planning for the replacement of IDENT with the HART system. Between 2011 and 2016, DHS worked on acquisition planning activities, such as developing a concept of operations, evaluating potential solution alternatives, and estimating costs to formal program approval.

In addition to providing all of the existing functionality of IDENT, the HART system is expected to address partner agencies' requests for conducting multiple biometric matching operations. For example, the system is expected to use two forms of biometric data to identify and verify an individual and provide options for contactless biometric data collection. The system is also expected to improve existing functionality, such as increasing the accuracy of detection and derogatory information

matching, providing greater interoperability with partner agencies, and achieving operations and maintenance cost efficiencies.[14]

Similar to IDENT, partner agencies will be expected to use HART for different purposes. Partner agencies may query the new system before making national security, law enforcement, immigration, and intelligence decisions. These agencies may also use the system to upload and store new biometric data that they have collected from individuals.[15]

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 data for trusted travelers scheduled to fly within the next 24 hours for use in identity verification at an airport's security checkpoint.[16] In addition, the U.S. Customs and Border Protection (CBP) is expected to use HART to support biometric identification and verification of in-scope travelers entering the U.S.

---

[14]Derogatory information is any information that potentially justifies rejecting an applicant. This information may prompt a request for additional investigation or clarification for resolution of an issue.

[15]HART's partner agencies who upload and store new biometric information are referred to as "data providers." Data providers include U.S. Customs and Border Protection; Federal Emergency Management Agency; U.S. Immigration and Customs Enforcement; Transportation Security Administration; U.S. Coast Guard; U.S. Citizenship and Immigration Services; DHS Under Secretary for Management; U.S. Secret Service; Department of Defense; Department of Justice; Department of State; Intelligence Community; state, local, tribal, and territorial law enforcement; and federal, state, and local investigative agencies, in coordination with the Department of Justice; and international partners such as Canada, New Zealand, Australia, the United Kingdom, Guatemala, Greece, Italy, and Mexico.

[16]The TSA PreCheck® Application Program allows the public to enroll for expedited security screening when traveling from more than 200 airports nationwide. Passengers who qualify for the program are considered low risk and become eligible to receive expedited screening and are referred to as trusted travelers. Biographic data, fingerprints, and a photograph are collected during enrollment.

GAO-21-386 Biometric Modernization Program

through air, sea, and land ports of entry to determine if further action is needed.[17]

As one example of the several different uses of HART, figure 1 describes and graphically depicts the planned process flow by which a CBP officer may use the system.[18]

---

[17]In-scope international travelers exclude: U.S. citizens; Canadian citizens visiting the United States temporarily for business or pleasure; visitors admitted on an select 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 and the Secretary of Homeland Security or the Director of Central Intelligence Agency jointly determine shall be exempt; and Taiwanese officials who hold the appropriate visas and members of their immediate families who hold these same visas.

[18]For recent information on the status of CBP's deployment of facial recognition technology at ports of entry, see GAO, *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues,* GAO-20-568 (Washington, D.C.: Sept. 2, 2020).

Figure 1: Planned Process Flow between U.S. Customs and Border Protection and the Homeland Advanced Recognition Technology (HART) System for Biometric Identification or Verification for Air, Land, or Sea Entry

U.S. Customs and Border Protection Officer (CBP)

① Biographic data collection and submission

CBP accesses a traveler's biographic information through a traveler's travel document (e.g., passport or other border crossing credential) or facial comparison technology and initiates a pre-verify search of the Homeland Advanced Recognition Technology (HART) system to determine if traveler's biographic information matches an existing identity in HART

② Pre-verify

HART compiles identity information from its database about the traveler, including any derogatory information and biometric data available for matching

Pre-verify results in no match or no valid biometric (e.g., fingerprint)

Pre-verify results in match

③ Biometric collection and submission

The CBP officer collects a biometric and submits it to HART for possible enrollment and verification

④ External search

HART initiates an identity search with other systems to determine if there is an identity match with the biometric provided

⑤ Assessment of results

CBP officer reviews system response to determine if further action is needed

⑥ HART stores interaction

HART records the interaction and biometric information provided and assigns it to the traveler's identity history

Source: GAO analysis of agency data; images: James Thew/stock.adobe.com, Buffaloboy/stock.adobe.com. | GAO-21-386

In April 2016, DHS approved the acquisition program baseline for HART. The baseline estimated the total lifecycle cost threshold of the new system to be about $5.8 billion.[19] Further, the baseline estimated that initial operating capability would occur in 2018 and full implementation would occur in 2021.

OBIM is implementing HART using an Agile incremental development approach. This approach emphasizes early and continuous software delivery, with development being broken down into 3-week iterations, called sprints. Each set of four sprints is compiled into deployable, working software, referred to as a release. The development cycle for each release is 16 weeks. The program holds planning sessions with stakeholders prior to the start of the development of the next system release or sprint, as well as review sessions at the end of each release or sprint to evaluate the work produced.

In 2016, OBIM planned to implement HART in four increments.

- **Increment 1:** This increment is currently under development and is intended to deliver all the existing IDENT functionality and the core foundational infrastructure necessary to operate HART. Once OBIM completes increment 1, all partner agencies are expected to migrate from IDENT to HART, with HART then being considered the biometric system of record. Following this transition, OBIM intends to decommission IDENT. Increment 1 was initially intended to be comprised of three releases. Initial operating capability was intended to be achieved with the deployment of increment 1.

- **Increment 2:** This increment was intended to add multiple biometric matching operations, such as using two forms of biometric data to identify and verify an individual, to increase overall system matching accuracy and potentially provide additional data storage. In January 2021, the program began working with its contractor to review the requirements associated with increment 2. Development on this increment began in February 2021.

- **Increment 3:** OBIM intended to deliver additional capabilities, such as new tools to improve human examination of multiple types of biometric data 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

---

[19]This figure represents the total lifecycle cost estimate in then-year dollars, which includes the effects of inflation.

GAO-21-386 Biometric Modernization Program

biometric data such as deoxyribonucleic acid (commonly known as DNA), palm, voice, scars, and tattoos. Development on this increment had not begun as of February 2021.

- **Increment 4:** Increment 4 was to include the ability to perform analyses and reporting based on the data storage established in increment 2, and to provide a holistic view of identities to assist customer adjudication and decision-making related to access, credentials, or benefits. Increment 4 also was intended to provide additional types of biometric data and enhancements in support of mobile access to HART. In addition, this increment was intended to provide analytics and reporting capabilities to improve accuracy and eliminate duplicative, noncurrent, and inconsistent data. Development on this increment had not begun as of February 2021.

Several DHS Entities Share Responsibility for Overseeing HART

The HART program is subject to DHS's oversight framework. Specifically, the program is to adhere to the department's acquisition policy, including its systems engineering lifecycle framework, which is intended to support the efficient and effective delivery of IT capabilities. The Under Secretary for Management serves as the Acquisition Decision Authority for the program, and is typically responsible for overseeing adherence to DHS's acquisition policies for the department's largest acquisition programs (i.e., those with lifecycle cost estimates of $300 million or more).

The Under Secretary for Management is supported by many offices within the department. One these offices—the DHS OCIO—is responsible for, among other things, setting departmental IT policies, processes, and standards. The OCIO is also responsible for ensuring that acquisitions comply with the department's IT management processes, technical requirements, and the approved enterprise architecture.

Within the OCIO, the Chief Technology Officer Directorate is responsible for leading the development of IT and standards across the department, and for offering guidance and assistance to programs to help improve their execution. As part of its responsibilities, the directorate is expected to lead, maintain, and manage the TechStat process. This process is intended to identify investments that are underperforming, conduct root cause analysis to mitigate risks, and provide OMB a report of the outcomes and results.

DHS acquisition oversight is also provided through the Acquisition Review Board, Executive Steering Committees, and other oversight bodies. DHS's Acquisition Review Board is chaired by the Under Secretary for Management and is made up of many executive-level members, including

the CIO. The board is to meet periodically to oversee programs' business strategies, resources, management, accountability, and alignment to strategic initiatives. Additionally, the Executive Steering Committees are generally comprised of component and DHS executive-level members, such as the component CIOs and Chief Financial Officers, as well as the DHS Chief Technology Officer. The committees are to provide governance, oversight, and guidance to programs to help ensure successful development and operations.

Along with the DHS CIO, OBIM is also located within the DHS Management Directorate, and the HART program management office resides within OBIM. The program manager is, among other things, responsible for directing the day-to-day operations and ensuring completion of the program's goals and objectives. Figure 2 provides an overview of key entities within the DHS Management Directorate responsible for the governance and management of the HART program.

Figure 2: Key Department of Homeland Security Entities Responsible for the Homeland Advanced Recognition Technology Program
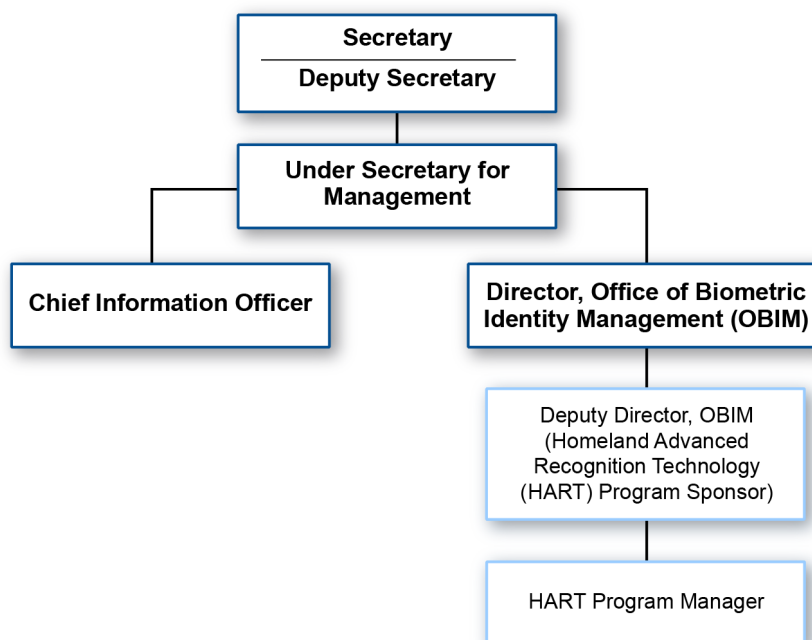
Source: GAO analysis of Department of Homeland Security data. I GAO-21-386

The HART Program Is Significantly behind Schedule and Has Exceeded Its Most Recent Cost Estimate

The HART program is significantly behind schedule and has exceeded its most recent cost estimate. Specifically, while DHS originally planned to implement the entire system by 2021, no increments of the program had been deployed as of April 2021. As of February 2021, the program tentatively planned to deploy HART's first increment in December 2021 and to implement later increments in 2022 and 2024.

HART's schedule problems first emerged in June 2017. At that time, the program declared that it had breached its schedule from its 2016 approved baseline, which established that the program would implement increment 1 in 2018 and fully implement the remaining increments by 2021. According to DHS officials, the breach was due to delays in awarding a contract for increments 1 and 2 and a bid protest. DHS subsequently awarded a $95 million contract to Northrop Grumman to develop increments 1 and 2 in September 2017. However, since 2017, DHS has modified the development contract 12 times and increased the cost to over $143 million.

In response to the June 2017 breach, DHS rebaselined the HART program 2 years later (in May 2019), and delayed the deployment date for increment 1 by 2 years (from December 2018 to December 2020). The department also pushed out the program's full deployment date by nearly 3 years (from September 2021 to June 2024).

In January 2020, the HART program declared a second schedule breach—8 months after rebaselining the program. According to HART's breach remediation plan, this breach was 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 requirements, and the technical approach for customer migration and biometric matching.

As of February 2021, the program had pushed out the planned completion date for increment 1 and its transition of users from IDENT to HART to December 2021 (3 years later than initially planned). As a result, the program has been even further delayed in transitioning partner agencies from IDENT to HART. This is an issue because, as DHS previously reported, IDENT has significant shortcomings that required DHS to make additional investments in the system to keep it operational much longer than planned. Program officials stated that they intend to revise the schedule estimate as part of another program rebaseline by the end of September 2021. Figure 3 provides a timeline of the changes that DHS had made to the HART program schedule, as of February 2021.

Figure 3: Changes in Homeland Advanced Recognition Technology (HART) Program Schedule, as of February 2021

Calendar years
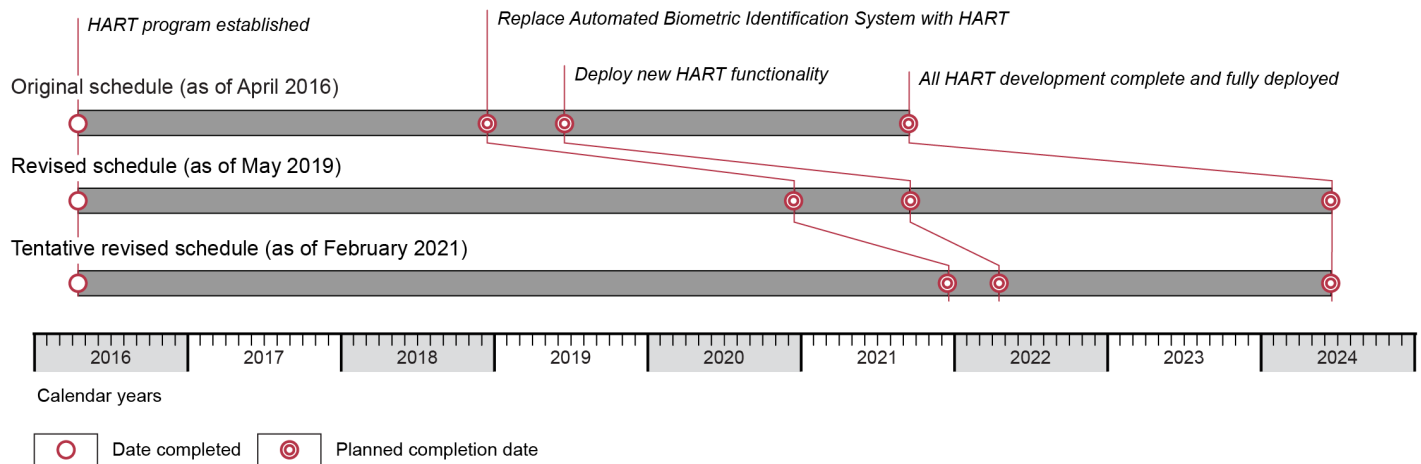
Source: GAO analysis of agency data. | GAO-21-386

In response to the 2017 breach, the program also rebaselined the HART program's lifecycle cost estimate in May 2019 which resulted in a decrease of about $2 billion (from $5.8 billion to approximately $3.9 billion).[20] Program officials primarily attributed the cost decrease to a decision to provide storage for HART data using a less expensive cloud-based solution,[21] rather than DHS's data centers. The officials indicated that another reason for the decrease was the removal of IDENT upgrade costs in the HART estimate.

However, in May 2020, the HART program reported that it had breached the cost estimate. In May 2020, the program revised its lifecycle cost estimate to about $4.3 billion (an increase of about $400 million).[22] According to HART's breach remediation plan, among other things, the reason for the cost breach was due to changes the program planned to make to address the technical issues that resulted in the schedule breach. Program officials also stated that the cost breach was due to

[20]The $3.9 billion figure that DHS and OBIM reestablished in May 2019 represents the lifecycle cost estimate threshold. This figure is presented in then-year dollars, which include the effects of inflation.

[21]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.

[22]The $4.3 billion figure represents the revised lifecycle cost estimate threshold amount in then-year dollars that the HART program developed in May 2020.

expanding the cloud computing environment to support future requirements and the need for additional program support. Similar to the schedule estimate, program officials stated that they intend to revise the cost estimate as part of the program rebaseline, by the end of September 2021. Figure 4 identifies the changes to the HART program's lifecycle cost estimate, as of February 2021.

Figure 4: Changes in the Homeland Advanced Recognition Technology Program Lifecycle Cost Estimate, as of February 2021

Total life-cycle cost (then-year dollars in billions)[a]
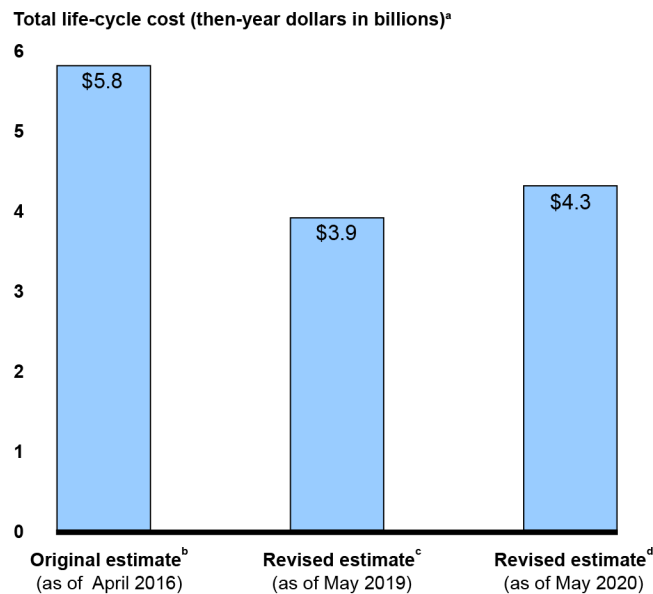
Source: GAO analysis of agency data. | GAO-21-386

[a]Then-year dollars include the effects of inflation. The HART acquisition program baseline numbers are in base years. The term base year means dollars that are expressed in the value of a specific year and do not include the effects of inflation.

[b]The original 2016 lifecycle cost estimate includes costs from fiscal years 2015 to 2029.

[c]The revised 2019 lifecycle cost estimate includes costs from fiscal years 2015 to 2033.

[d]The revised 2020 lifecycle cost estimate includes costs from fiscal years 2015 to 2033.

In response to the schedule delays and cost overruns, the program made changes to increment 1. Specifically, the program made a major contract modification in August 2020 to address the technical challenges related to the development of increment 1 and decided to combine increments 3 and 4 into a single increment, now referred to as future capabilities.

In addition, the program expanded its number of releases from three to eight releases for increment 1. As of February 2021, the program

GAO-21-386 Biometric Modernization Program

completed development on seven of its eight releases. The last release was planned for completion by May 2021. In addition, program officials planned to work on several activities from February 2021 to December 2021 to get the program ready to deploy increment 1, such as migrating users and data from IDENT to HART, completing independent testing, and training users.

Updates to Process Improved the Accuracy of HART's CIO Risk Rating and TechStat Requirements Were Met; but TechStat Policy Was Outdated

For a major IT acquisition such as HART, FITARA and OMB's guidance require federal CIOs to evaluate major IT acquisition investments (i.e., programs) and provide OMB with progress-related updates.[23] Among other responsibilities, these requirements stipulate that federal CIOs are to:

1. **Notify OMB of their risk ratings associated with major programs via the IT Dashboard.** Specifically, according to OMB, agency CIOs are to assess their investments against a set of pre-established evaluation factors and then assign a rating of 1 (high-risk) to 5 (low-risk), based on the CIO's best judgment of the level of risk facing the investment. Further, OMB guidance stated that the agency CIOs are to update the IT Dashboard within 30 days if the following were to occur: a TechStat review session is conducted for a program, a program experiences a baseline change, a new CIO numeric evaluation (1-5) score is identified for the program, the program experiences a status change to one or more of its projects, or the program experiences a status change to its risk information.[24]

2. **Conduct TechStat reviews and report on the outcomes for programs that have repeated high-risk ratings.**[25] To meet this requirement, DHS established a TechStat policy which defined a DHS TechStat review as a direct data-driven assessment, to identify weaknesses and to determine corrective actions or modifications, or to halt or terminate the investment. The policy stated that a major IT investment is subject to a TechStat review by the OCIO if the program

---

[23]*Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015*, Pub. L. No. 113-291, division A title VIII, subtitle D, 128 Stat. 3292, 3438-3450 (Dec. 19, 2014) and OMB, *Management and Oversight of Information Technology,* Memorandum M-15-14 (Washington, D.C.: June 10, 2015).

[24]OMB, *Fiscal Year 2021 IT Budget - Capital Planning Guidance* (Washington, D.C.: revised June 28, 2019).

[25]In 2010, OMB defined a TechStat review to be face-to-face, evidence-based accountability review of an IT program to intervene, turn around, halt, or terminate programs that are failing or are not producing results.

receives a high-risk or moderately high-risk rating on the IT Dashboard for 1 month and there are indications that the high-risk rating will continue, or for 3 consecutive months.[26]

This policy also stated that the department's CIO is responsible for leading, maintaining, and managing the TechStat process within the department. In addition, OMB's guidance and DHS's policy identified the following five requirements for TechStat reviews:

- establish a root cause analysis of performance issues,

- establish corrective action plans which address the root causes,

- establish a timeline for implementing the corrective action plans,

- document an assessment using OMB's "Investment and Portfolio Management Maturity Framework" template,[27] and

- provide results of the TechStat review to OMB.

In November 2020, DHS submitted a new CIO rating for the HART program to the IT Dashboard that accurately reflected its level of risk: the CIO rated the program high-risk. However, prior to November 2020, the CIO's risk rating on the IT Dashboard was out-of-date and did not reflect the status of the HART program. Specifically, as previously mentioned, the program entered a second schedule breach in January 2020 and a cost breach in May 2020; however, the IT Dashboard showed a low-risk CIO rating for the program from February 2020 until November 2020. This low-risk rating was based on a CIO evaluation that was submitted in November 2019, and had not been updated for a year.

Figure 5 identifies the CIO risk ratings that DHS submitted for the HART program to the IT Dashboard from November 2019 to February 2021.

---

[26]DHS, *Directive 102-03, TechStat Accountability Sessions* (Washington, D.C.: May 17, 2017). This policy also identifies other examples for when a TechStat can be initiated for a program (e.g., CIO requests an evaluation due to concerns over cost or schedule variance).

[27]The Investment and Portfolio Management Maturity Framework template identifies 20 areas that are associated with one of the following five categories: (1) Management, (2) People, (3) Process, (4) Technology, and (5) Acquisition. OMB's FITARA implementation guidance instructs agencies to use this framework for describing investment and portfolio management maturity with OMB.

GAO-21-386 Biometric Modernization Program

Figure 5: Chief Information Officer Risk Ratings Associated with the Homeland Advanced Recognition Technology (HART) Program

Chief Information Officer risk ratings

Low risk (5)

Moderately low risk (4)

Medium risk (3)

Moderately high risk (2)

High risk (1)
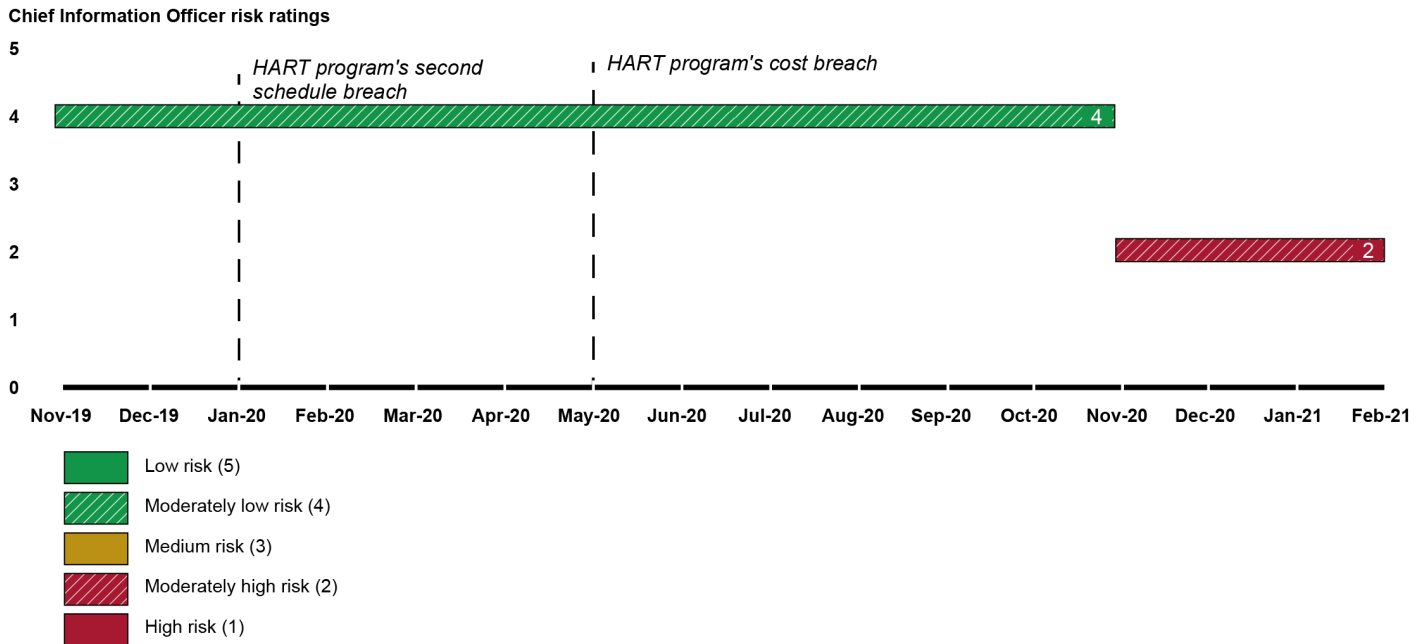
Source: GAO analysis of data from the Office of Management and Budget's IT Dashboard website. | GAO-21-386

OCIO officials acknowledged that the low-risk rating for HART on the IT Dashboard was inaccurate and out-of-date from February 2020 to November 2020. The officials stated that the reason for the delay in submitting a new risk rating for HART to the IT Dashboard was that in May 2020 the office had begun working on establishing a new quarterly program health assessment process for assessing risks related to all major and special interest IT programs such as HART.[28] While the OCIO evaluated the HART program as high-risk in June 2020 using this new process, OCIO officials explained that they decided to wait until the CIO reviewed the new assessments for all programs prior to submitting any updated risk ratings to the IT Dashboard in November 2020.

---

[28]According to DHS Acquisition Management Directive 102-01, major acquisition programs are expected to cost at least $300 million. Further, DHS also designates other acquisitions as special interest programs without regard to established dollar thresholds. For example, a program may be designated as a special interest if its importance to DHS's strategic and performance plans is disproportionate to its size or it has high executive visibility.

Moving forward, if effectively implemented, this new health assessment process could help improve the timeliness and value of the HART CIO ratings reflected on the IT Dashboard. Further, these improvements should also help provide more transparency to OMB, Congress, and others on the risks and issues facing the HART program.

With regard to the DHS CIO's utilization of the TechStat review process to oversee the HART program, we found that the OCIO had met the TechStat review requirements. Specifically, with regard to the first requirement (establish a root cause analysis of performance issues), the OCIO's Chief Technology Officer Directorate fully met the requirement by performing a technical assessment in August 2020 that identified three high-level root causes of HART performance issues. The assessment analyzed major program areas[29] and identified the following root causes for HART's issues: (1) lack of the program's and contractor's understanding of the breadth and complexity of requirements; (2) lack of contractor collaboration with the program management office; and (3) lack of contractor's adequate technical skill, planning, and execution in delivery of the products required.

The OCIO also met the second TechStat related requirement for establishing corrective action plans that address the root causes. For example, to address the issues associated with the lack of understanding the complexity of requirements, the OCIO identified corrective actions, such as ensuring the HART program manager was more involved in the requirements decomposition process. In addition, to address issues associated with the contractor's lack of adequate technical skills, the OCIO worked with the contractor to review the qualifications of its staff, which increased the quality of contractor's staff skills levels.

In addition, the OCIO met the third TechStat related requirement on establishing a timeline for implementing the corrective actions. In particular, the office's August 2020 technical assessment for HART identified relative timelines for implementing the corrective actions for HART. In addition, HART's breach remediation plan, approved in January 2021, documented the remaining actions needed to revise the program's

---

[29]The Chief Technology Officer Directorate's Technical Assessment reviewed program areas of: (1) Enterprise Architecture Alignment, (2) Solution Delivery Management, (3) Technical Development, (4) Systems Engineering Life Cycle, and (5) Configuration Management.

baseline. In May 2021, DHS and OBIM officials stated that they expected the rebaseline to occur by September 2021.

The OCIO met the fourth TechStat related requirement for assessing HART against OMB's "Investment and Portfolio Management Maturity Framework" template. In particular, the OCIO assessed and scored HART against the five categories identified in OMB's template through its new quarterly program health assessment process.

Lastly, the OCIO met the fifth TechStat related requirement for providing the results of the TechStat-type review to OMB. In March 2021, OCIO officials stated that they were planning to provide (1) the August 2020 technical assessment and (2) the November 2020 program health assessment for the HART program to OMB by April 1, 2021.

However, DHS's TechStat policy did not specify any of the above actions as the approved approach to meeting the five requirements. For example, the policy did not reference the Chief Technology Officer Directorate's technical assessment as the approach the department should be using to meet the requirement to establish a root cause analysis of performance issues (first requirement). In addition, the policy did not reference the CIO's new health assessment process as the approach the department should be using to assess HART against OMB's "Investment and Portfolio Management Maturity Framework" template (fourth requirement). The reason that the policy did not specify these actions was because it was developed in 2017 and no longer reflects the OCIO's processes that officials use to address the TechStat requirements.

OCIO officials stated that they met with OMB officials in January 2021 to explain how their existing acquisition oversight processes, such as the new program health assessment process and their technical assessments, met the intent of the TechStat requirements. The officials said that OMB was supportive of OCIO's approach to addressing the TechStat requirements. Further, the officials said they were working to address some of OMB's comments on their existing processes.

However, the OCIO officials were unable to identify a time frame for when they expected to update DHS's TechStat policy to be consistent with the processes that they are actually using. Accordingly, until the policy is updated, other departmental IT programs deemed high risk would likely not be readily aware of the specific process requirements.

The HART Program Fully Implemented Four Key Practices Related to Identifying and Managing Risks and Partially Implemented Three

According to the Capability Maturity Model® Integration for Acquisition,[30] an effective risk management process identifies potential problems before they occur, so that risk-handling activities may be planned and invoked, as needed, across the life of the project to mitigate adverse impacts on achieving objectives. Specifically, effective risk management practices include:

- determining risk sources (i.e., fundamental drivers that cause risks in a project or organization) and categories (i.e., cost, schedule, and contract management);

- defining parameters to analyze (i.e., probability of risk occurrence and impact and severity of risk occurrence) and categorize risks;

- establishing and maintaining a risk management strategy that includes potential mitigation techniques (i.e., prototyping, piloting, and simulation), defining when a risk becomes unacceptable to trigger the execution of a mitigation plan, and consideration of the costs and benefits of implementing risk mitigation plans for key risks;

- identifying and documenting risks;

- evaluating and categorizing each identified risk using defined risk categories and parameters, and determining its relative priority;

- developing a risk mitigation plan in accordance with the risk management strategy, which includes a determination of the thresholds that define when a risk becomes unacceptable and triggers the execution of a risk mitigation plan, and costs and benefits of implementing the risk mitigation plan for key risks; and

- monitoring the status of each risk periodically and implementing the risk mitigation plan as appropriate, to include resource commitments and the schedules for each risk-handling activity (i.e., start dates and anticipated completion dates).

The HART program fully implemented four of the seven key risk management practices and partially implemented the remaining three practices. Table 1 lists these practices and provides our assessment of the HART program's implementation of the practices.

---

[30]Software Engineering Institute, *Capability Maturity Model® Integration for Acquisition, Version 1.3* (Pittsburgh, Pa.: November 2010).

Table 1: Summary of the Homeland Advanced Recognition Technology Program's Implementation of the Seven Risk Management Practices

Practice	GAO assessment
1. Determine risk sources and categories	●
2. Define parameters to analyze and categorize risks	●
3. Establish and maintain a risk management strategy	◑
4. Identify and document risks	●
5. Evaluate and categorize each identified risk using defined risk categories and parameters, and determine its relative priority	●
6. Develop a risk mitigation plan in accordance with the risk management strategy	◑
7. Monitor the status of each risk periodically and implement the risk mitigation plan as appropriate	◑

Legend:
● = Fully implemented— available evidence demonstrated all aspects of the practice.
◑ = Partially implemented—available evidence demonstrated some, but not all, aspects of the practice.
○ = Not implemented—available evidence did not demonstrate any aspect of the practice.

Source: GAO analysis of agency data. | GAO-21-386

- **Determine risk sources and categories—fully implemented.** The HART program determined risk sources and categories. For example, HART's risk management plan, which was signed and approved by the program manager, included a table of possible sources of risk, such as requirements stability or system reliability. In addition, the risk management plan included a section on risk categories. For example, according to the risk management plan, all risks are to be identified in HART's risk repository and a risk owner is to determine one or more categories that each risk relates to. The five categories are: (1) programmatic, (2) cost, (3) schedule, (4) technical, and (5) support.

- **Define parameters to analyze and categorize risks—fully implemented.** The HART program defined parameters to analyze and categorize risks. For example, HART's risk management plan defined a quantitative and qualitative scale for risk owners to determine each risk's probability. Specifically, risk owners are to determine the probability of a risk materializing and becoming an issue, based on the following descriptions: (1) highly improbable, (2) unlikely, (3) possible, (4) probably, and (5) extremely likely. Once realized, a risk is to be classified as an issue with a 100 percent probability.

  In addition, the risk management plan defined a quantitative scale for identifying the risk impact. According to the plan, risk owners are to determine the impact if a risk materializes and becomes an issue,

based on a five-tier rating across the five risk categories: (1) very low, (2) low, (3) medium, (4) high, and (5) very high. The program is to assess a risk as low, medium, or high priority based on probability and impact scores.

- **Establish and maintain a risk management strategy—partially implemented.** The HART program partially established and maintained its risk management strategy in a risk management plan. Specifically, the plan described the methods and tools to be used for risk identification, analysis, and monitoring. For example, the plan included a section on the process to be used in order to nominate an emerging risk for the program manager's and deputy program manager's review for approval or rejection. However, the plan did not (1) discuss the mitigation techniques that may be used, such as prototyping, piloting, and simulation; (2) discuss defining triggers to indicate when a risk might occur and require execution of a risk mitigation plan; or (3) provide guidance for how risk management officials can consider the costs, such as those associated with needed resources, or the benefits of implementing risk mitigation plans for key risks.

  Program officials stated that they overlooked these elements and, thus, did not consider them for inclusion in the plan. The officials further stated that they would add these risk management elements to their next update to the risk management plan, scheduled for July 2021. Incorporating and effectively implementing these missing elements in its risk management plan should help DHS ensure that the program is appropriately identifying and mitigating all program risks and avoiding the likelihood that those risks materialize into issues.

- **Identify and document risks, including the context, conditions, and potential consequences of each risk—fully implemented.** The HART program identified and documented risks. As of February 2021, the program's risk register included 49 active risks. Of the 49 risks, seven were related to cost, eight were related to schedule, 17 were related to the technical category, 16 were related to the programmatic risks category, and one was related to the support category. These risks also accounted for environmental elements that can affect the project. For example, one risk was dedicated to disaster recovery and associated continuity of operations plans. In addition, the program manager assigned a risk owner to manage and maintain the data associated with each risk. The risk owner was responsible for ongoing updates of risks every 30 days and monitored and communicated the current status of risks and the progress of risk response plans.

- **Evaluate and categorize each identified risk using defined risk categories and parameters, and determine its relative priority—fully implemented.** The HART program evaluated and categorized each identified risk using defined risk categories and parameters. For example, in accordance with the program's risk management plan, risk owners documented a risk probability and impact for all active risks in the risk register. In addition, the program prioritized risks for mitigation based on their likelihood and severity. Of the 49 active risks in the HART risk register, all included a risk level (i.e., high, medium, or low) and associated risk rating. As of February 2021, the program rated seven risks as high, related to, among other things, accuracy of fingerprint matching, stakeholder schedule delays, customer migration, and defining future capabilities.

- **Develop a risk mitigation plan in accordance with the risk management strategy—partially implemented.** The HART program partially developed a risk mitigation plan in accordance with its risk management strategy. Specifically, it developed mitigation plans for all 49 active risks in the risk register. Each of the plans contained multiple actions (referred to as steps). As of February 2021, the program had developed 249 mitigation steps for handling its active risks. These mitigation steps were one of three types: (1) actions—specifics steps to reduce risk exposure, (2) controls—procedures to impact the risk, or (3) fallbacks—the contingency plans that are to be used when a risk is realized.

  However, the mitigation plans did not document a trigger indicating when a risk might become an issue. In addition, the program did not determine the costs, such as those associated with needed resources, or benefits of implementing the risk mitigation plans for key risks.

  The program did not document a trigger or consider cost benefit tradeoffs, because, as previously discussed, the risk management plan did not provide guidance on including these elements of risk mitigation. As previously mentioned, program officials acknowledged the plan lacked these elements and stated that they intend to incorporate program guidance regarding the elements in the next update to the plan, scheduled for July 2021. OBIM officials stated that they intend to use this guidance to document triggers and determine the costs and benefits associated with risk mitigation plans in the future. By capturing the triggers for executing risk handling measures, the program may better anticipate risk before it becomes an issue. In addition, by considering the costs and benefits of implementing risk

mitigation plans, the program may avoid unnecessary use of additional resources.

- **Monitor the status of each risk periodically and implement the risk mitigation plan as appropriate—partially implemented.** The HART program partially monitored the status of each risk periodically and implemented the risk mitigation plan. For example, the program periodically monitored risk status. Specifically, program officials held a weekly meeting to evaluate and determine the approach for how the program would address each risk and issue. In addition, the program discussed risks managed by the contractor during a monthly meeting and during planning sessions.

  However, while officials stated that these risk meetings included discussions of resource commitments needed for risk mitigation actions, they did not maintain records of their risk-related discussions. According to the HART risk manager, risk meeting discussions were not documented because program officials believed that the agenda for these meetings was sufficient. However, without documentation of the items discussed during these meetings, the program did not clearly capture the actions and decisions stemming from these meetings for future reference or to serve as a resource for anyone unable to attend the meetings. Further, without keeping records of these discussions, including those related to resource commitments for risk mitigation plans, the program may be less prepared to provide the resources needed to successfully execute these mitigation plans when necessary.

  Moreover, while program officials stated that the status of risk mitigation plans were discussed during risk meetings and that risk owners and assignees were responsible for taking corrective actions for their assigned risks, we found that the status of risk mitigation plans were not always updated in the risk register. For example, as of February 2021, of the 249 mitigation steps being managed by the program, 73 did not have a due date and nine steps had a status of "on track," despite being overdue. Program officials attributed these gaps to the fact that that they did not take additional steps to ensure that risk owners incorporated corrective actions for each risk mitigation plan. Until the program can ensure that risk owners maintain accurate and current status updates for each risk mitigation plan in the risk register, program management officials responsible for monitoring the implementation of these activities may make key decisions without a complete picture of the risk.

The HART Program Had Mixed Results in Implementing Selected IT Acquisition Best Practices

In addition to risk management, IT acquisition best practices developed by both industry and the federal government can help guide the successful acquisition of investments. To help organizations and agencies with implementing IT acquisition best practices, the Software Engineering Institute identified numerous practices related to (1) agreement management, (2) project monitoring and control, (3) and requirements management, among other areas and practices.[31]

The HART program had mixed results in implementing the selected IT acquisitions best practices. Specifically, of the 14 selected practices associated with the three IT acquisition areas, the HART program fully implemented seven practices and partially implemented the remaining seven practices.

Table 2 summarizes the extent to which the HART program had implemented the 14 selected acquisition practices associated with the selected acquisition areas.

---

[31]Capability Maturity Model® Integration for Acquisition, *Agreement Management, Project Monitoring and Control, and Requirements Management Process Areas*.

Table 2: Summary of the Homeland Advanced Recognition Technology Program's Implementation of the 14 Selected Practices Associated with the Three Selected Acquisition Areas

Selected acquisition area	Selected practice	GAO assessment
Agreement management	1. Conduct management reviews with the contractor and monitor the contractor's progress related to cost and schedule.	●
	2. Review the contractor's work products, including confirming that all issues have been corrected and all contractual requirements have been satisfied.	◑
	3. Manage contractor invoices and resolve all errors or issues prior to approval.	●
Project monitoring and control	4. Monitor actual project progress related to cost and schedule against those identified in the project plan.	◑
	5. Monitor staffing commitments against those identified in the project plan.	◑
	6. Monitor stakeholder involvement, including ensuring relevant stakeholders maintain involvement, consistent with the project plan.	◑
	7. Periodically review and communicate project performance with relevant stakeholders.	●
	8. Review and document project results, such as action items and decisions, at milestones.	●
	9. Manage corrective actions on identified issues to closure.	●
Requirements management	10. Establish an understanding of requirements with program stakeholders.	◑
	11. Obtain a commitment to requirements from program stakeholders by assessing the impact of requirements on existing commitments.	◑
	12. Manage changes to requirements throughout the lifecycle by evaluating the impact of requirement changes from the standpoint of relevant stakeholders.	●
	13. Maintain a clear and discernable association between high-level mission and operational requirements and the lower-level functional and technical requirements (referred to as bidirectional traceability) among program documents, which is typically achieved by using a requirements traceability matrix or automated requirements management system.	◑
	14. Ensure program plans remain aligned to requirements.	●

Legend:
● = Fully implemented—available evidence demonstrated all aspects of the practice.
◑ = Partially implemented—available evidence demonstrated some, but not all, aspects of the practice.
○ = Not implemented—available evidence did not demonstrate any aspect of the practice.
Source: GAO analysis of agency data. | GAO-21-386

HART Fully Implemented Two of the Three Selected Agreement Management Practices

According to Capability Maturity Model® Integration for Acquisition, the purpose of implementing agreement management practices is to ensure that the supplier (i.e., contractor) and the acquirer (i.e., in this case, the HART program) perform according to the terms of the supplier agreement (i.e., the performance work statement). From the acquirer's perspective, the supplier agreement is the basis for managing the relationship with the supplier. It defines the mechanisms that allow the acquirer to oversee the supplier's activities and work products and to verify compliance with the

requirements outlined in the supplier agreement. Among other agreement management practices, the acquirer should (1) conduct management reviews with the contractor and monitor the contractor's progress, (2) review the contractor's work products to confirm that all issues are corrected and all contractual requirements are satisfied, and (3) manage contractor invoices and resolve all errors or issues prior to approval.

The HART program fully implemented two of the three agreement management practices and partially implemented one practice. Table 3 lists these selected practices and provides our assessment of the HART program's implementation of them, as of February 2021.

Table 3: Summary of the Homeland Advanced Recognition Technology Program's Implementation of the Three Selected Agreement Management Practices

Selected practice	GAO assessment
1. Conduct management reviews with the contractor and monitor the contractor's progress related to cost and schedule	●
2. Review the contractor's work products to confirm that all issues are corrected and all contractual requirements are satisfied	◐
3. Manage contractor invoices and resolve all errors or issues prior to approval	●

Legend: ● = Fully implemented ◐ = Partially implemented ○ = Not implemented

Source: GAO analysis of agency data. | GAO-21-386

- **Conduct management reviews with the contractor and monitor the contractor's progress related to cost and schedule—fully implemented.** The HART program office held weekly, tri-weekly, and quarterly meetings with the contractor to review the contractor's progress and performance. For example, to support the HART system's incremental development approach, the program held system demonstration events every 3 weeks to review the new system functionality that the contractor had developed since the last demonstration meeting.[32] In addition, the HART program office monitored contractor-related costs through its ongoing invoice review and approval process (discussed later). The program office also

---

[32]The incremental development approach the contractor is using for HART increment 1 is based on the Scaled Agile Framework approach. It emphasizes early and continuous software delivery with development being broken down into time-boxed iterations called sprints, where teams commit to develop specific requirements into working software; and the deployment of such software is associated with another time boxed event called a release.

reviewed updates related to scheduled contractor activities on a
weekly basis.

- **Review the contractor's work products to confirm that all issues
  are corrected and all contractual requirements are satisfied—
  partially implemented.** The HART program office reviewed
  deliverables associated with the contract's data requirements
  (referred to as a contract data requirements list) that the contractor
  submitted to the program office.[33] For example, between March and
  April 2020, the program office conducted initial reviews and identified
  issues with six contractor-developed deliverables, such as the *HART
  Developmental Test Plan and the HART Software Application Design*.

  However, while the contractor's performance work statement specified
  that the contractor was required to address all critical issues and
  important clarifications on its contract deliverables, the program office
  did not consistently assign criticality levels (i.e., critical issue,
  important clarification, or editorial recommendation) to each of its
  initial comments on such deliverables. For example, in the HART
  program officials' review of the *HART Developmental Test Plan*, they
  identified 49 comments, but the program did not assign criticality
  levels for 18 of these comments.

  Program officials stated that they did not consistently assign criticality
  levels because they were focused on identifying the new development
  work that would be included in an upcoming contract modification for
  increments 1 and 2. However, in response to us identifying this issue,
  the program re-evaluated its remaining comments and assigned
  criticality levels to more of its comments. As a result, the contractor
  now has clearer expectations on which comments it needs to address
  prior to the program's acceptance of these deliverables.

  In addition, for the same six deliverables that the contractor submitted
  between March and April 2020, the program office did not ensure that
  its issues associated with each of the deliverables were addressed.
  Specifically, while the program office provided the contractor with
  comments on each of the deliverables, it did not validate that the
  contractor had addressed the issues.

  In November 2020, program officials stated that they had not yet
  validated whether the contractor had addressed their existing issues

---

[33]With regard to the contract deliverables we reviewed, the contractor was responsible for
updating these deliverables every developmental release whereas the invoices discussed
in the practice below are primarily associated with an individual Contract Line Item
Number. The frequency in which the contract deliverables and invoices needed to be
submitted to the HART program varied.

because they were interim, rather than final, deliverables. Specifically, officials added that the contractor plans to update the interim documents to support future system development work and that they plan to ensure that all of the existing issues associated with each deliverable will be addressed prior to the deployment of increment 1.

However, the program office's plan to defer addressing issues and updating documents increases the risk that the contractor will carry over issues in program system documentation repeatedly throughout the life of the existing system development work. As such, until the HART program office takes steps to address all issues associated with a contract deliverable prior to working on activities associated with the next developmental release, the program has increased the risk that it will introduce errors in the program.

- **Manage contractor invoices and resolve all errors or issues prior to approval—fully implemented.** The HART program office and the OBIM contracting officials reviewed (and approved, when appropriate) the invoices we selected for review.[34] Specifically, of the eight invoices we reviewed, program office officials and OBIM contracting officials approved seven invoices and rejected one revised invoice. They rejected the revised invoice because it included an additional 2 months of work and additional charges that were not included when the contractor initially submitted the invoice. In addition, prior to approving the seven invoices for payment, the program officials worked with OBIM contracting officials and the contractor to resolve the errors and issues associated with each invoice, when applicable.

HART Fully Implemented Half of the Six Selected Project Monitoring and Control Practices

According to Capability Maturity Model® Integration for Acquisition, an effective project monitoring and control process provides oversight of the program's performance, to allow appropriate corrective actions if actual performance deviates significantly from planned performance. Key practices in overseeing and tracking a program's performance include (1) monitoring actual project progress against the project plan, (2) monitoring staffing commitments against those identified in the project plan, (3) monitoring stakeholder involvement consistent with the project plan, (4)

---

[34]To select the invoices that we examined, we first asked the HART program officials to provide us with a list of invoices that the system development contractor had submitted between May 2019 and August 2020. This resulted in 33 invoices. Of the 33 invoices, we selected the seven most recent invoices associated with specific Contract Line Item Numbers. We selected one additional invoice which was the most recent invoice generally associated with the cost-plus-fixed-fee portion of the development contract (i.e.. a cost-plus-fixed-fee contract that provides for payment to the contractor of a negotiated fee that is fixed at the inception of the contract). This resulted in a total of eight selected invoices for our review.

periodically reviewing and communicating project performance with relevant stakeholders, (5) reviewing and documenting project results at milestones, and (6) managing corrective actions on identified issues to closure.

The HART program had fully implemented three of the six project monitoring and control practices and partially implemented three practices. Table 4 lists these selected practices and provides our assessment of the HART program's implementation of the practices, as of February 2021.

Table 4: Summary of the Homeland Advanced Recognition Technology Program's Implementation of the Six Selected Project Monitoring and Control Practices

Selected practice	GAO assessment
1. Monitor actual project progress against the project plan	◑
2. Monitor staffing commitments against those identified in the project plan	◑
3. Monitor stakeholder involvement consistent with the project plan	◑
4. Periodically review and communicate project performance with relevant stakeholders	●
5. Review and document project results at milestones	●
6. Manage corrective actions on identified issues to closure	●

Legend: ● = Fully implemented ◑ = Partially implemented ○ = Not implemented
Source: GAO analysis of agency data. | GAO-21-386

- **Monitor actual project progress against the project plan— partially implemented.** The HART program monitored the completion of program activities and milestones against the planned completion dates identified in the interim schedule (which was being used until the program formally approves the HART program's rebaselined schedule). As previously discussed, the program office also monitored actual contractor-related costs through an ongoing invoice review and approval process. In addition, according to program officials, as of January 2021, the program reported that it had spent about $132 million on contractor-related costs from fiscal years 2016 through 2020. These costs were for items such as contractor labor and the development of a performance test environment required to build, implement, and test the HART system.

  However, since 2016, the program had not tracked and monitored government-related labor costs specific to HART because the program had obtained DHS's approval to combine and manage the HART and IDENT programs' labor costs. Program officials stated that

they decided to track these costs together because almost all of OBIM's officials worked on both HART and IDENT, so this allowed them to avoid separately tracking the hours spent on each program. In February 2021, the officials stated that they were considering tracking government-related labor costs independently for HART and IDENT starting in October 2021 (to align with the new fiscal year). However, the program had not finalized its decision for how it planned to track and monitor government-related labor costs for the program moving forward.

In addition, while the program reported to OMB via the IT Dashboard that it had spent about $577 million, in total, from fiscal years 2016 through 2020, it was unclear how much of this spending was specifically associated with the HART program. This was because the figure also included the operations and maintenance costs for IDENT. DHS officials explained that HART's spending data on the IT Dashboard included costs related to IDENT because the department had decided to track the operations and maintenance costs for both systems under a single funding account. Program officials were unable to explain the rationale for why these costs were combined under a single account.

However, the department's decision to include IDENT costs with the HART program has significantly reduced the transparency of spending for HART—which may hamper OBIM and DHS management, as well as Congress, from effectively overseeing the program. Moving forward, without accurately tracking and monitoring costs associated with HART, including government-related labor costs and operations and maintenance costs, the program will be unable to have an accurate account of program spending, or compare actual costs against planned estimates.

- **Monitor staffing commitments against those identified in the project plan—partially implemented.** The HART program documented its staffing commitments for government staff that needed to allocate a portion of their time to support the program. The program also reassessed those commitments on an annual basis. Program officials stated that they coordinated with senior leadership across OBIM throughout the year to discuss any issues related to staffing commitments not being met.

  However, the program did not track and monitor the contractor's staffing resources. In particular, the contractor's performance work statement stated that the contractor was responsible for providing monthly updates related to its staffing plan commitments, but the contractor did not provide these updates. As a result, the program

was unable to monitor the extent to which the contractor was meeting its planned commitments.

Program officials stated that they did not receive these updates from the contractor and attributed it to an oversight. In November 2020, the program officials added that they were working with the contractor to determine the appropriate level of staffing data that should be provided by the contractor. The contractor began providing monthly updates related to staffing in January 2021.

Program officials added that, following the contractor's staffing updates, they plan to evaluate the staffing plan against the contractor's ability to deliver work planned versus work accomplished and whether staffing factors into any potential bottlenecks that may impede the completion of the planned work. By reviewing the contractor's staffing resources on an ongoing basis, the program should be better positioned to reduce the likelihood that it experiences delays due to a lack of staffing resources.

- **Monitor stakeholder involvement consistent with the project plan—partially implemented.** The HART program had a list of stakeholder organizations that it interacts with. In addition, program officials stated that they were monitoring stakeholder involvement through weekly meetings being held to prepare stakeholders that are expected to transition onto the HART system in late 2021.

  However, while the HART Program Management Plan stated that the program would develop a stakeholder management plan to identify stakeholders that could influence or be impacted by HART, and to define the extent to which it should be interacting with each of its stakeholders, the program did not develop this plan.

  Program officials stated that they had consistently interacted with their stakeholders through meetings with various oversight groups and that these groups had existing charters that define the frequency in which the meeting is to occur. However, program officials acknowledged that the charters for some of these groups were outdated and they were currently in the process of revising them. As such, until the HART program defines the extent to which it should be interacting with each of its stakeholders throughout the acquisition process and then monitors stakeholder involvement, the program cannot be certain that it is communicating with all of the appropriate parties that could influence or be impacted by HART.

- **Periodically review and communicate project performance with relevant stakeholders—fully implemented.** The HART program regularly communicated and documented the status of assigned

activities and work products to relevant stakeholders. For example, since the program declared its second schedule breach in January 2020, the program has conducted monthly meetings with senior DHS oversight officials, including the Deputy Under Secretary for Management, to review updates related to the program's contract performance, cost, and schedule information. In addition, the program has held quarterly meetings with senior leadership across OBIM to discuss updates related to the program's performance.

- **Review and document project results at milestones—fully implemented.** The HART program conducted and documented the results of its milestone reviews in acquisition decision memorandums. For example, following the milestone related to reviewing the system's preliminary design for HART increment 1, the program documented that the requirements associated with this milestone were completed. Further, the program documented the action items that were identified during the milestone review in a memorandum to ensure that these items would be addressed prior to the subsequent milestone review.

- **Manage corrective actions on identified issues to closure—fully implemented.** The HART program appropriately documented the corrective actions it took to address issues to closure. In particular, the program collected, analyzed, and documented issues and their associated corrective actions in an issues log. In addition, the program officials updated the status of their testing-related issues during the weekly meetings they had with the contractor.

HART Fully Implemented Two of the Five Selected Requirements Management Practices

According to Capability Maturity Model® Integration for Acquisition, an effective requirements management process helps an agency manage changes to the requirements throughout a program's lifecycle, and ensure continuous alignment of the program's high-level mission and operational requirements all the way down to the lower-level functional and technical requirements to ensure the delivered system will meet its original goals and the needs of its end users. Specifically, effective requirements management practices include (1) establishing an understanding of requirements with program stakeholders; (2) obtaining a commitment to requirements from program stakeholders by assessing the impact of requirements on existing commitments; (3) managing changes to requirements throughout the lifecycle by evaluating the impact of requirements changes from the standpoint of relevant stakeholders; (4) maintaining a clear and discernable association between high-level mission and operational requirements and the lower-level functional and technical requirements (referred to as bidirectional traceability) among program documents, which is typically achieved by using a requirements

traceability matrix or automated requirements management system; and (5) ensuring program plans remain aligned to requirements.

The HART program had fully implemented two of the five requirements management practices and partially implemented three practices. Table 5 lists these selected practices and provides our assessment of the HART program's implementation of the practices, as of February 2021.

Table 5: Summary of the Homeland Advanced Recognition Technology Program's Implementation of the Five Selected Requirements Management Practices

Selected practice	GAO assessment
1. Establish an understanding of requirements with program stakeholders	◑
2. Obtain a commitment to requirements from program stakeholders	◑
3. Manage changes to requirements throughout the lifecycle	●
4. Maintain bidirectional traceability	◑
5. Ensure program plans remain aligned to requirements	●

Legend: ● = Fully implemented ◑ = Partially implemented ○ = Not implemented
Source: GAO analysis of agency data. | GAO-21-386

- **Establish an understanding of requirements with program stakeholders—partially implemented.** The HART program officials established criteria for distinguishing appropriate requirements providers. In addition, program officials established objective criteria for the evaluation and acceptance of requirements and a mechanism for analyzing requirements to ensure that established criteria are met. For example, the program validated the acceptability of high-level requirements (i.e., operational, functional, and nonfunctional requirements) through independent verification and validation testing.[35] Stakeholders also validated and accepted lower-level requirements (referred to as features and user stories) during system demonstration events that occurred every 3 weeks.

  However, as previously discussed, the August 2020 technical assessment of HART's performance issues reported that the program and contractor lacked an understanding of the complexity of the requirements. The assessment also reported that the program had taken certain corrective actions aimed at addressing this issue. For

---

[35]Independent verification and validation provides an objective assessment of a project's processes, products, and risks throughout its lifecycle and helps ensure that program performance, schedule, and budget targets are met.

example, the program conducted functional requirements reviews intended to develop a common understanding of the requirements between the contractor and program officials. These reviews resulted in updating the program's high-level requirements in the *HART Functional Requirements Document*.[36, 37] In addition, as previously mentioned, the program officials were in the process of updating HART's lifecycle cost estimate to support its updated requirements. The officials said they expected the appropriate stakeholders to review and approve the estimate by September 2021. These corrective actions, if fully implemented, will help ensure that the program's requirements are better understood in order to avoid further delays and cost overruns.

- **Obtain commitment to requirements from program stakeholders—partially implemented.** The program's updated high-level requirements were reviewed and approved in the *HART Functional Requirements Document*. This document captured all functional and nonfunctional requirements that collectively make up the HART program. According to the HART requirements manager, the *HART Functional Requirements Document* was first reviewed by all OBIM division directors before being signed by stakeholders (i.e., the HART increment 1 and 2 project manager, the HART program manager, the HART Lead Business Authority, and the OBIM Deputy Director).

  In the fall of 2019, the contractor created a tailoring plan to define steps for obtaining ongoing commitments to lower-level requirements.[38] For example, the program is to hold a 2-day planning session prior to the start of developing the next system release. This

---

[36]The Functional Requirements Document is the central document in the DHS system engineering lifecycle. This document formally identifies the functional requirements for increments 1 and 2 of HART. The functional requirements in the document serve as the foundation of how the increment 1 and 2 solutions will be designed, developed, and tested. More specifically, the document serves as a critical input to the system designs and test cases created in subsequent phases of systems engineering lifecycle.

[37]*Homeland Advanced Recognition Technology Functional Requirements Document for increments 1 and 2* version 1.7, updated June 22, 2020, included 460 functional requirements and 213 nonfunctional requirements.

[38]Agile is a type of incremental development, which calls for the rapid delivery of software in small, short increments rather than in the typically long, sequential phases of a traditional waterfall approach. The HART development model for increments 1 and 2 follows the Scaled Agile Framework model. The Scaled Agile Framework is a governance model for organizations to use to align the product delivery for modest to large numbers of Agile software development teams. More information on the Scale Agile Framework can be found at https://www.scaledagileframework.com.

planning session is to include all development teams, product owners, and stakeholders. By the end of the planning session, all participants are expected to agree to the planned lower-level requirements targeted for development and the associated milestones for completion.

However, as previously discussed, the updated lifecycle cost estimate that supports the program's revised set of functional requirements had not been finalized to account for these changes. As such, the appropriate stakeholders had not committed to the total amount that is required to support all of the program's requirements. Program officials plan to obtain approval of the lifecycle cost estimate by September 2021. Obtaining approval of this estimate will help ensure that stakeholders support the HART program moving forward.

- **Manage changes to requirements throughout the lifecycle—fully implemented.** The HART program managed changes to requirements throughout the lifecycle. Specifically, program officials documented all requirements and requirements changes, as well as maintained a log of the requirements change history. The tracking of requirements changes included a rationale for the change. The HART Requirements Manager stated that the program relied on a board of representatives from OBIM to review new requirements or changes to existing high-level requirements and capture the outcome of these discussions in meeting minutes. For example, according to HART's breach remediation plan, certain functional requirement changes were required to address HART's performance issues, and these changes were reviewed and approved by the board. According to program officials, changes to lower-level requirements did not go through the board's review process. Instead, changes to lower-level requirements were first discussed and agreed upon between the program office and the contractor prior to an evaluation from other relevant stakeholders.

- **Maintain bidirectional traceability—partially implemented.** The contractor maintained clear traceability from high-level requirements down to the lower-level requirements. Specifically, the contractor maintained a requirements traceability matrix that listed all of the high-level requirements captured in the *HART Functional Requirements Document* and the underlying lower-level requirements. The contractor updated and submitted the matrix to the program office for review and acceptance at the end of every major release.

  However, the matrix did not maintain bidirectional traceability from lower-level requirements back up to the high-level requirements. According to an August 2020 technical assessment conducted by DHS's OCIO, only about half of HART's features mapped to high-level

requirements. Program officials stated that this lack of bidirectional traceability was because some necessary features did not directly support a high-level requirement and, thus, traceability of these features were not captured in the matrix.

After we discussed our concerns with the program officials, they stated that the contractor cleaned up the traceability of features to high-level requirements and provided updated documentation to OBIM on these efforts. In addition, program officials stated that modifications to the contract made in August 2020 require the contractor to report additional metrics that OBIM can monitor to ensure full traceability.

However, development work completed since these new measures were put into place continued to lack bidirectional traceability. For example, of the 101 features planned for HART's seventh release, approximately 70 percent lacked full traceability. According to the OCIO's technical assessment, a lack of bidirectional traceability 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 customer's needs upon integration. Until the program establishes and maintains a process to ensure bidirectional traceability in future development, it risks encountering the same challenges identified in the OCIO's technical assessment and also risks the contractor completing work that does not directly support the needs of the government.

- **Ensure program plans remain aligned with requirements—fully implemented.** The HART program ensured that program plans remained aligned with requirements. For example, the program office and contractor officials reviewed project plans, activities, and work products for consistency with new requirements or changes to existing requirements. Specifically, the program relied on System Requirements Reviews, which is one of many types of technical reviews in DHS's systems engineering lifecycle, to identify a baseline for high-level requirements. The program then held meetings to establish interim baselines for lower-level requirements. As changes occurred to requirements, the program revisited its program plans through a formal change proposal with the contractor. The contractor updated and submitted the revised system requirements baseline to the program office for review and acceptance at the end of every major Agile release.

Conclusions

OBIM's reliance on an overextended 27 year old biometric identity management system to support national security, law enforcement, and immigration decisions, emphasizes the critical need for OBIM to ensure that further delays, cost overruns, and performance issues with the HART program are avoided. The delays and issues experienced by HART since 2017 have prolonged DHS's and its partner agencies' dependency on IDENT for at least an additional 3 years beyond the original plan.

The DHS CIO's recent actions to improve the program health assessment process and report accurate ratings to the IT Dashboard will help provide more transparency to DHS, OMB, Congress, and others regarding the risks and issues facing the HART program. Although the OCIO met the TechStat review requirements, the DHS TechStat policy was out of date. Until DHS updates its policy to properly reflect the OCIO processes that should be used to address each of the five TechStat requirements, other departmental IT programs deemed high risk would likely not be readily aware of the specific process requirements.

In addition, while HART program officials fully implemented or had plans in place to fully implement the majority of key risk management practices, until the program (1) keeps records of its discussions related to risk mitigation, including the resources needed for risk handling activities and (2) ensures its risk owners maintain accurate and current status updates for each of its mitigation plans, the program is in jeopardy of not actively monitoring and documenting risks and keeping mitigation plans up-to-date.

Moreover, the HART program's mixed results in implementing IT acquisitions best practices has contributed to an increased level of risk for the program and could result in further implementation delays and cost overruns. Specifically, HART program officials fully implemented half of the 14 practices and had plans under way to address three of the seven practices that were partially implemented. However, until program officials fully implement the best practices of (1) fully reviewing the contractor's work products, (2) monitoring all program costs, (3) monitoring stakeholder involvement, and (4) maintaining bidirectional traceability of requirements, the program risks developing a system that may not meet its partner agencies' needs or experiencing further schedule delays and cost overruns.

Recommendations for Executive Action

We are making the following seven recommendations to DHS:

The Secretary of DHS should direct the Chief Information Officer to update existing policy to reflect the processes that should be used to address each of the TechStat requirements. (Recommendation 1)

The Secretary of DHS should direct the OBIM Director to ensure that the HART program keeps records of its discussions related to risk mitigation, including the resources needed for risk handling activities. (Recommendation 2)

The Secretary of DHS should direct the OBIM Director to ensure that the HART program's risk owners maintain accurate and current status updates for each risk mitigation plan in the risk register. (Recommendation 3)

The Secretary of DHS should direct the OBIM Director to ensure that the HART program office fully reviews and approves or rejects contractor deliverables prior to working on the next system release. (Recommendation 4)

The Secretary of DHS should direct the OBIM Director to ensure that, moving forward, the HART program tracks and monitors all of its costs, including government labor costs. (Recommendation 5)

The Secretary of DHS should direct the OBIM Director to ensure that the HART program defines the extent to which it should be interacting with each of its stakeholders throughout the acquisition process, and, once established, monitors stakeholder involvement against that defined level of involvement. (Recommendation 6)

The Secretary of DHS should direct the OBIM Director to ensure that the HART program establishes and maintains a process to ensure bidirectional traceability of its requirements in future development. (Recommendation 7)

Agency Comments and Our Evaluation

DHS provided written comments on a draft of this report, which are reprinted in appendix II. In its comments, the department concurred with all seven of our recommendations and provided estimated completion dates for implementing each of them.

For example, with regard to recommendation 1, the department stated that the DHS OCIO plans to update and further refine related policy to

reflect the OCIO's processes that address each of the five TechStat requirements. The department said it plans to complete this activity by November 2021.

In addition, for recommendation 4, the department stated that it intends to complete a review of backlogged deliverables for increment 1. Further, with regard to increment 2 development activities, the department stated that the HART program office will fully review and approve, or reject, contractor deliverables prior to working on the next system release. The department stated that it plans to implement these actions by August 2021. If implemented effectively, the actions that DHS plans to take in response to the recommendations should address the issues we identified.

We also received technical comments from DHS, CBP, OBIM, and Transformation Security Administration 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) 512-6151 or walshk@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 III.

Kevin Walsh
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) determine the status of the Homeland Advanced Recognition Technology (HART) program, (2) assess the accuracy of the Department of Homeland Security (DHS) Chief Information Officer's (CIO) risk ratings for the HART program reported on the IT Dashboard and whether the CIO met TechStat review requirements,[1] (3) assess the extent to which the HART program was identifying and managing its risks, and (4) assess the extent to which the HART program was implementing selected information technology (IT) acquisition best practices

To address our first objective, we obtained and reviewed data related to HART's initial, rebaselined, and current cost and schedule estimates. We also reviewed artifacts from the HART program's status reviews, such as monthly briefings to the DHS Deputy Under Secretary for Management and weekly minutes from project team meetings. Further, we reviewed HART's breach remediation plans. In addition, we interviewed knowledgeable officials from the DHS Office of the Chief Information Officer (OCIO), the Office of Biometric Identity Management (OBIM), and HART.

To address the first part of our second objective—to evaluate whether the DHS CIO risk ratings on the IT Dashboard accurately reflect the level of risk associated with HART—we obtained and analyzed OCIO's internal program health assessments and associated risk ratings for HART and analyzed the assessments and ratings against evidence related to program performance that we obtained while addressing the first objective. We used this information to determine if the OCIO health assessment ratings were consistent with the program's actual risks. We also compared the OCIO health assessment ratings to the CIO evaluations on the Dashboard to determine whether the ratings on the Dashboard were current and reflected the risk level associated with HART, as required by the Federal Information Technology Acquisition

---

[1]The Federal IT Dashboard is an Office of Management and Budget website that reports performance and supporting data for major IT investments (see itdashboard.gov). A major IT investment means a system or an acquisition requiring special management attention because it has significant importance to the mission or function of the government; significant program or policy implications; high executive visibility; high development, operating, or maintenance costs; an unusual funding mechanism; or is defined as major by the agency's capital planning and investment control process. A TechStat review is an evaluation of high-risk IT investments to determine whether to terminate or turn around investments that are in danger of failing or are not producing results.

Reform Act[2] and associated Office of Management and Budget (OMB)
implementation guidance.[3]

In addressing the second part of our second objective—to evaluate
whether the DHS CIO met TechStat review requirements to oversee the
HART program—we obtained and analyzed DHS oversight review
documentation for HART to determine if the CIO had assessed the
program against TechStat-related requirements that were identified in the
Federal Information Technology Acquisition Reform Act, the associated
OMB implementation guidance, and the department's related policy on
conducting TechStat reviews for programs that had repeated high-risk
ratings.[4] In particular, we determined the extent to which the HART
program addressed the five following TechStat-related requirements:

1. establish a root cause analysis of performance issues,

2. establish corrective action plans which address the causes,

3. establish a timeline for implementing the corrective actions,

4. use OMB's required "Investment and Portfolio Management Maturity
   Framework" template to conduct an assessment of the program, and

5. provide the results of the TechStat review to OMB.

In addition, for both parts of the second objective, we interviewed
appropriate officials from the OCIO, including the DHS CIO, to obtain
further information regarding HART's IT Dashboard risk ratings and the
use of the office's existing oversight processes to address the
requirements associated with a TechStat review.

To assess the reliability of the cost, risk, and requirements-related data
that were provided by the HART program officials and identified in the
program management and governance documentation for HART, we (1)
analyzed related documentation and assessed the data against existing
agency records to identify consistency in the information; (2) examined

---

[2]*Federal Information Technology Acquisition Reform provisions of the Carl Levin and
Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015*, Pub.
L. No. 113-291, div. A, title VIII, subtitle D, 128 Stat. 3292, 3438-3450 (Dec. 19, 2014).

[3]OMB, *Management and Oversight of Federal Information Technology, Memorandum M-
15-14* (Washington, D.C.: June 10, 2015).

[4]DHS Directive 102-03, *TechStat Accountability Sessions* (Washington, D.C.: May 17,
2017).

the data for obvious outliers, incomplete entries, or unusual entries; and
(3) interviewed knowledgeable program officials about the reliability of the
data provided.

To address the third objective, we assessed the program's risk
management documentation and compared it to the seven risk
management practices identified in the Software Engineering Institute's
Capability Maturity Model® Integration for Acquisition.[5] These practices
included:

- determining risk sources (i.e., fundamental drivers that cause risks in
  a project or organization) and categories (i.e., cost, schedule, and
  contract management);

- defining parameters to analyze (i.e., probability of risk occurrence and
  impact and severity of risk occurrence) and categorize risks;

- establishing and maintaining a risk management strategy;

- identifying and documenting risks;

- evaluating and categorizing each identified risk using defined risk
  categories and parameters, and determining its relative priority;

- developing a risk mitigation plan; and

- monitoring the status of each risk periodically and implementing the
  risk mitigation plan as appropriate.

We obtained and analyzed relevant program artifacts, including risk and
issue logs, risk-level assignments, risk management plans, risk mitigation
plans, weekly status reports, and results of technical reviews.

We assessed the HART program's implementation of the seven risk
management practices as:

- fully implemented, if available evidence demonstrated all aspects of
  the practice;

- partially implemented, if available evidence demonstrated some, but
  not all, aspects of the practice; and

- not implemented, if available evidence did not demonstrate any
  aspect of the practice.

---

[5]Software Engineering Institute, *Capability Maturity Model® Integration for Acquisition*,
Version 1.3 (November 2010).

In addition, we interviewed appropriate program and governance board officials, such as the HART program manager and HART risk manager, to obtain additional information about the program's risks and risk management practices. We also interviewed HART stakeholder groups: the OBIM Executive Stakeholders Board, which included members from the Departments of Defense, Justice, and State; and the HART Increments 1 and 2 Project Integrated Project Team, which included members from OBIM that were outside of the HART program office and other DHS components. We selected these stakeholder groups because they collectively provided representation from key stakeholders associated with the HART program. We obtained their perspectives on the key risks facing the program and the extent to which those risks were being addressed.[6]

To address the fourth objective, we first analyzed the 22 process areas within Capability Maturity Model® Integration for Acquisition and identified those areas which were relevant for assessing the HART program against. From the list of the 22 areas that we considered, we selected process areas associated with maturity level two.[7] Maturity level two establishes the foundation for effective acquisition practices. To narrow our list further, we excluded process areas that were not associated with the project processes category.[8]

For the six areas that remained, we then selected the areas that, based on our professional judgment, were the logical choice for selection given

---

[6]DHS's Office of Program Accountability and Risk Management—DHS's main body for acquisition oversight—developed department-wide risk management processes that acquisition programs are required to follow. For our review, we assessed the HART program against key industry best practices for risk management outlined in the Capability Maturity Model® Integration for Acquisition guide.

[7]Capability Maturity Model® Integration for Acquisition aligns each of its process areas to a maturity level. Maturity levels are a means of improving the processes corresponding to a given set of process areas (i.e., maturity level). The five maturity levels are designated by the numbers 1 through 5: Initial (1), Managed (2), Defined (3), Quantitatively Managed (4), and Optimizing (5).

[8]The 22 process areas in Capability Maturity Model® Integration for Acquisition are associated with one of the following four categories: Project Processes (11), Organizational Processes (3), Support Processes (4), and High Maturity Processes (4). The process areas associated with the Project Processes category contain practices that address acquirer activities related to establishing, executing, and ensuring the transition of an acquisition project. We excluded the remaining process areas associated with the other three categories because those areas included processes and practices that can be applied more generally to the organization.

where the HART program was in its system development lifecycle (i.e., post-contract award and in the system development phase). These areas include: (1) agreement management, (2) project monitoring and control, and (3) requirements management. Collectively, these three process areas identified a total of 20 practices.

From these 20 practices, we selected 14 that, based on our professional judgment, were more important aspects to review given where the program was in its system development lifecycle.[9] In addition, we excluded practices within a process area if another process area also identified a similar practice. Table 6 identifies the three selected acquisition process areas and 14 selected associated practices.

Table 6: Selected Acquisition Process Areas and Selected Associated Practices

Process area	Selected practice
Agreement management	1. Conduct management reviews with the contractor and monitor the contractor's progress related to cost and schedule.
	2. Review the contractor's work products, including confirming that all issues have been corrected and all contractual requirements have been satisfied.
	3. Manage contractor invoices and resolve all errors or issues prior to approval.
Project monitoring and control	4. Monitor actual project progress related to cost and schedule against those identified in the project plan.
	5. Monitor staffing commitments against those identified in the project plan.
	6. Monitor stakeholder involvement, including ensuring relevant stakeholders maintain involvement, consistent with the project plan.
	7. Periodically review and communicate project performance with relevant stakeholders.
	8. Review and document project results, such as action items and decisions, at milestones.
	9. Manage corrective actions on identified issues to closure.
Requirements management	10. Establish an understanding of requirements with program stakeholders.
	11. Obtain a commitment to requirements from program stakeholders by assessing the impact of requirements on existing commitments.
	12. Manage changes to requirements throughout the lifecycle by evaluating the impact of requirement changes from the standpoint of relevant stakeholders.
	13. Maintain a clear and discernable association between high-level mission and operational requirements and the lower-level functional and technical requirements among program documents.
	14. Ensure program plans remain aligned to requirements.

Source: GAO analysis of the acquisition-related process areas and practices identified in Capability Maturity Model® Integration for Acquisition. | GAO-21-386

[9]One of the 14 selected practices is a combination of three individual practices. We combined these practices into one practice because of the overlapping nature of the three practices.

To determine the extent to which the HART program had implemented
the selected IT acquisition practices, we obtained and assessed contract
management, program management, and requirements management
documentation and compared it against each of the selected practices. In
particular, we analyzed the HART increment 1 and 2 system development
contract and associated contract modifications, invoices, contract
deliverables, program management plans, agency-reported cost data,
schedule documentation, milestone review memorandums, issues log,
requirements management plan, and requirements traceability matrix. We
also interviewed program officials, including the HART program manager
and HART requirements manager, to obtain an understanding of the
process in place to manage the program. Further, we discussed with the
officials the program's efforts to implement the selected practices.

Moreover, to determine whether the HART program had managed
contractor invoices and resolved all errors or issues prior to approval, we
first asked the HART program officials to provide us with a list of invoices
that the system development contractor for HART increments 1 and 2 had
submitted between May 2019 and August 2020. The HART program
officials provided us with a list of 33 invoices. Of the 33 invoices, 29 were
associated with an individual Contract Line Item Number and the
remaining four invoices were generally associated with the cost-plus-
fixed-fee portion of the development contract.[10] Given the scope and
resources of our review, we selected the seven most recent invoices
associated with specific Contract Line Item Numbers, and one additional
invoice which was the most recent invoice generally associated with the
cost-plus-fixed-fee portion of the development contract. Accordingly, we
selected a total of eight invoices to review. We evaluated the selected
invoices to determine whether the HART program office and contracting
officials reviewed and approved these invoices.

We assessed the HART program's implementation of the 14 IT
acquisitions practices as:

- fully implemented, if available evidence demonstrated all aspects of
  the practice;

- partially implemented, if available evidence demonstrated some, but
  not all, aspects of the practice; and

---

[10]A cost-plus-fixed-fee contract provides for payment to the contractor of a negotiated fee
that is fixed at the inception of the contract.

- not implemented, if available evidence did not demonstrate any aspect of the practice.

We determined that the data used to support the findings in this report were sufficiently reliable for the purposes of our reporting objectives, with the exception of the agency-reported HART spending information. Specifically, we determined that the spending data provided by the HART program officials were not complete and reliable. With regard to the spending data provided by the HART program officials, the data were incomplete because they did not include information related to all government-related costs since DHS initiated the program in 2016. In addition, the HART spending data reported to the IT Dashboard were not reliable because the data also included the operations and maintenance costs for IDENT. We discuss the limitations of these data in the report. We have also made appropriate attribution indicating the sources of the data.

We conducted this performance audit from January 2020 to June 2021 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: Comments from the Department of Homeland Security

Homeland
Security

May 18, 2021

Kevin Walsh
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-21-386, "HOMELAND
       SECURITY: DHS Needs to Fully Implement Key Practices in Acquiring
       Biometric Identity Management System"

Dear Mr. Walsh:

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.

The Department is pleased to note GAO's positive recognition of the DHS Office of the
Chief Information Officer's (OCIO) recent actions to improve the program health
assessment process in May 2020 and report accurate ratings to the Information
Technology (IT) Dashboard in November 2020, which provides increased transparency
to DHS, the Office of Management and Budget (OMB), Congress, and others regarding
the risks and challenges facing the Homeland Advanced Recognition Technology
(HART) program. Once deployed, the HART system will provide an extremely capable
platform for delivery of biometric services to customers across the Department and to our
mission partners. It is important to note that the HART team made significant progress
on foundational elements, including efforts which set the stage for: (1) parallel
operations of the Automated Biometric Identification System (IDENT) and HART; (2)
operational assessment; and (3) HART Initial Operational Capability. The HART
program is working closely with its DHS and external stakeholders as these development
and test activities continue.

It is also important to note that the Department's Office of Biometric Identity
Management (OBIM) closely monitors costs and funding related to the HART program.

OBIM does not believe that tracking and monitoring combined Government-related labor costs for IDENT and HART is a significant transparency concern. All OBIM staff will support both programs through the operation and disposal of IDENT and development and operation of HART, as HART is the replacement for IDENT. Further, funding data is presented to DHS stakeholders, OMB, and Congress through other mechanisms, such as the Enterprise Architecture Board, the Acquisition Review Boards, and Congressional Budget Justfication materials and briefings, which ensures transparency with these stakeholders.

DHS remains committed to incorporating feedback to improve its program management and oversight processes. The Department will continue to provide its stakeholders with current and accurate cost and funding data through existing mechanisms and will continue to address the IT Dashboard on a continuing basis.

The draft report contained seven recommendations with which the Department concurs. Attached 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,

RANDOLPH D ALLES Digitally signed by RANDOLPH D ALLES
Date: 2021.05.18 06:11:54 -07'00'

R. D. Alles
Deputy Under Secretary for Management

Attachment

2

**Attachment: Management Response to Recommendations
Contained in GAO-21-386**

GAO recommended that the Secretary of DHS direct the Chief Information Officer to:

Recommendation 1: Update existing policy to reflect the processes that should be used to address each of the TechStat requirements.

Response: Concur. OCIO's Chief Techology Officer Directorate will develop updates and further refine the related policy to reflect the OCIO processes that address each of the five TechStat requirements, and which also drive positive program performance across the Department. This policy will establish these OCIO processes as the ongoing method by which TechStat activities will be addressed within the DHS Acquisition Lifecycle Framework. Estimated Completion Date (ECD): November 30, 2021.

GAO recommended that the Secretary of DHS direct the OBIM Director to:

Recommendation 2: Ensure that the HART program keeps records of its discussions related to risk mitigation, including the resources needed for risk handling activities.

Response: Concur. OBIM will retain meeting minutes for Government HART Risk Meetings and the HART System Integrator Risk Meeting, which include discussions related to risk mitigation and resources needed for risk handling activities. ECD: November 30, 2021.

Recommendation 3: Ensure that the HART program's risk owners maintain accurate and current status updates for each risk mitigation plan in the risk register.

Response: Concur. The OBIM and HART Risk Management plans currently require that risk owners "ensure risks are updated every 30 days for high priority risks, every 60 days for medium priority, and 90 days for low priority risks, or more frequently as warranted." Consequently, the OBIM Risk Managers will develop a methodology to ensure that each risk is updated pursuant to this guidance, and that all mitigation actions will be kept current. ECD: June 30, 2021.

Recommendation 4: Ensure that the HART program office fully reviews and approves or rejects contractor deliverables prior to working on the next system release.

Response: Concur. DHS OBIM will first complete a review of backlogged deliverables for Increment 1, then will implement an approach for Increment 2 development activities in which the HART program office fully reviews and approves, or rejects, contractor deliverables prior to working on the next system release. ECD: August 31, 2021.

3

Recommendation 5: Ensure that, moving forward, the HART program tracks and monitors all of its costs, including government labor costs.

Response: Concur. OBIM already closely tracks and monitors all of its program office support, acquisition, and operations and maintenance costs. For example, OBIM tracked program office support costs, which capture Government labor costs, for the entire office. However, this tracking did not separately break this information out within the model until late fiscal year (FY) 2020. Therefore, all OBIM's future models will include a separate breakout for program office support, including IDENT and HART Government labor costs. The HART re-baseline Life Cycle Cost Estimate for FY 2021 will include the separate IDENT and HART Government labor costs. ECD: September 30, 2021.

Recommendation 6: Ensure that the HART program defines the extent to which it should be interacting with each of its stakeholders throughout the acquisition process, and, once established, monitors stakeholder involvement against that defined level of involvement.

Response: Concur. Currently, OBIM monitors stakeholder involvement through formal existing mechanisms, such as the quarterly Executive Stakeholders Board and Executive Steering Committee. OBIM also utilizes working-level engagements via dedicated OBIM points of contact for each stakeholder organization, as well as weekly meetings of the HART Increments 1 and 2 Integrated Project Team and Working Group meetings such as Customer Migration, which are part of OBIM's ongoing stakeholder management process. OBIM will also conduct a review to determine which stakeholders are not participating in meetings and will take further action as appropriate, such as defining a required extent of interaction with stakeholders and monitoring stakeholder involvement . ECD: December 31, 2021.

Recommendation 7: Ensure that the HART program establishes and maintains a process to ensure bidirectional traceability of its requirements in future development.

Response: Concur. To maintain backward traceability of system level requirements and tests back to the higher level requirements provided by the Government, OBIM will work with the development contractors to ensure that user stories and features are properly tracked back to the Government requirements and, if such traceability does not apply, provide an explanation and rationale for why backward traceability is not necessary in certain cases (e.g., enabler features). OBIM requirements staff will then review the contractor deliverables and flag any issues with reverse traceability, and will address these issues with contractors, as appropriate. OBIM will also add accurate and consistent reverse traceability to the requirements traceability matrix and system requirements document acceptance criteria. ECD: October 29, 2021.

4

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contact	Kevin Walsh, (202) 512-6151, walshk@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), Javier Irizarry (analyst in charge), Mathew Bader, Chris Businsky, Rebecca Eyler, Jarek Frankovich, Andrew Knox, Jonah Silencieux, and Andrew Stavisky.