GAO@100 Highlights

Highlights of GAO-21-386, a report to congressional requesters

June 2021

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DHS currently uses an outdated system, implemented over 27 years ago, for providing biometric identity management services (i.e., fingerprint matching and facial recognition technology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.

View GAO-21-386. For more information, contact Kevin Walsh at (202) 512-6151 or walshk@gao.gov.

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