

DHS Office Transitions to New Biometric Identification System

The Office of Biometric Identity Management's new HART system, the largest of its kind, to help secure the nation.

[Connor Collins](#)

Fri, 05/24/2019 - 09:43



Photo credit: dem10/iStock

As federal agencies across the board focus on IT transformation, one Department of Homeland Security office is spearheading the important transition for the largest biometric identification database in the federal government to better execute its mission.

The [Office of Biometric Identity Management](#) (OBIM) is leading the transition for the government's biometric identification system used by a variety of federal customers to help secure the country, among other things. OBIM's efforts center around the

transition from the old Automated Biometric Identification System (IDENT) to the new Homeland Advanced Recognition Technology (HART) system.

DHS established IDENT in 1994 with limited technology available. Since then, the system has grown into the “largest automated biometric identification system in the U.S. government,” according to OBIM, which runs IDENT and will run HART. However, propping up IDENT’s older architecture comes at a cost, one that OBIM and DHS seek to solve with HART.

If the transition seems simple, consider the size of the enterprise involved and all of the stakeholders.

In terms of scale, in fiscal year 2017, IDENT held over 220 million unique biometric identifiers, processed more than 320,000 biometrics-related cases daily and executed prioritized queries “in less than 10 second with 99.7 percent accuracy,” according to OBIM.

Most people may think of fingerprints as the prime example of biometrics, but it includes much more.

“A biometric is a measurable physical characteristic or personal behavior trait used to recognize the identity or verify the claimed identity of an individual. The most common biometrics in use in the security market today include fingerprints, facial image or iris scans,” according to the [DHS Biometrics Strategic Framework](#) for 2015 to 2025 and originally released in June 2015.

David Grauel, OBIM’s replacement biometric system (RBS) program manager, recently discussed the changeover from IDENT to HART at Connect:ID 2019 April 30. In addition to giving an overview of OBIM and HART, Grauel emphasized a shift in focus from on-premises data centers to the cloud with a specific objective to remain cloud-agnostic over time.

“We are making a significant strategic shift from our enterprise data centers into the government cloud,” Grauel said. Grauel’s organization is starting with the Amazon Web Services GovCloud. Other federal agencies like the Small Business Administration have prioritized the move to the cloud and analyzed [the pros and cons of different cloud strategies](#).

These cloud capabilities diverge from the hardware-focused workload of the current

system, especially for fingerprint services, which are currently based on high performance hardware matching, according to Grauel. Cloud services will allow OBIM to more easily scale up and down during surges and lulls in requests to process biometric identification.

HART and the move to the cloud also comes with security considerations. Grauel referred to his organization's approach to cybersecurity as cyber resilience. Certainly personally identifying biometric data — including on U.S. citizens — must be secured to the highest degree possible. Privacy is another crucial and related aspect.

"We have taken a very serious stance on privacy. We've got a dedicated privacy team within our organization," Grauel said.

In terms of overall HART progress so far, Grauel said the team has completed approximately 90 sprints with seven agile teams using the agile development framework and is currently finalizing infrastructure development for data migration.

Grauel emphasized that OBIM is excited about the promise that HART and other transformational IT initiatives like the move to cloud computing will enable it to expand and improve its offerings to better service its customers, including many of the law enforcement and homeland security organizations that rely on OBIM's systems.

[View printer friendly version](#)
[identity management](#)

[DHS](#)

[national security](#)

[security](#)

[privacy](#)

[Standard](#)