DHS Office of Procurement Operations

Mission Systems Lifecycle Support (MSLS)

Industry Day Presentation

October 30, 2019

Homeland
Security

Welcome

Tracy Miller, Contracting Officer

DHS Office of Procurement Operations

Agenda

I. Welcome

II. Opening Remarks

III. MSLS Overview

IV. Acquisition Timeline

V. Question & Answer Panel

Purpose

The purpose of this Industry Day event is to:

•Provide our industry partners with a better understanding of OBIM history, and requirements for the MSLS effort.

•Provide a high-level timeline for the upcoming procurement and execution of the MSLS contract.

•Provide an opportunity for OBIM and OPO to strengthen the requirement by listening to industry feedback.

Ground Rules

- Speakers will go through each of their presentations, followed by a question and answer period at the end of all presentations.
- DHS will attempt to address questions that are presented today.
- The remarks, explanations, and information provided at this Industry Day are intended to assist Industry in gaining greater understanding of OBIM objectives as they relate to the MSLS effort and to exchange ideas with Industry in order to improve DHS' ability to achieve desired outcomes.
- The information presented during Industry Day discussions regarding stated requirements and procurement planning are subject to change prior to the issuance of the solicitation.

Opening Remarks

- Shonnie Lyon, OBIM Director

Mission Systems Lifecycle Support (MSLS)

Scott Shockey, MSLS Product Owner

DHS Office of Biometric Identity Management (OBIM)

Who We Are

The Value of Biometrics to DHS

- Positively confirm the claimed identity of a traveler, worker, benefit applicant, or detainee
- Alert that an individual has derogatory information associated with their biometrics
- Inform that an individual previously claimed a different persona

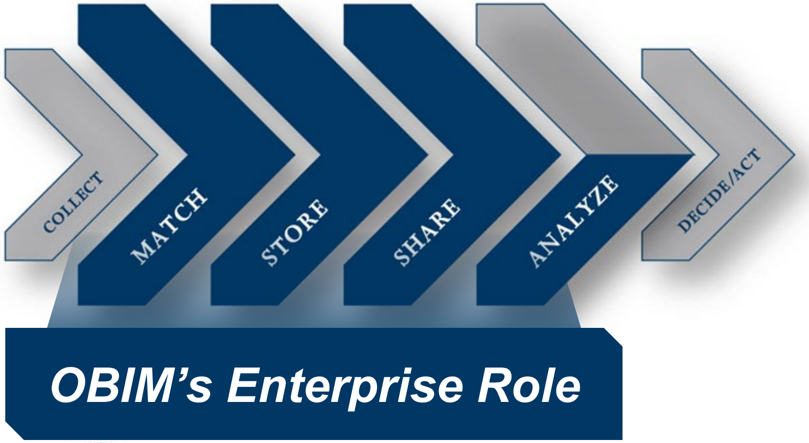
Immigration and Border Management	Law Enforcement	Defense and Intelligence	Credentialing

OBIM Identity Services Enabling Operations

- Operation of multimodal Automated Biometric Identification System (IDENT)

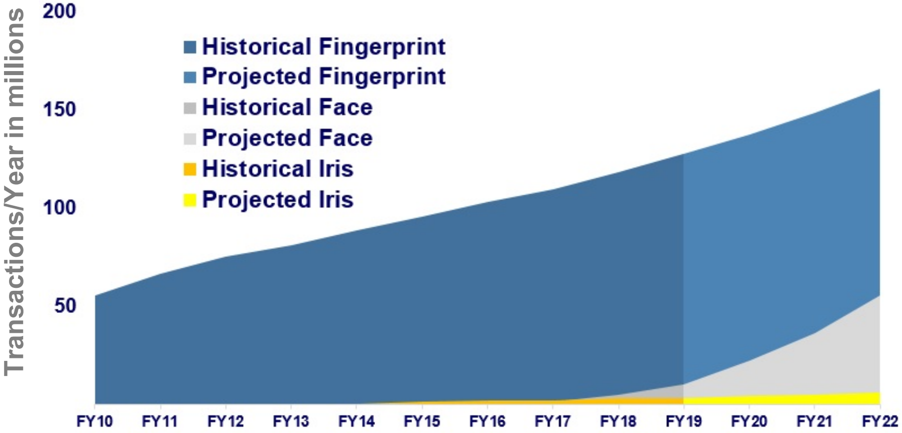
- Manual fingerprint examiner verification services where automation is insufficient
- Coordination with data owners for maximum information sharing

Biometric Continuum



OBIM's Enterprise Role

Growth of Biometrics in DHS



IDENT Gallery Size – 259M+ Unique Identities

OBIM Portfolio of Systems

The OBIM Portfolio includes the following:

- IDENT is OBIM's operational biometric system for rapid identification and verification of subjects using fingerprints, iris, and face modalities.
  - Basic IDENT functionality is to receive and store a set of subject data (fingerprints, a facial photo, and unique biographic identification data, such as name, date of birth, gender, and citizenship) from a component (stakeholder system), search the repository for prior encounters, create a record of the new encounter, and return search results to the end user or stakeholder system.
  - IDENT includes Biometric Support Center (BSC) and end user tools such as Candidate Verification Tool (CVT), AWARE Face Work Bench, Cogent Automated Biometric Identification System (CABIS) and the Secondary Inspection Tool (SIT) for further validation of biometric information.

- HART is the replacement system for IDENT
  - HART builds upon the foundational functionality within IDENT within the Amazon Web Services (AWS) Federal Risk and Authorization Management Program (FEDRAMP) certified environment.
  - Cloud agnostic application architecture based on microservices.
  - Cloud-based biometric matching; shifting focus from specialized hardware to software.
  - Layered security approach for the modern threat landscape.
  - Enhanced privacy protections and compliance.
  - HART also includes SIT and CABIS for further validation of biometric information.

OBIM Portfolio of Systems

The OBIM Portfolio includes the following:

- Program Support Systems (PSS) (Serena, TRACs, Remedy) consists of the suite of tools that support OBIM's mission systems.
  - These tools compliment the development lifecycle and include COTS and DHS-managed tools that support development, testing, monitoring, knowledge management, and requirements functions
  - PSS functionality will be migrated to AWS FEDRAMP or enterprise offerings.
- Automated Real-Time Identity Exchange System (ARIES) is an information exchange architecture with AWS FEDRAMP to support biometric exchanges between the Government of Mexico and DHS.
- Operational Data Store/Operational Data Reporting (ODS/ODR) is an AWS FEDRAMP reporting capability for IDENT information.
- Biometric Marketplace within HART Development and Test Environment (DTE) is an environment to demonstrate various biometric solutions.
  - Biometric marketplace will allow for multiple vendor testing to incorporate new biometric modalities & matching vendors/algorithms.

Mission Systems Capabilities

Objective

Provide development and maintenance support for the existing OBIM mission critical systems following the Scaled Agile Framework (SAFe®) and DevSecOps processes and tools.

- System Enhancements
- New Capabilities

System Enhancements

Actions

Facilitate the continued development, troubleshooting, operations, maintenance, configuration, and applications within the OBIM infrastructure to include:

OBIM Portfolio of Systems	System Type	System Status
IDENT (Legacy System) - Automated Biometric Identification System including SIT	Mission System	Operational in DHS Datacenters
HART - Homeland Advanced Recognition Technology System including SIT	Mission System	Under Development in FedRAMP Certified Commercial Cloud
PSS - Program Support Systems (Serena, TRACs, Remedy)	Mission Support Systems	Operational in DHS Datacenters
ARIES - Automated Real-Time Identity Exchange System	Mission System	Under Development in FedRAMP Certified Commercial Cloud
Operational Data Store/Operational Data Reporting (ODS/ODR)	Mission System	Operational in FedRAMP Certified Commercial Cloud
Biometric Marketplace within HART Development and Test Environment (DTE)	Mission Support Systems	Under Development in FedRAMP Certified Commercial Cloud
All additional systems developed under this contract (BSC Tools, HART web portal, mobile applications)	Mission Systems	To Be Developed in FedRAMP Certified Commercial Cloud

System Enhancements

Actions

- System Requests address perfective, adaptive, corrective, preventative, and security related changes to all OBIM systems.
    - Encompass application support to maintain the mission systems to include BSC and end user tools.
    - Changes are a continuous development functions and should not be bundled with new capabilities releases.
- Existing Service Requests, also known as Onboarding Requests, facilitate the use of existing OBIM IDENT Exchange Messages (IXM) services, to deliver biometric and biographic services to external organizations.
    - Existing service requests can also be utilized to support customer and stakeholder testing activities that require no development support, as well as to make configuration modifications for stakeholders currently using OBIM's IXM services.
    - Existing services do not need to be tied to release cycles and are delivered pending successful user acceptance testing and approvals through OBIM Change Management processes.
- Emergency Request address corrective system changes that can be deployed as an emergency release on an as needed based on criticality of the corrective fix or need being addressed.
    - These releases must be delivered following emergency change request criteria defined within the DHS Infrastructure Change Control Board (ICCB).

New Capabilities

Actions

- New Capabilities are large or complex requirements for enhancing an OBIM operational systems to meet baseline and new customer/partner mission needs.
  - New capabilities are identified and prioritized by the Government following Agile and DevSecOps Methodologies.
  - Development cycles for new capabilities shall be planned on a set frequency approved by OBIM.
  - Examples of new capabilities are listed below.
    - BSC Examination Tools
    - HART Portal and ARIES
    - Reporting and Analytics
    - Person-Centric Enhancements
    - Mobile Applications
    - Additional Biometric Modalities

New Capabilities: BSC Examination Tools

Objective

Generate Biometric Support Center (BSC) capabilities to expand tools and capabilities to biometrically verify candidates, support biometric examiner multimodal biometric analyses and decision making, support derogatory information case management.

Actions

1. Enhance the platform for use by the BSC that utilizes HART services to provide biometric examiners with the ability to review multimodal biometrics and make identity adjudications to expedite current OBIM process flows.
2. Enable users with identity maintenance functions, biometric data corrections capabilities, biometric record review, latent fingerprint processing, and Quality Assurance processes.
3. Create a prioritization and alert workflow within the examination tool enables OBIM with positive control over the order, urgency, and tasking of incoming requests.
4. Provide examiners and leadership with production-like training on the use and proper administration of the generated tool.
5. Perform emergency requests to enable corrective system changes that can be deployed as an emergency release on an as needed based on criticality of the corrective fix or need being addressed.

New Capabilities: HART Portal

Objective

Generate a web-based portal to increase the utilization of HART services and facilitate scalable interoperability with international and domestic partners.

Actions

1. Create a portal that is a configurable, authorization-based web user interface that will improve the user experience by providing a single point of access to HART services and data, streamlining customer onboarding, and reducing the amount of time and effort needed to perform required tasks.
2. Enable users with the ability to execute HART biometric, biographic, identity management, and notification services through role-based administration.
3. Create a tool for the administration of business rules management and service request provisioning to assist with the automation of onboarding activities and routine stakeholder maintenance.
4. Provide a bulk data load user interface that allows a user to import batches of records in supported formats and create IXM service requests for submission.
5. Generate a interface that allows provisioned users to retrieve data from HART and make data corrections.

New Capabilities: Reporting and Analytics

Objective

Generate analytical & reporting capabilities to provide the ability to perform pre-defined and ad-hoc analyses and reporting based on OBIM's existing data warehouse and data mart.

Actions

1. Enable authorized users with an interface to access HART data for the purposes of creating standardized and on-demand reporting capabilities.
2. Allow for the creation of customized queries in multiple export formats that can be quickly generated without impacting production systems.
3. Enable OBIM internal and external users with the ability to run on-demand reports and queries against HART data that are properly filtered in accordance with predefined business rules.
4. Provide analytical features to allow for the identification of patterns and trends using HART data. These patterns include, but are not limited to, potential fraud, data anomalies, migration patterns, and identity discrepancies.
5. Generate methods for business rule pattern and trend identification, biometric image problem detection, capacity planning and forecasting, and trigger based notifications.

New Capabilities: Person Centric Enhancements

Objective

Generate person centric service capabilities to provide a holistic view of identities to assist customer adjudication and decision making related to access, credentials, or benefits.

Actions

1. Enable back-end and user interface enhancements that improve the presentation of HART data, improve data integrity, and provide data from systems interoperable with HART.
2. Provide identity resolution services to perform automated or examiner-assisted identity resolution services based on triggering system events, such as receipt of additional or better quality biometrics or biographic information.
3. Enable indications when other systems contain information about a person's identity as well as a link to certain systems that HART is interoperable with (e.g. ADIS, NGI).
4. Configure organized service responses according to customer business rules to enable a person centric view of the identity data contained within the HART system.

New Capabilities: Mobile Applications

Objective

Develop mobile application capabilities to facilitate identity services, identity sharing and reporting capabilities.

Actions

1. Enable role-based access and configuration capabilities that allow for access to HART services from government approved mobile devices using a secured connection.
2. Provide the ability to for an authorized user to access standardized and custom reports through a mobile platform.
3. Enable a user with the ability to access authorized HART data through a mobile platform execute import/export file functions and batch uploads/downloads in multiple formats.

New Capabilities: Additional Biometric Modalities

Objective

Expand OBIM to enable additional biometric matching modalities for its stakeholders based on prioritization and mission need.

Actions

Perform the proper development, integration activities, testing, evaluation, threshold tuning, and accuracy studies necessary to enable the following biometric modalities:

1. Contactless Fingerprints
2. Palm Prints
3. Scars, Marks, and Tattoos (SMT)
4. Voice
5. Deoxyribonucleic Acid (DNA)
6. Other biometric modalities as required.

Mission Systems Lifecycle Support (MSLS)

Douglas Hansen, Solutions Architect

DHS Office of Biometric Identity Management (OBIM)

SAFe® and DevSecOps

Methodologies

Execution of the scope of this effort will be performed using SAFe® and DevSecOps methodologies in adherence to the DHS Acquisition Directive 102 Systems Engineering Lifecycle.

SAFe®

- Participate with the Government and other Contractors in a team-based, Scaled Agile Framework® (SAFe®) approach to deliver mission value frequently, cost-effectively, responsively, and with high quality.
- Alignment to the latest SAFe® approach at the time of contract award.
- Incorporate proposed DHS Acquisition level agile ceremonies as required within the DHS Acquisition Directive such as Program Increment Planning events, Release Planning Reviews (RPR), and Release Readiness Reviews (RRR) for releases.
- Define how SAFe® will be tailored to support acquisition through a government-approved SAFe® Tailoring Plan.

SAFe® and DevSecOps

DevSecOps

- Focus on communication, integration, and collaboration for rapid deployment of releases for OBIM's mission critical systems within the SAFe® framework focusing on the tight integration of security practices, development, and operations.
- Use common automated testing and development processes to enhance the efficiency and maintainability of existing development, security, and operational processes.
- Establish practices to enhance collaboration with OBIM government and contractor team members that concentrate on security throughout the engineering lifecycle of development activities.

CI/CD Pipeline

- Establish and maintain a robust OBIM-approved Continuous Integration/Continuous Delivery (CI/CD) pipeline and processes using government approved tools.
- Practice frequent check-in of code using an online development environment where code is stored, scanned for quality and security compliance, reviewed by team members, and subject to change by more than one person in short periods of time.

SAFe® and DevSecOps

CI/CD Pipeline continued

- Manage version control of code to reduce any potential issues.
- Utilize automated builds to compile computer code daily, scan for quality and security compliance, run tests, deploy software to production, and create documentation.
- Automate builds linking code together in a pre-defined manner.
- Follow continuous integration practices for frequent integration of code (e.g., hourly, or at least once daily) into a shared master code repository within a government approve tool.
- Code integration is verified by automated builds and tests to detect any integration errors automatically.
- Implement automated code quality scans, security scans, and a full suite of testing, and deployment activities within the CI/CD pipeline.
- Maintain dashboard and fully automated reporting functionality to support CI/CD pipeline results for builds.

SAFe® and DevSecOps

Milestones

Agile Release Train creation and execution of ceremonies and milestone events in adherence to SAFe®.

Program Increments

- 3 month or less Program Increments (PIs).
- PI Planning Event for demonstration of business context, current roadmap and vision, executive briefing and architecture briefing and features of the program backlog incorporating DevSecOps for multiple small deployments.
- The Innovation and Planning (IP) Iteration occurs every Program Increment (PI) and serves multiple purposes. It acts as an estimating buffer for meeting PI Objectives and provides dedicated time for innovation, continuing education.
- Inspect and Adapt (I&A) events to demo the solution and identify improvements for the backlog.

SAFe® and DevSecOps

Releases

- Releases can and should occur throughout Program Increments.
- Release Planning Reviews (RPRs) will be conducted to present the planning information for each new capabilities or perfective maintenance release and demonstrate the specific features/capabilities to be delivered in that release and the order of build and dependencies, and prioritized release backlogs including stories in just enough detail and the work to execute the stories has been estimated.
- Release Readiness Reviews (RRRs) will communicate that all work scoped during RPR has been through the documented definition of done and evaluate scope and metrics against Program Increment (PI) plans and estimates.

Acquisition Timeline – OPO

- November 2019
  - Updated FBO Announcement w/ copy of slides and Government Responses during Q&A
- December 2019
  - Updated FBO Announcement indicating MSLS Acquisition Strategy
  - Draft Solicitation Issued
- January 2020
  - Final Solicitation Issued
- June 2020
  - Award

Question and Answer (Q&A) Panel

- OBIM
  - Scott Shockey, MSLS Product Owner
  - Douglas Hansen, Solutions Architect
  - Joel Robinson, Branch Chief, A&E
  - Ryan Koder, Branch Chief, SBO
- OPO
  - Tracy Miller, Contracting Officer

Thank you for attending the MSLS Industry Day!