DEPARTMENT OF HOMELAND SECURITY
OFFICE OF PROCUREMENT OPERATIONS
MISSION SYSTEMS LIFECYCLE SUPPORT (MSLS)

THIS IS A SOURCES SOUGHT AND REQUEST FOR INFORMATION (RFI) ONLY. This Sources Sought and RFI is issued solely for information and planning purposes and does not constitute a solicitation. Nonetheless, submitters should properly mark their responses if the information is confidential or proprietary. Furthermore, those who respond to this RFI should not anticipate feedback with regards to its submission other than acknowledgment of receipt, should the submitter request an acknowledgement. Responses to this notice are not offers and cannot be accepted by the Government to form a binding contract. All submissions become the property of the Federal Government and will not be returned. Responders are solely responsible for all expense associated with responding to this request.

INTRODUCTION

The Office of Biometric Identity Management (OBIM) of the Department of Homeland Security (DHS) stores and analyzes biometric data, digital fingerprints, iris scans, and photographs, and links that data with associated biographic information to identify and enroll identities and subsequently match or verify the established identities. This provides OBIM with actionable information on immigration violators, criminals, and known or suspected terrorists and supports immigration management and border security decision makers. OBIM’s biometric identification and analysis services are used by DHS, other Federal agencies, State and local law enforcement, the intelligence community, and international partners to support counterterrorism, immigration and law enforcement, and credentialing efforts pertaining to identity services.

PURPOSE

The purposes of this Sources Sought and RFI are:

1) To identify vendors capable of developing and implementing the capabilities described in Section II, Sources Sought; and

2) To collect information from industry identifying products, solutions, and methodologies (including mature modifiable commercial products) supporting the outcomes and capabilities described in Section III, Request for Information.
Information submitted will help DHS in determining an appropriate acquisition strategy and may be utilized in the preparation of a future solicitation, provided DHS finds it in its best interest. Vendors are encouraged to review this RFI and determine if their competency meets DHS requirements.

I. Background

The Department of Homeland Security (DHS) Office of Biometric Identity Management (OBIM) is the designated lead entity within DHS for biometric identity services. OBIM matches, stores, shares, and analyzes biometric and associated biographic data to provide accurate, timely, and high assurance biometric identity information and analysis to DHS and its mission partners.

OBIM’s biometric identity services are enterprise-level capabilities that support national security and public safety and enable operational missions across DHS Components including Customs and Border Protection (CBP), the Transportation Security Administration (TSA), the Federal Emergency Management Administration (FEMA), Immigration and Customs Enforcement (ICE), United States Coast Guard (USCG), United States Citizenship and Immigration Services (USCIS), DHS Management Directorate, and the United States Secret Service (USSS). OBIM helps decision makers reach determinations on whether individuals pose a risk to the United States--by helping identify known or suspected terrorists, immigration violators, criminals and other national security threats--and helps determine whether individuals meet the requirements for a specific Government benefit or credential.

OBIM’s biometric identity services customers include a variety of users within DHS, as well as interagency customers. OBIM provides comprehensive biometric identity information through interoperability and biometric data sharing with the Department of Justice (DOJ) and its Next Generation Identification (NGI) system and the Department of Defense (DoD) and its Automated Biometric Identification System (ABIS). OBIM engages in information sharing with the Department of State (DOS) Consular Consolidated Database and has information sharing agreements with several foreign governments as well as State, local, tribal, and territorial law enforcement agencies.

The OBIM Portfolio of Systems includes the following applications:

- **IDENT (Legacy System) - Automated Biometric Identification System:** IDENT is OBIM’s legacy biometric processing 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 also includes a Secondary Inspection Tool for further validation of biometric information. IDENT is currently deployed within the DHS Data Centers.

- **HART (Replacement System) - Homeland Advanced Recognition Technology System:** HART is the replacement system for IDENT. HART has built upon the foundational functionality within IDENT with Amazon Web Services (AWS) Federal Risk and
OBIM is currently in the process of developing the HART system as its next generation identity management system. HART will reside in the Amazon Web Services (AWS) FedRAMP certified GovCloud. Data will be stored in PostgreSQL databases for textual data and Amazon S3 data stores for image data. HART will feature a microservice architecture based on RedHat OpenShift. Biometric matching capabilities for fingerprint, iris, and facial matching will be integrated with HART in the AWS GovCloud. The initial implementation of HART will operate through system-to-system interfaces to systems owned and operated by other DHS Components and by OBIM’s interagency partners. The initial implementation of HART will also include a minimal user interface for system management and performance monitoring purposes only and will not provide end user access to the HART’s biometric search, retrieval, matching, and maintenance capabilities.

II. Sources Sought

OBIM is seeking sources for the services necessary to develop, integrate, and implement capabilities for the OBIM Portfolio of Systems.

OBIM requests that respondents identify those features listed within items A through F below that are within their development and implementation capabilities. OBIM also requests that respondents identify contracts and contract type under which they have delivered these capabilities. PLEASE NOTE: DHS understands that RFI submissions may include subcontracting / teaming arrangements. In order for DHS to conduct a proper and thorough analysis, all submissions shall clearly delineate which company contains the capability/experience in the particular feature set (i.e. prime, teaming partner, subcontractor).

Responses to this section, Section II Sources Sought, are limited to a total of ten (10) pages.

A. Biometric Examiner Tools. OBIM will replace the software tools used by OBIM’s Biometric Support Center Examiners to resolve matches of biometrics captured at the
point of contact, to biometrics stored in IDENT or HART. OBIM is open to biometric examination tools operating on any type of platform. Examiner tools must enable operations which include fingerprint, iris, and face matching modalities. OBIM may implement additional modalities such as DNA; palm print; voice; scars, marks, and tattoos; contactless fingerprint; and other emerging biometric modalities. Biometric Examiners will also require tools capable of operating with any added modalities. Tools should be able to analyze an individual modality and analyze multiple modalities in conjunction with each other based on business rules. Key features of Biometric Examiner tools will include:

a. Biometric enrollment and search – both biometric and biographic
b. Examiner comparison verification
c. Identity resolution/maintenance
d. Examiner Training
e. Reporting

B. Web Portal. Initial access to HART functionality does not include an interface for end-user desktop access. OBIM will implement a web portal providing desktop access to biometric functionality. Portal features will enable end-user access to biometric capabilities including:

a. Identity services – access to internal back end identity services including biometric retrieval and matching, biographic retrieval, management, notification, and generation of fingerprint cards by encounter
b. User interface – configurable views and user access
c. Data sharing
d. Configuration and service request provisioning
e. Training

C. Reporting. OBIM will implement capabilities for creating user-defined reports, executing those reports, and returning results to the requestor. Report types will include:

a. Ad-hoc reports – one-time reports specified and submitted by end-users through a web portal with results returned to the submitter.
b. Pre-defined reports – capability accessible through a web portal to define reports, retain report definitions, and subsequently execute those reports through an automated schedule or in response to a request submitted through a web portal. Report results can be directed to an individual requestor, to web sites for posting, or to pre-defined distribution lists.

D. Analytics. Analytics will provide the capability to perform analyses of data resident in PostgreSQL and Amazon S3 databases in response to requests initiated through a web portal. These analyses may be implemented using big data technologies and may include items such as:
a. Detection of cases of identity fraud, resolution of cases of identity or biographical mix-up, and identity recognition
b. General data analytical processing
c. Graphical representation and display of analytical results

E. Person-Centric Capabilities. OBIM will enhance biometric applications with person-centric capabilities that will enable identity search, matching, and retrieval operations to assemble all available information resident within system databases and within the databases of OBIM’s DHS Component customers and interagency partners to present a comprehensive profile of the subject of an identity operation. This profile will be made available to OBIM’s DHS customers and interagency partners at the point of contact. Features of this capability will include:
   a. Identity resolution services
   b. Identity directory
   c. Person-centric enhancements

F. Mobile Applications. In addition to providing access to biometric services and features through a web portal with an interface designed for desktop and laptop computers, OBIM will also develop a user interface designed for mobile devices such as tablets and smartphone devices. Features of this mobile interface will include:
   a. Configurable views and user access options customized to device characteristics
   b. Access to identity services
   c. Submission of report generation requests and display of report results

III. Request for Information

OBIM is seeking information that identifies products, methodologies, and solutions available to address the subject areas listed in items A through H below.

A. End user access via web portal and mobile devices
B. Replacement Biometric Examiner tools
C. Automated testing
D. Biometric matching
E. DevOps accelerated development and automated delivery
F. Big data, reporting, and analytics
G. Cloud security
H. Adaptive, Perfective, Corrective, Preventative Maintenance

Respondents do not need to address each subject area (A through H) and may provide information pertinent to any or all of the listed subject areas. Information provided will guide OBIM in planning future development and expansion of biometric capabilities.

Responses to this section, Section III Request for Information, are limited to ten (10) pages.
A. End User Access via Web Portal and Mobile Devices

OBIM systems are essentially back-office processing systems accessed through system to system interfaces. OBIM plans to provide end-user access to processing features through a web portal and through mobile devices.

Question: What solutions are being applied by industry for improving end-user access to biometric processing capabilities via web portal and mobile devices?

B. Replacement Biometric Examiner Tools

OBIM plans to upgrade the software tools used by its biometric examiners to resolve identity matches that the cloud-based biometric matching capability could not resolve using fingerprints, facial images, and iris scans.

Question: What solutions are being applied by industry as an upgraded tool set capable of matching fingerprints, facial images, and iris scans?

Question: What solutions are being applied by industry to accommodate matching for future modalities such as DNA; voice; palm print; scars, marks, and tattoos (SMT); contactless fingerprint; or other emerging modalities?

C. Automated Testing

OBIM capabilities are migrating to the AWS GovCloud. Future development, maintenance, and application enhancement will also take place in the AWS cloud environment.

Question: What solutions are being applied by industry for implementing automated testing in the AWS environment to accommodate testing in all lifecycle phases?

D. Biometric Matching

OBIM biometric matching capability for fingerprint, iris, and facial image matching occurs in the cloud. OBIM plans to compare alternative matching technologies to those initially included in IDENT and HART implementations to compare performance and matching accuracy. OBIM also plans to pilot test matching technologies for those additional biometric modalities that DHS may choose to utilize.

Question: What matching capabilities for fingerprint, iris, and facial image are being applied by industry that can be implemented in the AWS GovCloud environment?

Question: What matching capabilities are being applied by industry for DNA; voice; palm print; scars, marks, and tattoos (SMT); contactless fingerprint; or any other emerging modality that are or will be available in the AWS GovCloud environment?

E. DevOps Accelerated Development and Automated Delivery

Moving beyond automated testing as addressed in Item C above, OBIM plans to automate the flow from development, to testing, to implementation in production.

Question: What solutions are being applied by industry that would accomplish this objective in an AWS GovCloud environment?
F. Big Data, Reporting, and Analytics

OBIM systems will generate large quantities of data that will be stored in the AWS GovCloud in PostgreSQL and Amazon S3 data bases.

**Question:** What solutions are being applied by industry that would address the problem of analyzing large quantities of data in the OBIM data stores located in the AWS GovCloud?

G. Cloud Security

OBIM is implementing or migrating capabilities in a secure AWS GovCloud environment. That said, the nature of cybersecurity threats is constantly evolving.

**Question:** What solutions are being applied by industry that would address securing/monitoring OBIM systems while developing and operating the systems in AWS GovCloud?

H. System Maintenance

OBIM requires system maintenance to address perfective, adaptive, corrective, preventative, and security related changes to all OBIM operational systems. These encompass application support to maintain the mission critical systems (to include OBIM’s Biometric Support Center (BSC) and end user tools). These changes are continuous development functions and should not be bundled with new capability releases. Existing Service Requests, also known as Onboarding Requests, facilitate the use of existing OBIM 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. 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.

**Question:** What solutions are being applied by industry that would address continuous delivery of system maintenance across all OBIM operational systems?

**SUBMISSION INSTRUCTIONS**

Submissions should include a cover letter no longer than 2 pages in length with the following information:

1. Vendor official name, address and phone number.
2. Point of Contact information, including name, phone number and email address.
3. The vendor’s country of origin.
4. For any products submitted, please include the product’s country of origin.
5. If applicable, one URL for the vendor’s official web site.
6. If applicable, your company’s GSA Schedule contract number.
7. If applicable, any relevant DHS strategic sourcing vehicle under which your company currently holds a contract and the associated contract number.

8. If applicable, any relevant Governmentwide Acquisition Contract (GWAC) under which your company currently holds a contract and the associated contract number.

Please Note: the Government reserves the right to hold one-on-one meetings as a result of responses received from this RFI as part of its market research. Meetings may be held in particular with vendors who provide comprehensive responses to the questions posed.

**Responses are due no later than 5:00pm Eastern Time on July 17th, 2019.**

Please provide responses to Michael Horvath at michael.horvath@hq.dhs.gov as well as Tracy Miller at tracy.miller@hq.dhs.gov. The subject line of the email should contain the RFI number (70RNPP19RFI000008).

(End of Request for Information)