U.S. Department of Homeland Security

Solicitation Number HSHQDC-16-R-00080

Homeland Advanced Recognition Technology (HART)
Office of Biometric Identity Management
National Protection and Programs Directorate

Office of Procurement Operations
Washington, District of Columbia
February 13, 2017

EXECUTIVE SUMMARY

This Request for Proposal (RFP) is for the Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) Office of Identity Management's (OBIM) new, more robust biometrics system, titled the Homeland Advanced Recognition Technology (HART). HART will replace the existing Automated Biometric Identification System (IDENT).

TABLE OF CONTENTS

REQUEST FOR QUOTATION

(THIS IS NOT AN ORDER)

THIS RFQ ☐ IS ☒ IS NOT A SMALL BUSINESS SET ASIDE

PAGE 1 OF PAGES 158

1. REQUEST NO.	2. DATE ISSUED	3. REQUISITION/PURCHASE REQUEST NO.	4. CERT. FOR NAT. DEF. UNDER BDSA REG. 2 AND/OR DMS REG.1	RATING
HSHQDC-16-R-00080	02/13/2017	RNIM-16-00063		

5a. ISSUED BY

Contracting Office
MGMT/OPO NPPAD
Mailstop 0115
Department of Homeland Security
245 Murray Lane SW
Washington DC 20528-0115

6. DELIVERY BY *(Date)*: Multiple

7. DELIVERY: ☒ FOB DESTINATION ☐ OTHER *(See Schedule)*

9. DESTINATION

a. NAME OF CONSIGNEE: VARIOUS LOCATIONS

b. STREET ADDRESS

5b. FOR INFORMATION CALL: *(No collect calls)*

NAME	TELEPHONE NUMBER	
	AREA CODE	NUMBER
Shannon Ozoria	202	447-0230

8. TO:

a. NAME | b. COMPANY

c. STREET ADDRESS | c. CITY

d. CITY | e. STATE | f. ZIP CODE | d. STATE | e. ZIP CODE

10. PLEASE FURNISH QUOTATIONS TO THE ISSUING OFFICE IN BLOCK 5a ON OR BEFORE CLOSE OF BUSINESS *(Date)*: See RFP Part 5.1.2

IMPORTANT: This is a request for information, and quotations furnished are not offers. If you are unable to quote, please so indicate on this form and return it to the address in Block 5a. This request does not commit the Government to pay any costs incurred in the preparation of the submission of this quotation or to contract for supplies or services. Supplies are of domestic origin unless otherwise indicated by quoter. Any representations and/or certifications attached to this Request for Quotations must be completed by the quoter.

11. SCHEDULE *(Include applicable Federal, State and local taxes)*

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)
	The Department of Homeland Security (DHS) Office of Procurement Operations (OPO) National Protection and Programs Acquisition Division (NPPAD) is considering awarding a Hybrid (Firm Fixed Price, Fixed Price Award-Fee, Cost Plus Award-Fee, Time and Materials and Cost Reimbursable) task order under the department-wide EAGLE II, FC1 (Unrestricted) Indefinite-Delivery Indefinite-Quantity (IDIQ) contract. The purpose of this task order is to procure a new, more robust biometrics system, referred to as the Homeland Advanced Recognition Technology (HART), to support the National Protection and Programs Directorate(NPPD) Office of Biometrics Identity Management (OBIM). Continued ...				

12. DISCOUNT FOR PROMPT PAYMENT	a. 10 CALENDAR DAYS (%)	b. 20 CALENDAR DAYS (%)	c. 30 CALENDAR DAYS (%)	d. CALENDAR DAYS NUMBER	d. CALENDAR DAYS PERCENTAGE

NOTE: Additional provisions and representations ☐ are ☐ are not attached

13. NAME AND ADDRESS OF QUOTER	14. SIGNATURE OF PERSON AUTHORIZED TO SIGN QUOTATION	15. DATE OF QUOTATION
a. NAME OF QUOTER		
b. STREET ADDRESS	16. SIGNER	
	a. NAME *(Type or print)*	b. TELEPHONE AREA CODE
c. COUNTY		
d. CITY / e. STATE / f. ZIP CODE	c. TITLE *(Type or print)*	NUMBER

AUTHORIZED FOR LOCAL REPRODUCTION
Previous edition not usable

STANDARD FORM 18 (REV. 6-95)
Prescribed by GSA - FAR (48 CFR) 53.215-1(a)

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	DO/DPAS Rating: NONE Period of Performance: 42 months from effective date of award				
0001	Phase I/Increment 1 Core Biometric Management System (FPAF) BPO Sections 2 & 5 PoP: Completion 18 months after effective date of task order Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT	1	LO		
0001 A	Phase I/Increment 1 Award-Fee (Offeror may propose) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT				
0001 B	Phase I/Increment 1 Hardware and Software (CPFF) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT				
0001 C.1	Phase I/Increment 1 DHS Hosting and Support Services - DHS Data Center (FFP) Levels 2 and 3 Support (Quote N/A if not applicable) (per month charge x estimated number of months) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT		MO		
0001 C.2	Phase I/Increment 1 Non-DHS Hosting and Support Services (FFP) Levels 1, 2 and 3 Support (Quote N/A if not applicable) (per month charge x estimated number of months) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT		MO		
0002	Phase IIA/Increment 2 Production-Scaled Multimodal Modality Matching and Fusion (FFP) BPO Sections 4 & 5 Continued ...	1	LO		

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	PoP: Completion 18 months after Notice to Proceed Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT				
0002 B	Phase IIA/Increment 2 Hardware and Software (CPFF) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT				
0002 C.1	Phase IIA/Increment 2 DHS Hosting and Support Services - DHS Data Center (FFP) Levels 2 and 3 Support (Quote N/A if not applicable) (per month charge x estimated number of months) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT		MO		
0002 C.2	Phase IIA/Increment 2 Non-DHS Hosting and Support Services (FFP) Levels 1, 2 and 3 Support (Quote N/A if not applicable) (per month charge x estimated number of months) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT		MO		
0003	Phase IIB/Increment 2 Data Warehouse (FFP) (Optional CLIN) BPO Section 6.1 PoP: Completion 18 months after Notice to Proceed Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT	1	LO		
0003 B	Phase IIB/Increment 2 Hardware and Software - Data Warehouse (CPFF) (Optional CLIN) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT				
0003 C.1	Phase IIB/Increment 2 Data Warehouse DHS Hosting and Support Services - DHS Data Center (FFP) Continued ...		MO		

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Levels 2 and 3 Support (Optional CLIN) (Quote N/A if not applicable) (per month charge x estimated number of months) (Option Line Item) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT				
0003 C.2	Phase IIB/Increment 2 Data Warehouse Non-DHS Hosting and Support Services (FFP) Levels 1, 2 and 3 Support (Optional CLIN) (Quote N/A if not applicable) (per month charge x estimated number of months) (Option Line Item) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT		MO		
0004	Travel (CR) Related to Phases I & II Not-to-Exceed $305,000 PoP: Duration of Phases I & II Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT				
0005	Transition Out (FFP) (Optional CLIN) BPO Section 6.6 PoP: After Receipt of Notice to Proceed Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT	1	LO		
0006	Legacy Interface Development (T&M) (Optional CLIN) Not-to-Exceed 3,304 Hours BPO Section 6.5 PoP: After Receipt of Notice to Proceed Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT				
0007	IXM Specification Version Translation (FFP) (Optional CLIN) BPO Section 6.4 PoP: After Receipt of Notice to Proceed Continued ...	1	LO		

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT				
0008	Post IOC Customer Migration (FPAF) BPO Section 3 PoP: Completion 6 months after IOC Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT	1	LO		
0008 A	Post IOC Customer Migration Award-Fee (Offeror may propose) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT				
1001 A.1	OPTION 1 - Post Deployment Support (Period 1): DHS Hosting and Support Services in DHS Data Center (FFP) Optional CLIN BPO Section 6.2 Includes all labor, service and hosting charges (materials included). PoP: 12 months (following completion of Increment 1) (Option Line Item) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT	12	MO		
1001 A.2	OPTION 1 - Post Deployment Support (Period 1): Non-DHS Hosting Services (FFP) Optional CLIN BPO Section 6.2 Includes all costs non-DHS hosting services only. PoP: 12 months (following completion of Increment 1) (Option Line Item) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT	12	MO		
1002	OPTION 1 - Travel (CR) Post Deployment Period 1 Not-to-Exceed $150,000 PoP: 12 months (following completion of Increment Continued ...				

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	1) (Option Line Item) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT				
2001 A.1	OPTION 2- Post Deployment Support (Period 2): DHS Hosting and Support Services in DHS Data Center (FFP) BPO Section 6.3 Includes all associated labor, service charges and materials. PoP: 12 months (following Post Deployment Period 1) (Option Line Item) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT	12	MO		
2001 A.2	OPTION 2- Post Deployment Support (Period 2): Non-DHS Hosting and Support Services for Data Warehouse (FFP) BPO Section 6.3 All costs non-DHS hosting services only. PoP: 12 months (following Post Deployment Period 1) (Option Line Item) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT	12	MO		
2001 B.1	OPTION 2- Post Deployment Support (Period 2): DHS Hosting and Support Services in DHS Data Center for Data Warehouse (FFP) Optional CLIN BPO Section 6.3 All labor, service charges and materials costs for Data Warehouse only. PoP: 12 months (following Post Deployment Period 1) (Option Line Item) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT	12	MO		
2001 B.2	OPTION 2- Post Deployment Support (Period 2): Non-DHS Hosting and Support Services for Data Continued ...	12	MO		

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Warehouse (FFP) Optional CLIN BPO Section 6.3 All labor, service charges, and materials for Data Warehouse non-DHS hosting services only. PoP: 12 months (following Post Deployment Period 1) (Option Line Item) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT				
2002	OPTION 2 - Travel (CR) Post Deployment Period 2 Not-to-Exceed $150,000 PoP: 12 months (following Post Deployment Period 1) (Option Line Item) Product/Service Code: D302 Product/Service Description: IT AND TELECOM-SYSTEMS DEVELOPMENT				

PART 2. BASELINE PERFORMANCE OBJECTIVES

This page left blank intentionally.

BPO Table of Contents

List of Tables

This page intentionally left blank

1 Introduction

1.1 Purpose

The Department of Homeland Security (DHS) Office of Biometric Identity Management (OBIM) seeks to replace its existing identity management system, the Automated Biometric Identification System (IDENT) with an enhanced, scalable, modular, and multimodal identity management system to be known as the Homeland Advanced Recognition Technology (HART) system.

1.2 Background

The *Consolidated and Further Continuing Appropriations Act, 2013* designated OBIM, a subcomponent of the National Protection and Programs Directorate (NPPD), as the lead entity within DHS for biometric identity management services. OBIM assumed this cross-cutting responsibility from the former United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program. This responsibility to match, store, share, and analyze biometric identity information includes the operation, maintenance, and modernization of IDENT as well as providing identity services expertise.

Congressional mandates established US-VISIT in 2003 as the DHS provider for biometric and associated biographic identity screening and analysis services. US-VISIT's mission was to receive, maintain, and share information on foreign nationals to enhance national security, facilitate legitimate travel and trade, and ensure the integrity of the Nation's immigration system, while deploying the program in accordance with existing privacy laws and policies. US-VISIT accomplished this mission by deploying identity management capabilities through IDENT, based on the system of the same name developed in 1994 and used by the Immigration and Naturalization Service (INS). The program's biometric and associated biographic identity services directly supported its customers including DHS Components; the Departments of State (DOS), Justice (DOJ), and Defense (DoD); State, local, tribal, and territorial law enforcement; the Intelligence Community; and foreign country partners.

An Analysis of Alternatives (AoA), *United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program Technical Engineering and Architecture Recommendations for US-VISIT 1.0 Analysis of Alternatives*, dated July 31, 2012, determined that the aging IDENT system is at risk of failure and requires replacement. This determination was revalidated on November 30, 2014.

1.3 Mission and Needs

OBIM's mission is to provide enduring identity services to DHS and its mission partners that enable informed decision making by producing accurate, timely, and high assurance biometric identity information and analysis in compliance with the 2013 Appropriations Act. The ability of DHS and its partner agencies to fulfill their missions requires access to actionable, timely, and accurate information that distinctly identifies individuals. Decision makers must be able to verify presented identities, identify persons who may be inadmissible to the United States, and identify persons ineligible for certain status or privileges granted by the Government. Biometrically established and verified identity information provides a higher level of assurance of an

individual's identity than the mere possession of identity affirming documents. Persons of specific concern are those who may be immigration violators, domestic and international fugitives, military detainees, known or suspected terrorists (KSTs) or national security threats (NSTs)

Decision makers require actionable, timely, and accurate information supported by high-trust identity capabilities to:

- Determine visa issuance and admissibility into the United States;
- Establish eligibility for immigration benefits;
- Issue credentials (i.e., determine whether an individual should be granted access to a sensitive facility or sensitive system);
- Take law enforcement actions with potential homeland security implications;
- Verify the identity of persons associated with matters of national security; and
- Conduct intelligence and trend analyses employing identity determinations and verifications provided by OBIM.

OBIM's customers typically carry out their missions by capturing biometric data and submitting the biometric data to OBIM. OBIM's mission functions are to match, store, share, and analyze the results.

Stakeholder operational mission needs require DHS biometric identity service capabilities that provide biometric matching, storing, sharing and analyzing capabilities, and other services using multiple and expanding sets of biometrics beyond just fingerprints to increase identity assurance. System capabilities must include the ability to:

- Extend biometric identification services to accommodate a rapidly growing customer base;
- Receive and exchange information through standards-based interfaces that maximize the use of sharable data and support increased interoperability;
- Provide timely and accurate biometric matching results to customers based on varying operational requirements;
- Match multiple types of biometrics and leverage or fuse identity determinations based on multiple biometric modalities for increased accuracy;
- Provide forensic (latent) fingerprint and other biometric matching services involving partial biometrics captured during investigations;
- Efficiently store and retrieve biometric identification records including associated biographic information and photographic images;
- Meet customer-specific requirements for data storage, retention, and deletion;
- Handle continued growth in storage and processing demands;
- Enable the search, management, and analysis of biometric and associated biographic data;

- Provide reporting and data analysis capabilities on biometric identity records;
- Provide timely identity determinations during stakeholder encounters with applicants for entry to the US or for other government benefits thereby enabling fraud detection;
- Protect, access, and filter available data based on information security, privacy and civil rights and civil liberties requirements, and data ownership guidelines; and
- Share biometric and associated biographic identity information to an expanding customer and partner base, including:
    - Providing fingerprint and other biometric identification sharing services to other Federal agency biometric systems or non-Federal customers as appropriate; and
    - Supporting international information sharing agreements.

Independent analyses of IDENT have identified performance limitations. Some of those limitations have been addressed for the near term; others can only be addressed through adoption of a new foundational system architecture that provides solutions to resolve current and projected shortfalls. Critical architectural limitations and risks include:

- Diminishing returns from adding additional hardware to increase capacity in the face of exponential growth in transaction volumes and biometric image gallery sizes necessary to provide continuing support to current customers;
- Inability to guarantee near 7x24x365 system availability to avoid service disruptions to OBIM's customers' operations supporting their respective missions;
- Increasing costs of maintaining and sustaining system operations due to increasing biometric image gallery growth and increasing demand;
- Inability to implement new customer requirements and administrative changes to existing processing without complex systems development;
- Inability to respond to new customer requirements in a timely fashion;
- Inability to integrate system security with DHS enterprise security;
- Inability to store and match additional biometric modalities being captured by OBIM's customers;
- Inability to complete a search of the entire gallery of stored fingerprints to determine whether a submitted fingerprint matches a known identity within 10 seconds; and
- Inability to easily resolve identities among the multiple disparate identity systems currently in use – specifically the Federal Bureau of Investigation (FBI) Next Generation Identification (NGI) system and the DoD Automated Biometric Identification System (ABIS).

OBIM's inability to achieve near 7x24x365 availability is due to the necessity of taking the system offline in order to implement application patches, updates, and new IDENT releases.

HART shall be developed with a service oriented architecture and standards-based interfaces. The redesign and development of the system will address the baseline and the current gaps including capacity, increased security and privacy protections, interoperability, unsustainable

costs, and performance and availability. Support of the system for additional biometric identity modalities beyond fingerprints will address the gaps of accuracy and surety of matching results and interoperability.

1.4 Homeland Advanced Recognition Technology Program

HART will be developed in four increments.

1.4.1 Increment 1 – HART Foundation

Increment 1 forms the architectural foundation for HART. This Increment replaces IDENT and its monolithic, custom-coded IDENT transaction processing application with the HART core application - a modular application that results from the integration of proven, off-the-shelf software applications, open source products, or frameworks. The HART core application shall provide business workflow and business rules management; interface to biometric matching services; feature an authentication and authorization web service; and fully integrate with DHS enterprise system security.

HART shall have a modular biometric matching subsystem interface architecture that enables the application to communicate with multiple biometric matching subsystems concurrently and that isolates the transaction and business processing components of the HART core application from the internal details of individual biometric matching subsystems.

HART Increment 1 will include fingerprint matching capabilities and analysis that encompass OBIM's current 10-print and 2-print matching subsystems either by replacing or incorporating those subsystems. HART will also provide latent fingerprint management and analysis capabilities. HART shall have the capability to incorporate matching subsystems for additional fingerprint matching technologies and matching technologies for additional biometric modalities, specifically large scale iris and facial modalities. All biometric matching subsystems will connect to HART through a standard biometric matching subsystem interface without the need to modify the main business and transaction processing system. In Increment 1, the existing Multimodal Bridge Solution (MMBS) capability face and iris matching subsystem implemented with NEC technology will continue to operate. Implementation of production scaled face and iris matching will occur in Increment 2. In Increment 1, the HART Contractor will be expected to treat MMBS as a distinct application that must interface to HART. The HART Contractor will be expected to modify the MMBS interface as necessary to connect to HART through the HART standard biometric matching subsystem interface. This interface will communicate iris and face matching requests to the MMBS and return matching results from MMBS to HART. Fingerprint matching subsystems implemented during Increment 1 will also connect to the HART application through this biometric matching subsystem interface. All future matching subsystems will use this same interface.

Increment 1 shall implement a new data architecture and includes the transition of existing data to that new architecture. The new data architecture includes logical and physical data models, data management capabilities, and physical storage for both identity data and biometric image data where each identity may have multiple associated biometric images of the same or different modalities. All data models (such as conceptual, logical and physical), if relational, shall be developed by adhering to the standards and the data modeling development life cycle defined in OBIM Data Modeling Methodology Standards document. The data architecture and data storage

architecture shall be designed for scalability to address the projected growth in identity and image data volumes, log and monitoring data volumes, data warehousing volumes, and to accommodate long term data retention requirements for storage growth projections.

The physical infrastructure for HART shall be designed and the necessary capabilities and capacities shall be acquired, tested, and deployed in an operational-ready status during Increment 1 and shall support initial production processing. This deployment shall achieve the system's formal Initial Operating Capability (IOC) milestone. The production environment shall be designed to meet OBIM's objectives for system availability and for scalability to provide for increased capacity to meet future processing demand.

Increment 1 includes the implementation of a new system development and testing environment for performing maintenance on HART applications and enhancing and extending the capability of those applications. This environment shall be accompanied by a new testing protocol suitable for future HART maintenance and enhancements efforts and a Performance Test Environment.

During Increment 1, existing IDENT biometric matching subsystems that are retained for incorporation into the HART architecture will connect to HART; internal operation of each matching subsystem will remain unchanged. The HART contractor will modify the interface with each retained matching subsystem as required to interface to HART. Matching subsystems that may be incorporated and which may be affected include the 3M Cogent 10-print, 2-print and latent print matching subsystems and the MMBS limited production face and iris matching subsystems.

The Performance Test Environment shall have storage and processing capacities capable of stressing the application. The Performance Test Environment shall contain sufficient capacity in servers, data storage, and application and utility software to mimic the architecture and performance of the production system. It shall have the capacity to store large quantities of identity data and identity transactions that can be used in volume stress testing of the application during initial development and during later maintenance and enhancement efforts. The test data used in conjunction with simulation capabilities will enable OBIM to simulate transaction and data access workloads similar to those that will be encountered in actual production processing. Test data in the Performance Test Environment shall include data to be used in measuring the accuracy of installed HART biometric matching technologies and the accuracy of matching technologies that may be candidates for addition to HART.

1.4.2 Increment 2 – Multimodal Biometric Identity Management and Data Warehouse

Increment 2 builds on the business processing workflows implemented in the HART core application in Increment 1. Increment 2 shall implement multimodal matching through the addition of full production scale iris and facial image matching and by adding business processing that leverages the results from multiple biometric matching operations to increase overall system matching accuracy. The production level iris and face matching capabilities added in Increment 2 shall supersede the current limited MMBS iris and facial matching capabilities. Increment 2 shall also provide OBIM's forensic examiners with the integrated capability to adjudicate matching results and provide identity management services for iris and facial modalities. Increment 2 shall introduce the capability to improve biometric matching accuracy by fusion of the matching results from multiple biometric modality matches.

Increment 2 shall expand the Performance Test Environment created during Increment 1 to include the infrastructure and applications necessary to subject the capabilities introduced during Increment 2 to testing under production-like workloads. Increment 2 shall add test data to the Performance Test Environment to enable testing multimodal identity matching performance and multimodal matching accuracy.

The optional Increment 2 HART Data Warehouse task shall implement data warehousing and data mart capabilities to establish the foundation for improved reporting and analytical processing. Data stores associated with data warehouse and data mart subsystems shall be established and continuously updated with operational data and shall be available for analytical processing and operational reporting without affecting production system performance.

1.4.3 Future Requirements

HART Increments 3 and 4 are not in scope for this solicitation. Those increments will be addressed in future solicitations and are included here to describe the future intent for the overall program.

1.4.3.1 Increment 3 – Web Portal and Applications

Increment 3 is not in scope for this solicitation. Increment 3 will establish a web portal that provides web access to the various HART services implemented in earlier Increments. These will include but are not limited to: identification, pre-verification, verification, information retrieval, information update, information addition, redress, and notification. Increment 3 will also implement an identity directory that links identities present in OBIM data storage and in multiple external identity data stores to provide the capability to achieve an overall person-centric view of all information associated with an identity. Increment 3 will add additional biometric modalities for storage and retrieval but without biometric matching and will implement an expanded information sharing service with external customers.

1.4.3.2 Increment 4 – Advanced Examination Tools, Reporting and Analytical Processing

Increment 4 is not in scope for this solicitation. Increment 4 will fully integrate OBIM biometric verification and identity management capabilities across biometric modalities and will introduce user-available reporting and online analytical processing (OLAP) applications for advanced data analysis along with the necessary data stores and processing infrastructure to support both the analytical processing and the enhanced reporting and analysis that OLAP enables. System full operating capability (FOC) will be achieved with the completion of Increment 4.

1.5 Scope

The Contractor shall design, engineer, develop, acquire, integrate, test, and install the software applications required to fulfill HART requirements. The Contractor shall also acquire or otherwise provision the infrastructure necessary to host HART processing. The Contactor shall also provide or otherwise ensure post-deployment operations and maintenance support for both the HART software applications and the HART infrastructure. This effort includes not only developing and integrating the new biometric system itself but also designing a scalable information technology (IT) infrastructure to host the system; designing scalable image and data

storage architecture; acquiring all hardware, hosting services, and software necessary to provision the supporting IT infrastructure both for new system testing environments and for production operating environments; and providing post-deployment operational support.

This Baseline Performance Objectives (BPO) document describes the objectives of Increments 1 and 2 of the HART program - the design, development, and implementation of the HART core application and its supporting infrastructure. The HART core application shall be based on the integration of commercial, government, and/or open-source off-the-shelf software components and/or frameworks. This effort also calls for the design and provisioning of the computing, data management, data storage, and network infrastructures necessary to support both testing and production operations for the HART system and the transition of data and processing from the current IDENT system to the replacement system.

The scope of this BPO, in addition to the work described above, includes the following optional efforts.

- Post-Deployment Support – Period 1;
- Post-Deployment Support – Period 2;
- Increment 2 – Data Warehouse Capability Implementation;
- Legacy Interface Development;
- IDENT Exchange Messages (IXM) Specification Version Translation; and
- Transition Out.

The scope of the post-deployment support includes maintenance and enhancement support for the HART application and O&M support for the HART infrastructure in place at the end of Increment 1 and shall include any additional software applications or infrastructure added to the HART processing environment during Increment 1 and during Increment 2 as a result of Increment 2 development. These options also include the provision of Level 2 and Level 3 system support (see description in Appendix C, Definitions) for all HART infrastructure, data, and applications.

1.6 IDENT and Reuse Guideline

The proposed HART architecture may retain, re-use, repurpose, or dispose of any IDENT components. Reuse of existing IDENT components is available but not required. However, OBIM requires the redesign and replacement, not the reuse, of the existing Transaction Manager application. Any proposed component reuse shall not affect the availability of the IDENT system, the integrity of IDENT data, or degrade IDENT system performance in any way. The HART Contractor shall take no action during the development and deployment of HART that affects IDENT performance or availability until such time as all customer service request processing has been successfully transitioned from IDENT to HART.

1.7 Period of Performance

The base period of performance for the contract will be 18 months for Increment 1, the implementation and production deployment of the HART Core Application and Infrastructure and the migration of processing to HART from IDENT for at least one OBIM customer,

achieving HART IOC during that period of performance. The period of performance for completing customer migration to HART for those customers whose migration was not completed during Increment 1 will be 6 months. The period of performance for Increment 2, Multimodal Biometric Identity Matching Implementation, will also be 18 months. The period of performance for the optional Increment 2, Data Warehouse Capability Implementation, will be 18 months. The optional Post-Deployment Support – Period 1, for Post-Deployment Support, will have a period of performance of 12 months beginning at the end of Increment 1; the optional Post-Deployment Support – Period 2, will extend the support initiated in Period 1 for an additional 12 months. The optional Legacy Interface Development and IXM Specification Version Translation efforts will, if awarded, be concurrent with Increment 1 but will have a shorter period of performance. The optional Transition out task will be exercised so as to terminate concurrently with the completion of the periods of performance of the last activities performed as a result of other awarded tasks under this solicitation; period of performance to be specified in the notice to proceed.

Table 1. Periods of Performance

Task	Period of Performance (in months)	Start Work Condition
Increment 1		
HART Core Application and Infrastructure	18	Contract effective start date
Customer Migration	6	Completion of Increment 1
Increment 2		
Multimodal Biometric Identity Matching	18	Notice to Proceed
Option – Data Warehouse	18	Option Award
Optional Tasks (Concurrent with Increment 1)		
Legacy Interface Development	< 18	Option Award
IXM Specification Version Translation	< 18	Option Award
Post-deployment Support		
Support Period 1	12	Option Award (At end of Increment 1)
Support Period 2	12	Option Award (At end of Post Deployment Support Period 1)
End of Contract Transition Out	Specified in Notice to Proceed	Notice to Proceed

1.8 Place of Performance

The primary place of performance shall be the Contractor's facilities where system design development and integration activities will occur, with periodic travel to DHS, NPPD, and OBIM facilities within the National Capital Region (NCR). Periodic travel to the DHS Enterprise Data Centers in Stennis, Mississippi and Clarksville, Virginia or to other hosting locations engaged by the Contractor may be necessary; on-site Contractor support will be required at all locations. In addition, Contractor provided training will require travel to San Diego CA and OBIM facilities within NCR. Contractor access to any testing and production environments located in the DHS Enterprise Data Centers will be granted through remote access technology managed by the DHS Enterprise Data Centers.

1.9 Document Organization

Section 1 of this Baseline Performance Objectives document contains general HART program background information.

The objectives to be accomplished under this solicitation are described in the following sections:

Section 2 contains the objectives to be accomplished during HART Increment 1;

Section 3 contains the objectives to be accomplished during HART Post-IOC Customer Migration;

Section 4 describes Increment 2 Multimodal matching objectives;

Section 5 describes general HART objectives;

Section 6 describes the objectives of each of the HART optional tasks.

Section 7 lists the types of deliverables that OBIM expects to receive in fulfillment of HART objectives.

Section 8 lists guidelines and mandatory constraints and restrictions.

Section 9 contains lists of applicable documents.

Appendix A lists the performance requirements specified in the *HART Operational Requirements Document (ORD) that HART* that the HART system shall satisfy.

Appendix B provides general system sizing targets.

Appendix C provides definitions of terms used in the Baseline Performance Objectives document.

2 Performance Objectives – HART Increment 1 – HART Core Application and Infrastructure

Increment 1 of HART shall establish the foundational system architecture for subsequent development and expansion. Increment 1 shall establish the HART identity database, biometric image storage, a fingerprint matching subsystem, and a latent fingerprint matching subsystem. Increment 1 includes the design, development, and integration of the HART core application software suite, the implementation of testing environments for developmental and performance testing, system functional and performance testing, the conversion of existing IDENT data stores into the HART data management architecture, and the partial migration of processing under IDENT to production processing under HART.

The HART Contractor shall perform system design, development, engineering, and integration activities in its own facilities. The Contractor shall transfer the source code repository containing the developed and integrated HART system to OBIM for placement under OBIM configuration control, and loading into an OBIM source code repository and testing environments for integration testing with OBIM's customers, security authorization, and formal operational and acceptance testing. The HART Contractor shall provide operations and maintenance (O&M) support both before and after system implementation.

The existing IDENT system includes the following major components. Each includes capability to be addressed by HART – either through replacement or through component reuse and incorporation in HART. The HART Contractor shall have the discretion to incorporate and reuse the following components in whole or in part in the HART system.

- Active and stand-by computing environments. IDENT currently has duplicate computing environments, one in each of the DHS Enterprise Data Centers. IDENT does not operate in an active/active configuration. A primary site handles all processing; the secondary site is in standby mode for activation in response to loss of the primary. Application updates and new software releases require that OBIM take IDENT offline to accomplish the updates thus degrading system availability.
- Duplicate data storage and update. IDENT currently employs a duplicate data storage architecture. Identity and image data stores are duplicated in the two DHS Enterprise Data Centers; updates to identity and image data are applied to both data stores to keep them in synchronization.
- Enterprise Service Bus (ESB). IDENT currently employs a TIBCO enterprise service bus as its primary interface for communicating with external customers transmitting identity-related transactions to IDENT for processing. TIBCO ActiveMatrix Business Works is the application used to develop services, automate business processes, and integrate applications.
- Duplicate fingerprint matching subsystems. IDENT currently has duplicate fingerprint matching subsystems in each DHS Enterprise Data Center for 10-print, 2-print, and latent fingerprints. These subsystems operate concurrently in an active-active configuration. Matching requests are load balanced between the subsystems at the data centers. Updates made to the fingerprint galleries in each data center are replicated in the corresponding matching gallery in the other data center. All matching subsystems use 3M-Cogent

matchers. Latent fingerprint processing is provided by the Cogent Automated Biometric Information System (CABIS).

- Processing locations. All IDENT infrastructure is currently installed in the two DHS Enterprise Data Centers located in Stennis, MS and Clarksville, VA.
- Cloud based data reporting. OBIM is in the initial stages of implementing a data reporting system designated as the Operational Data Store / Operational Data Reporting (ODS/ODR) system. The ODR (reporting) portion will implemented on the Amazon Web Services (AWS) GovCloud. The ODR will employ the Amazon Redshift database and the Birst business intelligence tool for reporting and analysis. The ODS (data store) component is a data storage staging area hosted in a DHS Enterprise Data Center. The ODS consists of selected data tables copied from IDENT using Informatica. An extract from ODS is planned for upload to the GovCloud ODR. ODS/ODR is currently in development; the extract, translate, and load (ETL) from ODS to ODR has not yet occurred and specifications are not yet available.

The performance objectives for HART Increment 1 follow.

2.1 System Architecture Objectives

OBIM requires that the HART Contractor deliver a high availability system architecture that shall achieve the availability requirements specified in HART ORD. Depending upon the Contractor's system architecture and deployment plan, the resulting HART testing and production systems may consist of components that are:

- Provided by cloud-based infrastructure services;
- Installed and operated in one or more non-DHS data centers, Government-owned or commercial;
- Installed and operated in one or both of the DHS Enterprise Data Centers; or
- Installed and operated as any hybrid of the above options.

The HART system shall have the following architectural characteristics.

a. HART shall have a high availability architecture that avoids single points of failure. The HART architecture may leverage any combination of cloud-based infrastructure services, infrastructure installed in DHS Enterprise Data Centers, or infrastructure installed in other Government or commercial data centers in order to provide the redundant capabilities necessary to meet the *Availability* and *Mean Time to Repair* targets specified in Appendix A.

b. HART shall have a Service Oriented Architecture that makes the system functionality available as discrete services, callable and capable of being orchestrated where needed in system processing workflows.

c. HART shall have a modular design that incorporates an open systems design and utilizes open standards to the maximum extent possible. Commercial off-the-shelf (COTS), Government off-the-shelf (GOTS), and open-source products are desired with minimal

customization. New systems development is discouraged unless specific processing capabilities or workflows are not addressed within existing COTS, GOTS, or open-source solutions or if performance targets are not otherwise achievable. If significant customization would be required to COTS or GOTS solutions, purpose-built functionality on open source frameworks can be considered.

d. The HART design shall provide for the expansion of interoperable services similar to those provided to FBI and DoD systems to include additional Federal agency biometric systems and non-Federal customers without requiring modifications to the foundational system architecture.

e. The system design shall make provision for defining new transaction processing workflow functionality and modifying existing workflow functionality without requiring modifications to the underlying system design or requiring systems development activity.

f. The system architecture shall be designed to be scalable and shall be able to accommodate increasing workloads resulting from increased numbers of transactions due to the addition of new services and the addition of new customers.

g. The system architecture shall be designed to support rapidly expanding identity and biometric image data volumes as well as expanding volumes of monitoring and audit trail data without the need to modify the underlying system architecture or workflows.

h. The system infrastructure shall be capable of processing the business volume growth forecast over the three (3) years following the end of Increment 1 without the need for a capacity upgrade.

i. The HART system design shall maximize the ease and efficiency of O&M. The design shall, to the extent practicable, standardize hardware platforms, peripherals, operating systems, and data management systems to simplify O&M, minimize technical complexity in the architecture, and limit the types of technical expertise necessary for the ongoing maintenance of the HART operating environment.

j. The HART system shall be designed such that system and application software patches, upgrades, and releases can be applied and implemented in the production processing environment without affecting system availability and without taking the system offline.

k. The HART system design shall also maximize hardware and software monitoring to facilitate failure and degradation detection, notification, and fault isolation.

l. The HART system shall collect and store data on service requests received, responses generated, referrals to external systems, matching requests sent to biometric matching subsystems, and responses from biometric subsystems and external systems. HART shall also generate periodic traffic analyses by customer and request type, response type, and external referral type.

m. The HART architecture shall include a biometric matching subsystem interface through which the HART core application will communicate with all HART biometric matching subsystems. This interface shall provide the standard application programming interface for connecting any vendor’s matching subsystem to the HART core application and shall isolate the HART core application from the internals of each separate HART biometric matching subsystem or technology.

2.2 Data Management

IDENT currently maintains duplicate data stores for identity-related data and for biometric images. Updates made to the identity and image data stores attached to the active IDENT system instance in one DHS data center are replicated to their respective duplicate data stores in the other data center to ensure availability of up-to-date identity and image data in the event of a system failure. The HART data architecture shall ensure that the integrity and currency of HART identity and image data are maintained at all times.

a. HART shall ensure the availability of current, up-to-date identity and image data. The Contractor shall implement a data architecture leveraging those combinations of cloud-based and data center-based storage necessary to achieve both data integrity and continuous data availability in accord with the targets in Appendix A.

b. The HART data architecture shall be capable of recovering identity and image data stores following system failures within the parameters established in Appendix A.

c. HART shall store and manage identity data, biographic data, encounter data, biometric images, monitoring data, system logs, audit logs, and administrative data.

d. HART shall enable the entry, update, and maintenance of identity and biometric information in the HART data stores and provide the capability to correct erroneous information. HART shall also enable the resolution of incorrect associations of biometrics with identities.

e. HART shall ensure overall integrity of all identity data as well as that of biometric image data stores (e.g. fingerprint images, latent fingerprint images, iris images, and facial images). Integrity maintenance includes ensuring the ability to recover or restore HART data stores in the event of storage device failure, system failures, or natural disaster.

f. HART shall maintain a record of biometric images enrolled into the latent fingerprint subsystem.

g. HART shall ensure the availability of all data stores and ensure that no data loss ensues from system component failures or loss of communication with processing sites hosting HART processing.

h. HART shall have the capability to store the data supporting match results returned to customers including any biographic information matched and biometrics matched so that OBIM has a record of the information provided back to a customer such that OBIM can recreate the match (or no-match) scenario that generated the result returned to the customer.

i. Images shall be stored regardless of whether HART includes matching capability for a particular image type at the time of receipt. HART shall provide the framework for adding matching capabilities for additional image types when those capabilities are required to satisfy demand from OBIM customers.

j. HART shall have the capability to automatically manage the storage and retention of identity and biometric image data along with associated biographic data as specified by each data owning customer’s unique data retention policies. These policies are specified

in each customer's Service Level Agreement (SLA), Memorandum of Agreement, or Memorandum of Understanding.

2.3 External Biometric System Service Request Processing

HART will process service requests submitted by the FBI NGI biometric identity management system and by ABIS and respond to those requests. In addition, HART will function as an intermediary between NGI and ABIS and other HART customers.

a. HART shall support and maintain current interoperability with the FBI NGI system which includes outbound transmission of EBTS messages to NGI.

b. HART shall receive transactions from customer systems that require access to services provided by external Federal biometric matching systems such as the FBI NGI system and DoD ABIS. HART shall forward these transactions to their intended destinations. HART shall likewise receive responses from those external systems and forward those responses to the originating customer systems.

c. HART shall initiate service requests for biometric matching and identity information retrieval to external biometric systems such as NGI or ABIS and receive responses to those requests from those systems.

d. HART shall receive requests for biometric matching and identity information retrieval from customers of external biometric systems such as NGI or ABIS whose requests are transmitted to HART through the NGI or ABIS interface mechanisms. HART shall perform the necessary processing to satisfy those requests and respond to those external systems' customers through those same external systems.

2.4 Business Processing

HART shall process service requests received from its customers and generate responses to those requests requiring a response. HART shall perform biometric matching and shall store, retrieve, or update identity information as each specific request requires.

a. HART shall respond to incoming service requests by executing the business rule logic, performing biometric matching, retrieving biometric and biographic identity data, and updating identity and image data stores as necessary to respond to those service requests.

b. The Contractor shall configure the HART architecture so that it can receive, process, and respond to all message formats in the IXM specification and respond to four additional service requests not currently part of the IXM specification that will be submitted by the Secondary Inspection Tool (SIT) application. These are services unique to SIT and are not intended to be used by OBIM customers and stakeholders; these services are therefore not found in the IXM specification. The three additional services are:

    i. Merge identities;
    ii. Separate identities;
    iii. Delete photos

c. HART shall process the service requests documented in the HART Functional Requirements Document (FRD) for implementation during Increment 1.

d. HART shall implement each of the system to system interfaces with OBIM's customers' systems for both inbound and outbound messages. There are currently 40 interfaces currently implemented using the IDENT Enterprise Service Bus (ESB) consisting of TIBCO-implemented messaging protocols and twelve (12) legacy interfaces using a total of six (6) different technologies to communicate with IDENT.

e. HART shall implement a business rules processing capability and establish a centralized business rules repository containing sets of configurable business rules that can be managed using well recognized processes and maintained under configuration control.

f. Business rules shall be configurable and shall govern transaction processing, data sharing, and data access.

g. Business rule execution shall occur in business rule engine instances executing business rules maintained and controlled in the central business rules repository and distributed from that repository to rules engines embedded in processing workflows.

2.5 IXM Specification Version 6.1 Upgrade

The baseline version of the IXM specification at time of contract award will be IXM 6.0.9. IXM version 6.0.9 implements a 1:N facial identification capability along with various minor capability enhancements. The Contractor shall generate a major update to the IXM specification, version 6.1, to add new service requests planned for implementation during Increment 1 and specified in the FRD to the 6.0.9 baseline to generate the IXM 6.1 specification.

a. The Contractor shall identify the data requirements associated with each service request specified in the FRD for implementation during HART Increment 1.

b. The HART Contractor shall create the specification for IXM version 6.1 which shall be the upgrade to IXM 6.0.9 incorporating updates necessary to implement all Increment 1 service request data requirements. Note that IXM schema updates should pursue NIEM conformance where appropriate.

c. The Contractor shall implement all HART Increment 1 service requests in accord with the new IXM 6.1 specification.

2.6 Workload Management

HART shall have the capability to monitor and dynamically manage its workload processing and shall provide HART systems administrators the means to establish processing priorities for each type of incoming service request for each customer submitting that type of request.

a. HART shall have the capability to enable systems administrators to establish a processing priority for each type of service request received and have the capability to customize that priority for each customer submitting that type of request.

b. HART shall have the capability to enable systems administrators to set a schedule for changes to service request processing priorities to accommodate cyclical fluctuations in transaction volume.

c. HART shall provide the capability to automatically alter transaction priorities according to a pre-established schedule. HART shall include the capability to change workload management parameters on a prescheduled basis or by immediate override.

d. HART shall include a workload management capability that dynamically, and to the maximum extent practicable, automatically manages workload prioritization, scheduling, and processing in response to varying workload conditions to facilitate compliance with OBIM SLAs and achieve overall processing efficiency.

e. HART shall manage the execution of the mix of service requests submitted by OBIM customers through established interfaces and batched transactions delivered as datasets separately from normal interface submissions to ensure that SLAs are met and that system resource utilization is optimized automatically with minimal need for operator intervention or override.

f. HART shall monitor the workload under active management and processing at any given point in time and shall generate dashboard displays for OBIM systems administrators to monitor real time system activity. HART shall also generate periodic workload analyses covering pre-selected time periods for evaluating overall system workload management.

g. HART shall identify processing bottlenecks, automatically override transaction processing priorities to ensure SLA fulfillment, and provide the capability for systems administrators to dynamically modify transaction priorities to account for special or unforeseen circumstances such as special processing requests or system failures. HART shall also log all automated priority modifications and manual priority overrides for later priority tuning analysis.

h. HART shall record audit trails of changes made to service request processing priorities and changes made to system operating parameters and thresholds.

2.7 Biometric Matching

In Increment 1, HART will process biometric matching requests for all of the biometric modalities currently being processed by IDENT. IDENT currently has five (5) matching subsystems: 10-print fingerprint, 2-print fingerprint, latent fingerprint, iris, and face. At present, the iris and face MMBS matching is limited in scale. The current limitations include: limited numbers of transactions being processed; no attempt to reconcile or “fuse” the separate matching results from the iris and face matching subsystems for increased accuracy and returning to the service requestor the raw results of both the iris and face matchers.

The interface between IDENT and each of the existing matching subsystems conforms to the IDENT Matcher Interface Service (MIS) Specification. OBIM’s matching vendors were tasked with modifying the interface to their respective matching subsystems to comply with the MIS specification.

In Increment 1, the HART Contractor shall implement fingerprint matching capabilities that will encompass 10-print, 2-print, and latent print matching. The Contractor may retain some or all of the current IDENT fingerprint matching technologies, may choose to replace those existing technologies, or choose to introduce new technologies to operate in parallel with existing technologies. The existing limited-scale MMBS iris and face matching subsystem will be retained during HART Increment 1.

a. The HART Contractor shall implement a biometric matching subsystem interface that shall be the common, well-defined interface through which the HART core application shall communicate with all biometric matching subsystems – current and future.

b. The Contractor shall connect all of the HART biometric matching subsystems to the HART application through the HART biometric matching subsystem interface as the standard for connecting biometric matching subsystems to the HART core application. These subsystems may include the redesigned or retained 10-print and 2-print fingerprint matching subsystems, the unmodified limited-scale MMBS iris and face matching subsystems, and the latent print matching system – whether the retained CABIS subsystem or a replacement. The HART Contractor shall make any modifications to the interfaces to existing matching subsystems necessary in order to connect those subsystems to HART.

c. The HART system architecture shall be designed to enable the expansion of biometric matching capability by the addition of subsystems for matching existing modalities (i.e. fingerprint, iris, and face) and by adding subsystems for matching new biometric modalities. This architecture shall enable the removal or replacement of biometric matching subsystems without impact beyond the subsystem connection through the HART biometric matching subsystem interface and necessary workflow modifications.

d. The HART system architecture shall be designed to provide a clear path for increasing the processing and storage capacity of all biometric matching capabilities to accommodate increasing volumes of matching requests and growth in gallery sizes.

e. HART shall have an open biometric matching subsystem interface that will enable any biometric matching vendor to develop an interface that conforms to the HART biometric matching subsystem interface specification. Conformance with that specification will allow any vendor's matching technology to integrate with HART. The HART biometric matching subsystem interface shall be an open application programming interface for connecting any biometric matching subsystem to the HART core application, regardless of vendor or modality to be matched.

f. The HART Contractor shall document the HART biometric matching subsystem interface in a formal specification suitable for distribution to biometric matching technology vendors or third party developers for use in integrating vendor matching solutions with HART.

g. The HART architectural framework shall be open and flexible to allow multiple vendors' biometric matching technologies to operate concurrently for each biometric modality. The system shall also have the capability to add, update, and remove matching algorithms in each matching subsystem.

h. HART shall perform quality assessments on each submitted biometric image during receipt processing.

i. HART shall have a configurable capability to set quality thresholds.

j. HART shall have the capability to assess quality based on multiple standards including, at a minimum, National Institute of Standards and Technology (NIST) standards.

k. HART shall be capable of adding additional quality standards and assessing image quality against those standards.

l. HART shall be capable of removing, replacing, or updating quality standard comparison parameters.

m. HART shall also be capable of storing multiple quality assessments against different standards for each image.

n. HART shall achieve accuracy levels in matching biometric modalities listed in Appendix A.

o. HART shall achieve the system response time targets specified in Appendix A. Those response times are for the sum of the processing time attributed to the biometric matching subsystems added to the processing time attributed to the HART core application.

p. HART shall have the ability to route candidate matches to a submitted image to the BSC for expert examiner review and match determination when either the submitted image or the reference image is of low quality or where the results of matching operations are indeterminate.

q. When a matching operation against the full biometric gallery using one or more biometrics returns one or more candidate matches, HART shall record the result of that matching operation, the biometric images used as search parameters, and the context (i.e. time, date, location, agency, officer, purpose, documents, source of match determination, etc.) in a transaction log that shall be retained for an OBIM-specified period of time.

r. HART shall be capable of accepting bulk transmissions of biometric transactions or deliveries of transactions in bulk file format and processing those transactions to accomplish high volume on-boarding of new customers or historical identity loading. HART shall execute transactions received in bulk quantities at low priority to avoid interference with current processing demand. Biometric transactions received in bulk may be fingerprint, latent print, iris, or facial modality transactions. This will be a new capability not currently available in IDENT.

2.7.1 Fingerprint Matching – 10-Print and 2-Print

In Increment 1 the Contractor shall deploy fingerprint matching capabilities that satisfy the performance and accuracy requirements specified in Appendix A. IDENT currently has separate fingerprint galleries for 10-print and 2-print modalities. Matching for each is performed by a 3M Cogent matching subsystem. The government seeks creative technical approaches to fingerprint matching that meet service level agreement performance guarantees and offer opportunities for optimizing efficiency in both hardware and software design and operation. The government encourages solutions that offer opportunities for initial and ongoing cost control.

a. HART shall implement fingerprint matching capabilities that meet the performance and accuracy targets listed in Appendix A.

b. HART biometric matching subsystems shall communicate with the HART core application through the HART biometric matching subsystem interface.

c. OBIM is open to technical strategies including but not limited to the following:

    1. Increasing the capacity of the existing duplexed IDENT fingerprint subsystems, one currently resident in each of the DHS Enterprise Data Centers, to satisfy future growth projections and performance requirements.

    2. Introducing completely new fingerprint matching subsystems to replace one or both of the existing IDENT fingerprint subsystems.

    3. Including multiple vendor fingerprint matching technologies or multiple matching algorithms from one or more vendors that may be focused on different processing tasks or workloads.

    4. Re-engineering the currently separate 10-print and 2-print matching subsystems into a single subsystem with a single fingerprint gallery. OBIM recognizes that 10-print and 2-print can be combined into a single gallery.

d. OBIM is open to matching solutions hosted as described under Hosting Environments in Section 8.1, *Guidelines.*

e. The HART fingerprint matching subsystem(s) shall support the forecast matching transaction volumes summarized in Appendix B.

f. The HART fingerprint matching subsystem(s) shall be scalable such that the increasing volume of fingerprints can be managed within the proposed architecture and such that matching subsystem performance and response can be maintained with appropriate capacity upgrades as the fingerprint gallery increases in size.

g. The Contractor shall provision all biometric matching capabilities.

    1. For data center hosted solutions, the Contractor shall design, size, procure, and installed any infrastructure (e.g. servers, data storage, and networking) needed to host the proposed matching subsystem(s).

    2. For matching provided as a cloud-based infrastructure service, the Contractor shall establish that service and provision all capabilities necessary to interface that service to the HART core application.

h. The Contractor shall provision any communications capacity necessary for the proposed solution design.

i. If the HART Contractor introduces a new fingerprint matching technology, the Contractor shall enroll those legacy fingerprint images currently residing in IDENT image storage, if necessary, in the HART matching subsystem employing that new matching technology.

j. The Contractor shall migrate fingerprint matching operations from the existing legacy fingerprint matching subsystem to the HART system. Matching operations will continue

during the migration from IDENT to HART without interruption or performance degradation.

2.7.2 Latent Fingerprint

HART shall have a latent fingerprint management subsystem. The IDENT system currently utilizes the 3M Cogent CABIS system and Cogent Programmable Matching Accelerator (PMA) hardware matchers as its latent fingerprint management subsystem.

CABIS is a commercial product currently consisting of a matcher interface, back end database, and the CABIS front-end interface. The matcher interface acts as the communication layer between the latent sub-system and IDENT. IDENT manages enrollments of IDENT known-print records both in IDENT and in the latent system. There is also a process where a daily download of new latent prints is received by the latent system, automatically encoded, and launched for matching against the known-print galleries in the latent system. Candidate matches to the known-print gallery from both processes are reviewed by latent print examiners in the Biometric Support Center using CABIS workstations. Match adjudication results are recorded in the latent sub-system and reported on from there. If a submitted latent print is not identified, it is enrolled in the Unsolved Latent File (ULF).

All fingerprints submitted by OBIM's customers are enrolled both in IDENT fingerprint galleries and in the latent print galleries. The "known-print" gallery in the latent system therefore contains at least one set of prints for each identity in IDENT; some records with derogatory information may have more than one latent enrollment to account for rolled and flat prints for additional matching accuracy on those high interest records. There are currently approximately 200 million identities enrolled in the latent known print gallery and 350 thousand in the ULF. Because each identity enrolled in the IDENT production matching subsystem is also enrolled separately in the latent system, growth of the latent print gallery can be expected to mirror that of the IDENT production fingerprint matching subsystem.

a. The HART Contractor shall implement a latent print matching capability. This capability may be achieved by reusing the existing CABIS, by introducing a replacement system, by introducing a new technology to operate alongside CABIS, or by providing a cloud-based infrastructure service. The HART latent fingerprint matching subsystem may be cloud-based, a physical subsystem installed on-site in the DHS Enterprise Data Centers, a physical subsystem hosted in some other data center, or a hybrid of these approaches.

b. The HART latent fingerprint matching subsystem shall be scalable such that the increasing volume of fingerprints can be managed within the proposed architecture.

c. HART latent fingerprint matching solution shall communicate with the HART core application through the HART biometric matching subsystem interface.

d. HART shall receive and process incoming service requests for latent fingerprint image matching and addition to the HART latent print gallery.

e. HART shall generate responses to the initial request, if required, using the message format specified for that response.

f. HART shall store incoming latent fingerprint images in the HART biometric modality image store, enroll those images in both the HART latent fingerprint

matching subsystem and the HART production fingerprint matching subsystem, and compare the submitted latent prints against the full OBIM fingerprint gallery for potential matches.

g. HART shall forward potential matches to the BSC for examiner confirmation.

h. HART shall have the ability to compare latent fingerprint submissions to the system's existing 10-print and 2-print fingerprint holdings and generate a list of candidate matches to those existing fingerprint holdings.

i. HART shall provide the ability for identities associated with fingerprints to be marked as having been matched to a latent submission.

j. HART shall provide BSC with tools necessary to allow them to compare 10-print and latent fingerprint images submitted through HART interfaces and through direct external communications to images stored in the OBIM image data stores.

k. HART shall provide the BSC with the capability to manage the incoming matching workload from HART, assign priorities to incoming match requests, reprioritize in-queue match requests, distribute the matching workload among BSC examiners, track work queues and time to examination completion, and generate workload analyses.

l. HART shall provide the BSC with the capability to receive fingerprints from non-HART sources, dispatch those fingerprints to HART for enrollment in the latent or 10-print fingerprint galleries as appropriate, and examine those prints received out-of-band in the same manner as prints received through regular HART customer interfaces. HART shall enable BSC examiners to examine all prints, regardless of source, using BSC examination tools.

m. The Contractor shall enroll legacy latent print images currently residing in IDENT image storage, as necessary during migration from IDENT to HART, in the HART latent fingerprint matching subsystem. Reenrollment will likely involve expert examiner interaction and print remarking. Latent print matching operations shall successfully transition from the existing legacy latent print matching subsystem to the HART system. Matching operations shall continue during the transition from the old system to the new system without interruption or performance degradation.

2.7.3 Multimodal Bridge Solution (MMBS)

The MMBS is IDENT's low volume iris and facial matching subsystem. MMBS runs on the existing IDENT infrastructure and responds to messages submitted using the IDENT MIS specification. MMBS is implemented using NEC Integra technology and employs DeltaID and NEC iris matching algorithms and a NEC facial matching algorithm. MMBS communicates with IDENT using the MIS specification and TIBCO Enterprise Messaging Service queues on the IDENT Enterprise Service Bus.

a. HART shall support the continued operation of the MMBS until the Increment 2 multimodal capability has been implemented.

b. HART shall interface with the MMBS and transmit matching requests to MMBS. MMBS shall continue to receive matching requests conforming to the MIS specification and operate until such time as the HART multimodal capability is implemented and iris and

facial matching has been successfully migrated from MMBS to the HART multimodal capability.

c. The HART Contractor, as part of the implementation of HART Increment 1, shall ensure that the MMBS continues to operate and receive and respond to matching request messages without interference.

d. The HART Contractor shall make any modifications necessary to enable the MMBS NEC matching subsystem to connect to the HART core system.

2.8 Biometric Support Center Support Tools

Support for BSC examiners requires that software applications be provided to allow them to perform essential biometric examination operations and that existing software applications continue to operate until replaced by next-generation capabilities.

2.8.1 Basic Support Capabilities

HART shall provide essential examination support applications for BSC examiners.

a. HART shall provide BSC examiners with tools necessary to allow them to compare submitted fingerprint images to file images that are candidates for a match; perform biometric image corrections; retrieve current and historical identity information; retrieve a history of changes to identity information; and make necessary corrections to identity information and resolve incorrect associations of biometric images with identities.

b. HART shall provide BSC examiners with the capability to retrieve and view any image independent of matching operations for troubleshooting, correction, and redress purposes. This applies specifically to iris images for resolving easily identifiable issues (e.g. cosmetic contact lens; partially obstructed image) but not to issues associated with matching operations.

c. HART shall provide BSC examiners with the capability to override automated HART match determinations. In Increment 1, this routing shall be limited to potential fingerprint matches.

d. HART Contractor shall ensure that there are sufficient numbers of software licenses to support a minimum of 64 fingerprint examiners in two locations: San Diego CA and Arlington VA.

2.8.2 Support Application Upgrades

The BSC currently has two software applications used for performing its identity management operations that require interaction with the current IDENT identity and image databases and will require interaction with the HART data stores in the future. Those tools are the Candidate Verification Tool (CVT) and SIT. CVT and SIT are custom coded applications. CVT interacts directly with the IDENT database to perform its operations; this system will require modification to interact with the new HART identity database. SIT interacts with the current IDENT database using service request messages conforming to the IXM specification and using four additional service requests that are not part of the IXM specification. CVT requires modification by the HART Contractor; SIT does not require modification.

a. The Contractor shall modify the CVT application so that it operates under HART and provides the same functionality that it currently provides while operating with IDENT. The modification shall enable the CVT application to interact directly with the future HART identity and image data stores. The Contractor shall assume maintenance and enhancement responsibility for the CVT application under HART.
b. The Contractor shall configure the HART core application so that it can receive, process, and respond to all message formats in the IXM specification and to the four additional service requests submitted by the SIT application that are not found in the IXM specification. These services are:
    i) Merge identities;
    ii) Separate identities;
    iii) Add and remove photographs; and
    iv) Delete encounters.

2.9 System Management

HART will provide OBIM with capabilities for dynamically managing the HART transaction processing environment, providing visibility into the operations of that environment, and generating after-the-fact analyses and records of service volumes and efficiency of service delivery.

a. HART shall provide the capability for system administrators to perform system operations management and modify system operational parameters without having to engage in source-code-level systems development (maintenance programming) activities and associated code-level testing.
b. HART shall provide an administrative interface that will allow systems and business administrators to create and modify processing workflows, configure business processing rules, load and update customer SLAs, and perform other routine operations.
c. HART shall provide the capability to track and log changes made to workflows, business processing rules, SLAs, and other administrative parameters and shall maintain audit trails of all such changes.
d. HART shall create logs of identity transactions executed and of administrative changes made to the system. The system shall create and retain audit logs of all identity data retrieval requests, searches, and biometric matching results disseminated in response to customer service requests. It shall also capture processing statistics, metrics, and analytical data for performing system operations and root cause analyses.
e. HART shall include a capability that establishes transaction processing performance baselines, monitors transaction performance relative to those baselines, detects deviations from baseline performance and diagnoses performance problems and isolates those problems to the specific subsystem where the problem originated in under an hour.
f. HART shall create dashboard displays showing current system operating statistics, work queues, and general system health characteristics to enable system managers to assess and respond to processing issues in real time.

g. HART shall create standard operations reports and enable the creation of ad-hoc reports from various dashboard displays by system administrators.

h. HART shall include the generation of periodic operational reports analyzing such system characteristics as overall transaction response times, response times delivered to specific customers, general workload management and disposition, log file analysis, and out of band operating incidents for further investigation and remedy.

2.10 Performance Testing Prior to Production

OBIM requires that all new applications and maintenance or enhancement releases of existing applications be subjected to performance testing prior to being deployed in production. This testing shall stress the HART application with workloads that both approximate and exceed workloads expected to be encountered in actual production processing. This test will determine whether the application meets its response time and matching accuracy targets.

a. The Contractor shall develop a plan for executing a performance test for the HART system developed and integrated during Increment 1 that exercises all components of the HART application, employs quantities of transaction data that approximate anticipated transaction throughput, and operates against a representative identity database.

b. The Contractor shall employ an OBIM-provided set of identities including identities selected for both transaction throughput and matching accuracy testing. This set of identities will consist of approximately 50 million identities for volume testing. This set of identities will have corresponding images – multiple per modality per identity – for use in testing.

c. The Contractor shall implement a simulation capability to supplement the OBIM-provided set of identities (see above) to increase the stress load on the system up to and beyond OBIM's forecasts for growth in its identity data stores.

d. The Contractor shall provide the infrastructure necessary for the performance test and ensure its installation and operational support. For HART Increment 1, the performance test infrastructure may consist of all or part of that infrastructure that that the Contractor has put in place to host HART production processing provided that IDENT production processing is not degraded. Alternatively, in Increment 1, the performance test infrastructure may be independent of the HART production environment and may include all or part of the full Performance Test Environment that the Offeror will deliver as part of the HART effort.

e. Following the achievement of IOC, the Contractor shall conduct all required performance tests using the Performance Test Environment infrastructure.

f. The Contractor shall ensure that the selected testing environment generates sufficient measurement data to demonstrate at a minimum response times achieved, matching accuracy levels attained, control of access to and release of system data, security and access control, and transaction volumes processed.

2.11 Performance Test Environment

HART shall include an independent testing environment for stress testing HART and other OBIM applications prior to implementation in production without affecting system availability or degrading production processing performance. OBIM does not currently have a robust testing environment that is independent of the IDENT production environment in which it can stress test new releases of the current IDENT system and has been criticized for installing system releases in production without prior high-volume stress testing. The HART Performance Test Environment will be the venue for performing appropriate stress testing and will house sufficient amounts of test data (i.e. transaction data, identity data, and image data) to allow for the approximation of production processing volumes. OBIM will provide the necessary test data for test execution. Performance and stress tests shall be conducted prior to moving HART applications into the production processing environment.

a. HART shall implement a permanent performance testing environment that is independent of the HART production environment and is capable of subjecting HART and its component applications to performance tests that replicate production workloads in transaction volume, timing, mix of transaction types and sources, interfaces, and workload management configuration. This test environment shall enable the assessment of HART's ability to withstand and process workloads that match and exceed anticipated production workloads.

b. The HART Performance Test Environment shall archive performance data and related input conditions to support regression analysis of performance.

c. The Performance Test Environment shall be independent of the production processing environment and shall duplicate the architecture, but not necessarily the sizing or the specific equipment items, in the HART production environment. This environment shall contain all of the operating system, application, data management, system management and monitoring, and utility software found in the production environment.

d. The Performance Test Environment may be hosted following the *Hosting Environments* guidelines in Section 8.1. If the Performance Test Environment is not hosted in the same facility as the production environment, it should employ the same hardware as the production environment. If any part of the production environment is hosted in the cloud, the corresponding elements of the Performance Test Environment should be hosted by the same cloud provider.

e. The Performance Test Environment shall host a test identity data store, a test image data store, and a test transaction stream that includes a set of business processing transactions for test purposes that reflects a typical mix transaction types encountered in normal production processing. Test data shall also include matching accuracy test cases that can be used to verify the matching accuracy of each of the HART matching subsystems. The test identity database shall contain a sufficient volume of identity and associated data to approximate production processing performance of data access, retrieval, and update operations during testing. The accuracy test database shall be able to be updated periodically to add test cases to address changing characteristics of incoming biometric modality images and to add test cases for new biometric modalities. The actual test data will be provided by OBIM.

f. The Performance Test Environment shall be able to store a transaction stream for use in testing and have the capability to resubmit that transaction stream sufficient numbers of times to achieve the necessary transaction volumes.

g. The Performance Test Environment shall be capable of simulating test parameters. The Performance Test Environment will share access to simulation capabilities with the Test Systems described in Section 5.5. HART testing environments shall have the capability to simulate the following:

    i. Transaction load – a capability to generate a test transaction stream in lieu of or in addition to a stream of IDENT transactions captured for testing purposes.

    ii. Biometric matching operation – a capability to simulate the action of biometric matching capabilities during testing operations when actual biometric matchers are unavailable and for volume testing when matchers attached to a test system lack the capacity for production level processing. This simulation is a substitute for a full complement of biometric modality matching subsystems when biometric matching performance or accuracy is not specifically being tested.

    iii. Interfaces – a capability to simulate interfaces with external systems currently connecting to IDENT for test purposes without the participation of the external interface owning organization.

    iv. End user interaction – a capability to simulate end user system interactions for testing purposes.

h. The Performance Test Environment shall include monitoring, data capture, and logging capabilities necessary to collect the data necessary to demonstrate performance results using analytical methods to determine test result accuracy.

i. The Performance Test Environment shall include a limited scale matching subsystem for each matching technology present in the HART production system for each biometric modality being matched by the overall system. Each matching subsystem shall have the capacity to hold and process a gallery of 2 million identities for each distinct modality to be matched by HART (i.e. 10-print; 2-print; iris, and face). The Performance Test Environment shall also be capable of connecting to additional matching subsystems for testing different matching technologies for current or biometric modalities and technologies for matching additional biometric modalities in the future. These limited scale systems shall be used for conducting matching accuracy tests and shall house specialized ground truth test data (i.e. transaction and identity data) for evaluating the accuracy of biometric matching technologies.

j. The Performance Test Environment shall have the capability to manage a test data set and restore that data set to its pre-test condition following performance tests.

k. The Contractor shall provide Level 2 and Level 3 operational support (see Appendix C, *Definitions*) for the Performance Test Environment if implemented in a DHS Enterprise Data center and ensure the equivalent of Level 1, 2, and 3 operational support if all or part of that environment is hosted in other data centers or implemented using cloud-based infrastructure services.

l. The HART Contractor shall manage the operation of the Performance Test Environment.

m. At IOC, the Performance Test Environment shall be provisioned with the application software, data storage capacity, computing capacity, and data necessary to conduct production volume stress tests of the HART Increment 1 core application suite and infrastructure. Post-IOC, this environment shall be used to stress test all additions, updates, and enhancements to the HART system before being transferred into the HART production processing environment.

n. The Contractor shall provision the Performance Test Environment so that it duplicates the architecture of the HART production environment but not necessarily the capacity. This provisioning shall include provisioning all required computing, data storage, networking, and software services for cloud-based implementations. Provisioning shall include the procurement of any computing, data storage, networking, peripheral equipment, and software infrastructure necessary for data center implementations and ensuring the delivery and installation of that infrastructure in the subject data centers. For cloud-based infrastructure service implementations, provisioning shall include providing all capabilities and capacities necessary to support the testing objectives of the environment. The Contractor shall ensure that the entire Performance Test Environment and all of its components have been tested and are in an operational state.

o. Performance Test Environment software or software services shall include all infrastructure software (e.g. operating systems, utilities, monitoring applications, data store management systems, etc.) necessary to mirror the HART production software environment; all software tools to be used in testing the HART system processing application; and all COTS, GOTS, or open-source applications integrated into HART.

p. The Performance Test Environment architecture shall, to the extent practicable, be sufficiently flexible so as to enable the rapid reconfiguration of test components and test data

2.12 Pre-Production Operations and Maintenance Support

Depending upon the Contractor's system architecture and deployment plan, the resulting HART testing and production systems and all associated subsystems may be hosted following the *Hosting Environments* guidelines in Section 8.1.

Components of both test and production systems will be implemented in their respective hosting environments during system development and integration.

a. The HART Contractor shall ensure the provision of Level 1, Level 2, and Level 3 pre-production O&M support for all HART components and subsystems depending on hosting arrangements. See Appendix C, Definitions, for a description of Levels 1, 2, and 3. This applies to virtualized developmental and testing environments, the Performance Test Environment, and production environments – both before and after the initiation of production processing.

b. For HART components installed in DHS Data Centers, the Contractor shall provide Level 2 and Level 3 O&M support beginning with the installation of those components in the data center. DHS has contracts in place that provide Level 1 O&M support for systems installed in the DHS Enterprise Data Centers; OBIM will issue the necessary contracts or task orders for this Level 1 support. All HART components residing in the

Enterprise Data Centers will receive Level 1 O&M support under those existing contracts.

c. For HART components that are retained from the IDENT system, the Contractor shall assume Level 2 and Level 3 O&M support for those components at the time they are incorporated into the HART system architecture. At IDENT retirement, all remaining components of the IDENT infrastructure planned to be absorbed into HART shall transfer to the HART Contractor for Level 2 and Level 3 O&M support.

d. For HART components provisioned as a cloud-based infrastructure the HART Contractor shall ensure the provision of the equivalent of Level 1, Level 2, and Level 3 equivalent O&M support from the date of service initiation for the cloud-based services.

e. The Contractor shall apply regular system patches and implement HART application upgrades, software patches, and application releases no less frequently than monthly.

f. The Contractor shall apply security patches within 20 business days from patch release or as directed by the Government.

2.13 Migration from IDENT to HART Production Processing

The progression of HART from development through integration, testing, acceptance to implementation of production operation will require the planning of a phased migration of customer workload from IDENT to HART; the conversion of IDENT data stores into their HART equivalents; a period of parallel operation of IDENT and HART maintaining synchronization between IDENT and HART data stores; and contingency planning in the event that reversion to IDENT becomes necessary.

a. The Increment 1 migration from IDENT operations to HART operations shall occur without unscheduled interruption of service delivery to OBIM's customers, with minimal scheduled service outages, and without degradation in service levels (response time) to those customers. This shall apply to any incremental implementation of HART functionality.

b. Any IDENT components or subsystems planned for reuse into HART shall continue to support IDENT processing and support IDENT service delivery without interruption until such time as those components are no longer required for IDENT processing.

c. Migration from IDENT to HART shall be preceded by the modification of the CVT application used by BSC examiners to ensure the continuation of support for 10-print and 2-print fingerprint match adjudication during and after migration (See Section 2.8.2).

d. A migration plan addressing both system and data store conversion and migration shall be developed and submitted to the Government for review and approval. The plan shall also address the phased migration of OBIM customers from IDENT to HART processing.

e. Migration shall be accompanied by fully documented operating procedures that detail the process for executing the migration from IDENT to HART, including procedures for the installation, operation, and maintenance of the HART core application suite and supporting infrastructure developed during Increment 1.

f. As part of HART migration all identity, encounter, and image data characterizing identities in the production IDENT identity and image data stores shall be converted from the IDENT data store structure to the HART data structure. Conversion shall include a quality assessment of IDENT identity data and any data clean-up, separation of identities, identity deduplication, identity consolidation, data correction, or other data modification that may be necessary to prepare IDENT identity data for loading into the HART data store structure. The Contractor may use any existing OBIM data migration tools, data cleansing tools, and data correction methods and techniques in the migration effort.

g. The Contractor shall migrate fingerprint matching operations from the existing legacy fingerprint matching subsystem to the HART system. The Contractor shall, if necessary, enroll legacy fingerprint images in the HART fingerprint matching subsystem(s) as part of the migration. Fingerprint matching operations will continue during the migration from IDENT to HART without interruption or performance degradation.

h. The HART Contractor shall procure or develop any applications necessary for accomplishing data store conversion and shall provision any temporary computing or data storage infrastructure that the Contractor's migration plan deems necessary to accomplish the IDENT data store conversion and subsequent coordination between IDENT and HART during parallel operations. Any temporary computing capacity or data storage, if required, may either be cloud-based or installed in a data center.

i. During parallel operations, database updates to legacy IDENT and HART shall be kept in synchronization; updates shall be made to both systems' data stores.

j. The HART Contractor shall test all elements of the data migration effort prior to conducting the actual migration.

2.14 Increment 1 – Customer Migration

During Increment 1, the Contractor shall transition OBIM customers from IDENT processing to processing under HART. The contractor shall migrate a minimum of one customer during Increment 1.

a. The HART Contractor shall identify the OBIM customers to be migrated and develop a plan for accomplishing the migration.

b. The HART Contractor shall coordinate with each customer to configure and test each customer's service request interface to ensure that the interface has been properly configured and that interface operation and interaction with HART have been successfully tested and demonstrate proper service execution.

c. The HART Contractor shall schedule and coordinate the redirection of each customer's incoming service requests from IDENT to HART.

d. In Increment 1, the HART Contractor shall migrate at least one current OBIM customer from IDENT to HART in order to achieve IOC while IDENT processing continues for the remainder of OBIM customers and without affecting the service response for the migrated customer or other OBIM customers.

e. During Increment 1, the Contractor shall migrate such other customers as practicable during the Increment 1 schedule timeframe.

2.15 Increment 1 – Operational Data Reporting Continuity

OBIM is in the process of implementing a cloud based data warehouse, the ODS/ODR system. This system will include a data warehouse implemented on the AWS GovCloud using the Amazon Redshift database and the Birst business intelligence application. The ODS/ODR consists of two distinct parts: ODS and ODR.

ODS is a data staging area located in the Enterprise Data Center that holds a subset of the IDENT database. Storage size for this subset is currently estimated to be between 40 and 50 terabytes of data. The information in the ODS consists of tables selected from the IDENT Oracle database and copied from the inactive IDENT database into the ODS using Informatica PowerExchange Change Data Capture. The ODS database is managed in a separate Oracle database. The copied tables contain only text identity and biographical information – no biometrics are included.

Informatica PowerCenter executes extract, translate, and load operations to extract data from the ODS and format it for upload to Amazon Simple Storage Service (S3); PowerCenter Integration Service copies data from Amazon S3 to the Amazon Redshift data warehouse for reporting and analytical processing using the Birst business intelligence tool. There are currently forty-one (41) recurring operational reports that will be generated by the ODR. The ODR will be used to respond to ad-hoc information and additional reporting and analytical requests to support OBIM operations and requests from OBIM customers.

The operation of ODS including copying of IDENT Oracle data tables to the ODS, ETL data extraction, and upload to ODR is the responsibility of the Enterprise Data Center operations contractor. Use of the Birst tool operating in the AWS GovCloud will initially be limited to a small number of OBIM staff or support contractors who will provide analytical and reporting services. Use of ODR will expand within OBIM as expertise with the Birst tool becomes more widespread. Eventually, OBIM will grant access to Birst to small numbers of staff in selected customer organizations. Initially, OBIM has contracted for fifty (50) licenses for Birst.

In Increment 1, the cloud portion of the system, the ODR, will remain in place without modification.

a. The HART Contractor shall ensure that the existing ODR system continues to operate during Increment 1. The Contractor shall implement an ETL process operating on the HART data stores that extracts from HART the same information as that currently extracted from the IDENT ODS and formats that extracted data for upload into the existing ODR.

b. The HART Contractor shall operate the ETL process against the HART data stores and upload the data extracted by the HART ETL process to the ODR in the Amazon GovCloud to maintain the currency of ODR data and support continued analytical and reporting operations conducted by OBIM personnel.

Note: ODS/ODR implementation is currently in progress but not yet complete.

ETL specifications and data structures, while not currently available, will be provided when completed.

2.16 Increment 1 Training

The Contractor shall develop and deliver training that will enable OBIM to maintain, operate, enhance, and sustain the HART system as delivered in Increment 1.

a. The Contractor shall develop Increment 1 training for audiences drawn from the following classes of HART system users.
    a. System administration, operation, and hardware maintenance personnel
    b. Software application development, maintenance, and enhancement personnel
    c. BSC biometric examination personnel. (Note: Training for BSC personnel shall be required if and only if any of the relevant tools or systems pertaining to BSC operations have been changed or modified during Increment 1)
b. The Contractor shall develop and deliver training for relevant members of the above three audiences in two modes: 1). Classroom with guided hands-on training; and 2). Web-accessible training available on a self-service basis.
c. The Contractor shall deliver training to contract staff providing HART operations, maintenance, and technical support and to Federal operational and technical staff.
d. Web-based training must be Sharable Content Object Reference Model (SCORM)-compliant and compatible with Internet Explorer version 11 and above, Google Chrome, and other major browsers. Training may be delivered via multiple learning management systems.
e. During Increment 1, the Contractor shall conduct up to 6 sessions of classroom with hands-on training for up to 20 attendees per session and shall address the following topics at a minimum:
    i. HART operations and maintenance for HART production, NPE, and Performance Test environments
    ii. HART system health monitoring and operations management
    iii. HART disaster recovery
    iv. HART automated test and continuous testing frameworks and operations
    v. Biometric identification system workflow definition and modification and business rule specification, modification, and management
    vi. Fingerprint and Latent Print recognition system designs
    vii. New fingerprint examination tools, if introduced during Increment 1
f. The Contractor shall develop the instructional content and presentation and shall conduct the training. The Contractor shall also develop training presenting the same content in a recorded webinar format that can be viewed on a self-service basis.
g. The Contractor shall present each module to OBIM for one (1) instructional design review cycle.
h. If BSC training is required due to a change in BSC tools during Increment 1, the Contractor shall conduct six (6) sessions of classroom with hands-on training to be held in Arlington VA with from 8 to 10 attendees in each session. For BSC personnel located

in San Diego, the Contractor shall conduct five (5) sessions to be held in San Diego for from 8 to 10 attendees per session.

i. The Contractor shall conduct 2 sessions of classroom with hands on training focused specifically on help desk personnel for up to 15 attendees each. The Contractor shall also develop training presenting the same content in a recorded webinar format that can be viewed on a self-service basis.

3 Post-IOC Customer Migration

Following IOC and the completion of Increment 1, the Contractor shall continue the migration of OBIM customers from IDENT to HART until all IDENT service request processing has been migrated to HART and IDENT is no longer processing incoming service requests.

a. The Contractor shall identify those OBIM customers whose service request processing was not migrated to HART during Increment 1.

b. The Contractor shall schedule and coordinate the redirection of each customer's incoming service requests from IDENT to HART.

c. The Contractor shall coordinate with each customer to test each customer's interface and associated services to ensure proper operation and interaction with HART.

d. The Contractor shall successfully complete the migration of OBIM Customers' service request processing from IDENT to HART.

e. The Contractor shall coordinate as required with Government and other contractor personnel responsible for IDENT operation and maintenance to ensure the smooth migration of each customer's processing to HART.

4 HART Increment 2 - Production-Scaled Multimodal Modality Matching and Fusion

Multimodal matching will implement iris and face matching capacities at levels that can meet the projected matching workloads for those modalities. Multimodal matching will introduce those new business processing workflows and business rules necessary to leverage multiple biometric modalities to improve the overall level accuracy of OBIM's matching operations.

4.1 HART Multimodal Infrastructure

Multimodal infrastructure will consist of iris and face matching subsystems capable of meeting HART production processing volume and performance targets specified in Appendix A.

a. HART Increment 2 shall implement high volume iris and facial matching subsystems to its infrastructure.

b. Face and iris matching may be hosted in any environments described in the *Hosting Environments* guidelines in Section 8.1.

c. At the completion of Increment 2, OBIM shall have an identity management system capable of determining whether the fingerprint, iris, and facial image scans on file match those submitted by an OBIM customer.

d. The HART production level iris and facial matching subsystems may be implemented by expanding the capacity of the existing limited scale MMBS pilot iris and facial matching capability. Alternatively, the Contractor may augment the MMBS matching capability or replace it with one or more alternative matching technologies.

e. The Contractor shall select, procure, install, tune, optimize, and implement matching technologies for iris and facial matching subsystems if those subsystems are to be

deployed in an Enterprise Data Center. If those matching services are to be deployed in a non-DHS data center or be provided as a cloud service, the Contractor shall connect that service to the HART core application and ensure that any cloud service provider or alternative data center meets the security requirements in Section 4.1.

f. The Contractor shall design subsystems for iris and facial matching; the Contractor shall acquire, install, and test the infrastructure necessary for implementing those subsystems. The face and iris matching subsystems shall be sized to accommodate the volume of images specified in Appendix B.

g. The Contractor shall transition facial images from the production IDENT image data store and from the MMBS facial matching subsystem, if necessary, into the HART facial matching subsystem. The Contractor shall perform a quality analysis on photographic images currently in IDENT and select those that meet an OBIM specified minimum quality threshold for loading into the HART facial matching subsystem.

h. The Contractor shall transition iris scans from the IDENT image store and from the MMBS iris matching subsystem, if necessary, to the HART iris matching subsystem and shall enroll each iris scan in the HART iris matching subsystem.

i. The Contractor shall connect each matching subsystem (or service) to the HART core application through the HART biometric matching subsystem interface. Each individual subsystem shall be tested for basic operation, performance, and matching accuracy; each subsystem shall meet or exceed the accuracy thresholds specified in Appendix A.

4.2 Multimodal Transaction Processing

HART Increment 2 will implement service request processing that processes iris and facial matching service requests in addition to processing fingerprint matching service requests.

a. The Contractor shall implement the service requests documented in the HART FRD for Increment 2.

b. The Contractor shall implement service requests capable of service request processing for fingerprint, face, or iris modalities individually and in any combination.

c. The Contractor shall develop the necessary workflows and business processing rules required to implement service request processing for each biometric modality individually and shall implement workflows and business rules necessary to implement fusion processing for any combination of biometric matching results from fingerprint, iris, and facial matches and shall integrate those into the HART core application.

d. The Contractor shall develop and implement a fusion capability that can leverage the matching results from combinations of fingerprint, iris, and facial modality matching results from two or more matching subsystems to achieve a higher match confidence and accuracy than would be possible with a single match result from a single modality alone.

e. The Contractor shall transition production iris and facial modality processing from the legacy MMBS subsystem to the new full capacity HART subsystems.

4.3 Multimodal Biometric Service Center Support

The implementation of multimodal processing in HART Increment 2 will increase examination demands on the BSC by adding iris and facial match examination to the BSC's existing fingerprint workload. The BSC will require software applications that will enable its examiners to compare potential iris and facial matches in order to make an expert determination.

a. The Contractor shall equip the BSC with software applications and supporting infrastructure that shall allow examiners to view and compare iris and facial modality scans in addition to 10-print fingerprints and latent prints; resolve indeterminate biometric matches; merge and split identities; resolve incorrectly sequenced biometrics; and transfer mismatched biometrics and biographical data from one identity to another. Those software tools shall enable examination of facial matches and shall enable troubleshooting of iris matching results.

b. The Contractor shall equip the BSC with any infrastructure, software, and associated licenses to accommodate a minimum of fifteen (15) examiners for face and iris match adjudication, nine (9) to be located in San Diego CA and six (6) located in Arlington VA.

c. The Contractor shall integrate new software applications supporting BSC operations with the BSC's automated queue-based workflows and workflow management system.

4.4 Increment 2 Testing Environments

Increment 2 will add capabilities to the HART system. In order for the Performance Test Environment to be capable of subjecting the complete HART application as it exists at the end of Increment 2 to production level transaction processing and data management workloads, additional hardware and software elements may need to be added to that environment to fully reflect the implementation of multimodal processing during Increment 2. Additions to the HART development and test environments may also be necessary for future maintenance and enhancement to the HART application.

a. The Contractor shall complete the build-out of the Performance Test Environment in Increment 2. The Contractor shall make all additions to the Performance Test Environment implemented during Increment 1 necessary to mirror the production environment resulting from Increment 2 development and integration efforts.

    i. The Contractor shall implement all hardware and software capabilities necessary to mirror the HART system production environment. The Contractor shall identify the necessary capabilities and size, acquire, implement, test, and ensure that the environment is ready for the conduct of production volume performance and stress testing.

    ii. The Contractor shall add iris and facial matching subsystems to the Performance Test Environment infrastructure for matching accuracy testing purposes. These subsystems shall be of the same technologies as

those selected for production face and iris matching. Increment 2 shall add simulation capability to substitute for actual iris and facial matching during production workload volume testing.

iii. Test data present in the Performance Test Environment shall include both a test identity data store and a test image data store. The Contractor shall load test identity, image, and transaction data into the Performance Test Environment as necessary to test multimodal biometric matching and fusion and load test data necessary for testing the accuracy of iris and facial modality matching operations.

iv. At the completion of Increment 2, the Contractor shall deliver a fully functioning performance testing infrastructure capability ready to test releases of the HART core application and its associated subsystems under transaction processing loads and database volumes. Tests shall be conducted in a technical environment having an architecture identical to the architecture, but not necessarily the capacity, of the OBIM production processing environment, but which is hosted and provisioned such that testing conducted in the Performance Test Environment has no impact on production system operation, availability, or performance.

b. The Contractor shall implement scaled-down iris and facial matching subsystems accessible by the non-production environment (NPE) testing environments – both the Performance Test Environment and testing systems described in Section 5.5 - to ensure that those environments contain the ability to test each matching technology in use in HART. These environments shall be sized to accommodate galleries holding 2 million iris and 2 million face modality templates.

c. The Contractor shall implement a simulation capability in the NPE testing environments so that application testing can proceed without actually engaging the physical test matching subsystems.

4.5 IXM Specification Version 6.2 Upgrade

Service requests planned for implementation during Increment 2 and specified in the FRD will require updates to the IXM 6.1 specification to accommodate the data requirements of the service requests planned for implementation during Increment 2.

a. The Contractor shall identify the data requirements associated with each service request specified for implementation during HART Increment 2.

b. The HART Contractor shall create IXM version 6.2 which shall be the upgrade to the IXM 6.1 specification developed during Increment 1 necessary to implement all Increment 2 service request data requirements. Note that IXM schema updates should pursue NIEM conformance where appropriate.

c. The Contractor shall implement all HART Increment 2 service requests in accord with the new IXM 6.2 specification and ensure that all HART service requests implemented in both Increment 1 and Increment 2 operate using IXM 6.2

4.6 Increment 2 Training

The implementation of HART Increment 2 will be accompanied by training necessary to enable the future operation and maintenance of the system.

a. The Contractor shall develop and deliver training for new capabilities enabled during increment 2. The Contractor shall also enhance the training developed during Increment 1 to account for system features and functions added to HART during Increment 2 that apply to the following classes of HART system users.
    i. System administration, operation, and hardware maintenance personnel
    ii. Software application development, maintenance, and enhancement personnel
    iii. BSC personnel
b. The Contractor shall develop and deliver training for relevant members of the above three audiences in two modes: 1). Classroom or guided hands-on training; and 2). Web-accessible training available on a self-service basis.
c. The Contractor shall deliver training to contract staff providing HART operations, maintenance, and technical support and to Federal operational and technical staff in the National Capitol Region.
d. Web-based training must be Sharable Content Object Reference Model (SCORM)-compliant and compatible with Internet Explorer version 11 and above, Google Chrome, and other major browsers. Training may be delivered via multiple learning management systems.
e. During Increment 2, the Contractor shall conduct up to 6 sessions of classroom with hands-on training modules specifically related to HART for up to 20 attendees per session that shall address at a minimum the following topics:
    i. HART operations and maintenance update for multimodal processing
    ii. Multimodal processing including workflow definition and modification and business rules creation, modification, and management for multimodal processing
    iii. Iris and Facial examination, comparison, and matching tools for the BSC
    iv. Facial recognition systems design
    v. Facial recognition training for the BSC
    vi. Iris recognition systems design
f. The Contractor shall also enhance the webinar-based training developed during Increment 1 to include the above Increment topics and conduct two (2) sessions of classroom with hands-on training specifically for help desk personnel for 15 attendees each. The Contractor shall also develop training presenting the same content in a recorded webinar format that can be viewed on a self-service basis.
g. The Contractor shall develop training for BSC personnel in the use of those software tools provided to support iris and facial match examination and adjudication. The Contractor shall also develop training presenting the same content in a recorded webinar format that can be viewed on a self-service basis.
h. The Contractor shall conduct two (2) sessions of classroom with hands-on training to be delivered in San Diego CA for 6 to 8 attendees each for BSC personnel located in San Diego, CA and two (2) sessions of classroom with hands-on training to be

delivered in Arlington VA for 6 to 8 attendees each for BSC personnel located in Arlington VA.

i. The Contractor shall present each module to OBIM for one (1) instructional design review cycle.

5 General Objectives

The objectives in this section shall apply to each HART Increment and to each exercised Option.

5.1 Security

HART is categorized as a Federal Information Processing Standard (FIPS) 199 “High”, “High”, “High” for Confidentiality, Integrity, and Availability (CIA) and requires commensurate levels of system security.

a. The Contractor shall design, develop, and implement a security authentication and authorization process for HART that shall integrate with DHS Enterprise Security and shall comply with DHS Sensitive Systems Policy Directive 4300A, Homeland Security Presidential Directive 12, and all other applicable DHS security requirements.

b. The Contractor shall ensure that the HART security authentication and authorization shall comply with the eighteen security control families set forth in NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems* and at https://web.nvd.nist.gov/view/800-53/Rev4/home.

c. The HART Contractor shall ensure that any cloud infrastructure provider included in the HART solution possesses FedRAMP certification at the “High”, “High”, “High” levels and shall ensure that:

   i. Data in the cloud is secured in accordance with all applicable federal regulations, DHS management directives, and industry best practices;

   ii. Audit records are detailed and incidents can be rapidly coordinated with the DHS Security Operations Center (SOC); and

   iii. Statutory data reproducibility requirements and Federal Rules of Evidence for Criminal Proceedings and eDiscovery are supported.

d. The HART Contractor shall ensure that any non-DHS data center proposed as a hosting location for HART meets the minimum security requirements specified in FIPS 200.

e. The HART Contractor shall ensure that any non-DHS data center proposed as a hosting location for HART is certified to host federal information systems with a security categorization of “High”, High”, “High” for CIA as defined in FIPS 199.

f. The Contractor shall ensure that HART interfaces and interacts with the Password Issuance Control System (PICS) and support approved DHS Homeland Security Presidential Directive (HSPD)-12 Public Key Infrastructure (PKI) Methods for access control.

g. HART shall be resilient to denial of service attacks.

h. HART shall be resilient to attacks that cause degradation of service.

i. HART shall implement access controls to mitigate data manipulation attacks.

j. HART shall monitor system activities to identify and take action on:

   i. Potential data manipulation attacks

ii. Potential data exfiltration attacks

k. HART shall maintain separate roles and access privileges as part of a strategy to mitigate external pivot attacks.

5.2 Security Authorization Process

Each major implementation of HART components must complete the security authorization process, formerly known as certification and accreditation (C&A), prior to being placed in operation. The result of a successful security authorization process will be an Authority to Operate (ATO) issued by the Authorizing Official (AO).

a. The Contractor shall execute all security authorization process analysis and generate all required security authorization process artifacts for each HART component or subsystem requiring an ATO. The Contractor shall deliver all security authorization process documentation for transmittal to the DHS Inventory Management Team for entry in the DHS Information Assurance Compliance System (IACS).

b. The Contractor shall generate security authorization artifacts, as determined to be required, leading to an ATO for the all components of the HART program including but not limited to the following:

   i. HART Increment 1 – HART core application and production environment(s);

   ii. HART Increment 1 – Performance Test Environment;

   iii. HART Increment 1 – Non-production development and testing environment;

   iv. HART Increment 1 – Fingerprint matching subsystems for 10-print and latent print matching;

   v. HART Increment 2 – Multimodal face and iris matching subsystems and updates to the HART core application to incorporate face and iris match processing and fusion with fingerprint matching results;

   vi. HART Increment 2 – Performance Test Environment, if required as a result of Increment 2 upgrades;

   vii. HART Increment 2 – Non-production development and testing environment, if required as a result of Increment 2 upgrades; and

   viii. HART Increment 2 – Data Warehouse.

c. The Contractor shall remediate all significant security weaknesses identified in HART during testing or during the security authorization process in a timely manner to allow the AO to issue the ATO for each deployed HART Increment and for each subsequent system release or enhancement.

5.3 Early Delivery of Functionality

The DHS Agile Development and Delivery Instruction identifies Agile as the preferred approach for all IT programs and projects, when appropriate. This guidance is consistent with the concept of modular development as outlined in the *25 Point Implementation Plan*, which places a relatively short “time box” around a project or project segment in which to plan, design, develop,

test, and implement a capability. This guidance calls for the delivery of working software to users in discrete increments within shortened time frames of six months or less for initial delivery of new projects.

a. The Government's objective is to develop and deploy HART in production and begin to phase-out the IDENT system as early as is practicable. To that end the Government encourages the early delivery of useful system segments of capability, ultimately resulting in the early implementation of the system in production. Useful segments may be fully developed, integrated, and tested applications; operations-ready system components such as servers or data storage; necessary development products that are prerequisites for subsequent design and development activities such as the delivery of a data architecture, logical data model or physical data model; the delivery of a subsystem design; or the installation of a system component such as a server ready for application integration.

b. The Government now requires the use of development approaches that embrace Agile principles and that are iterative, useable, and time boxed resulting in the opportunity for the delivery of identifiable, successfully tested, and measurable capabilities sooner in the systems engineering life cycle. The Government invites Contractors to propose innovative strategies to achieve partial or total production operation at the earliest possible point in their proposed schedules using Agile approaches. The Government invites proposals of strategies that provide transparency and visibility into development throughput and performance metrics throughout the development life cycle.

5.4 Testing

HART operational and performance testing shall include testing of HART applications and the procedures developed for system operation, system maintenance, system administration, business process administration, and help desk support.

a. The Contractor shall rigorously test all HART applications prior to acceptance by the Government and shall successfully complete performance and stress testing prior to the transition of the system from test to production operation, according to the test plans developed by the Contractor, approved by the Government, and in accordance with the test strategy and framework documented in the Test and Evaluation Master Plan (TEMP). Performance and stress testing shall occur with operationally-representative transaction and data volumes and the Contractor shall demonstrate system resilience and the ability to meet transaction response requirements specified in SLAs under production workloads.

b. The Contractor shall employ the Agile principle of continuous testing during HART application development and integration.

c. The Contractor shall support third party testing activities in addition to conducting its own testing activities. The Contractor shall support independent verification & validation (IV&V) activities and testing directed by the HART Operational Test Agent (OTA). An IV&V contractor will perform analyses and will execute tests in the various HART system test environments. The HART OTA will design and oversee formal operational testing of the system prior to transition to production. Testing will verify the fulfillment of all HART requirements. The HART Contractor shall provide all artifacts and other

information requested by the Government, IV&V contractor, or the OTA to facilitate validation, verification, and operational testing activities. The Contractor shall work with the OTA and other members of the OT&E community, under HART Program Office direction, to support test data collection and preparation of OT&E plans and procedures.

d. The Contractor shall provide the OTA with design data, system performance data, and analytic support as needed to support the operations test team's independent assessment of the HART design.

e. During the Early Operational Assessment phase, the HART Contractor shall be responsible for providing the OTA with design data and analytic support at such times as are needed to support the operational test team's independent assessment of the HART design. To ensure effective and efficient integrated test and evaluation, the HART Contractor shall support questions and answers for the IV&V contractor. The Government will provide copies of project deliverables to the IV&V contractor.

f. The HART contractor shall support and facilitate the deployment of applications to a designated testing environment that the IV&V contractor can access. During both Early Operational and Operational phases, the Hart Contractor's development team shall be responsible for enabling OTA observations of development, test, and evaluation activities. The HART Contractor shall be responsible for data collection and analysis in support of operational test and evaluation during the Concurrent Operational Test and Evaluation and Follow-on Test and Evaluation phases. HART will be operated in parallel with IDENT during these test and evaluation phases.

5.5 Non Production Environment

The delivered HART system shall include operationally representative, fully functional, non-production environments (NPE) to be used in developmental, application integration, functional, integration, performance, operational, and acceptance testing and as a training environment that, at a minimum, meets the capabilities of the existing IDENT training environment. These environments shall be in addition to the Performance Test Environment. These NPEs shall support the testing program described in the HART TEMP. All testing environments including computing capacity, data storage capacity, development tools, testing and test automation tools shall be provisioned by the Contractor.

NPEs will be development and testing environments in which maintenance of the HART application can take place and in which system enhancements can be developed. NPEs shall contain all of the development tools necessary to accomplish system maintenance and enhancement. The NPE environments shall host test data necessary to test HART updates and future system releases while in development life cycle phases and for conducting acceptance tests of system releases.

a. The Contractor shall design, provision, and implement a virtualized NPE to provide test systems necessary to develop, implement, maintain, and enhance the HART application and to which customer systems may connect for testing and customer training purposes.

b. The Contactor shall implement a virtualized NPE testing infrastructure from which development and testing environments can be provisioned automatically in response to on-demand, self-service requests.

c. The Contractor shall determine where and how each testing environment shall be hosted and implemented following the *Hosting Environments* guidelines in Section 8.1.

d. For testing environments proposed to be either totally or partially implemented as cloud services, the Contractor shall ensure that those services include all elements necessary for development and testing.

e. For any testing environments proposed for total or partial installation in a physical data center the Contractor shall design the data center testing environment, procure all hardware and software components necessary for the total implementation of that testing environment, ensure delivery and installation, and ensure that all components are operational.

f. The Contractor shall access any environments located in DHS Enterprise Data Centers remotely.

g. The Contractor shall provision each testing environment with a full suite of development and testing tools used by the Contractor in the development and integration of the HART application including the software repository containing developed HART application code.

h. The Contractor shall implement a defect tracking mechanism within the testing infrastructure for tracking issues identified during the conduct of tests through issue resolution.

i. The Contractor shall provision each testing environment with non-developmental software applications and components that are being integrated into the HART application and provide licenses for all such components for each environment.

j. The Contractor shall design and develop procedures for managing testing environments and for advancing components of the developed and integrated applications through the testing environments, to the Performance Test Environment, and into production.

k. The Contractor shall manage and operate all test systems and provide Level 2 and Level 3 infrastructure support for systems installed in DHS Enterprise Data Centers and ensure provision of Level 1, 2, and 3 support for systems provided in other hosting environments.

l. The Contractor shall provide at least five (5) licenses to the Government for each testing and development tool employed by the Contractor in the development and testing of HART.

m. The Contractor shall implement connections to customer systems for integration testing and customer training purposes. These connections shall support both OBIM and customer integration testing and shall enable OBIM customers to execute test and training scenarios in which their client applications interact with HART. There are currently eight (8) customer systems connected to an IDENT integration testing environment; others may be added at any time. The Contractor shall ensure that these eight existing connections are supported in the HART NPE and shall plan to implement up to four (4) additional customer system connections to the NPE for a total of twelve. The current 8 connecting customers are:

    1. Customs and Border Protection Passenger Systems Program Office (PSPO)

2. Immigration and Customs Enforcement (ICE)
3. Department of State (DOS)
4. United States Citizenship and Immigration Services (USCIS)
5. Federal Emergency Management Agency (FEMA)
6. Transportation Safety Administration (TSA)
7. International Criminal Police Organization (INTERPOL)
8. Department of Justice Criminal Justice Information Services (CJIS)

n. The Contractor shall ensure connection of scaled-down implementations of each type of biometric matching subsystem included in HART to the NPE testing environments. These shall be the same matchers described in Section 2.11 Performance Test Environment. Each scaled-down matching subsystem environment shall be capable of supporting a gallery containing 2 million identities. These implementations will allow OBIM customers to execute very low-volume end-to-end tests of IXM message request processing including matching operations.

o. The Contractor shall design the capacity of the NPE testing environments such that those environments are able to host test data in sufficient quantities, in accordance with the TEMP, to support functional testing.

p. The Contractor shall implement simulation capabilities for use during testing operations. The Contractor shall provide simulation capabilities for transaction load generation, biometric matching simulation, external system interface substitution, and end user interaction as part of the testing infrastructure (See Section 2.11h). These will be the same simulation capabilities called for and accessible in the Performance Test Environment.

q. The Contractor shall develop a program plan that specifies when the testing environments shall be delivered. The Contractor shall plan the delivery of these environments at a point in the schedule in time for integration testing with customer systems prior to system acceptance and performance testing. The Contractor shall deliver the completed HART application into the NPE environment.

5.6 Test Automation, Continuous Testing, and Continuous Integration

OBIM desires to establish an automated testing capability for the HART program and utilize continuous testing approaches during HART development and during subsequent HART maintenance and enhancement. To that end, OBIM desires that the HART Contractor implement such capabilities in the delivered development environment.

a. The Contractor shall implement a test automation framework as part of the NPE testing environments for use during HART development and integration that includes testing tools, programming interfaces, protocols and procedures enabling the automated management of testing activities. The automation framework shall represent and validate production capabilities and shall be updated with new, revised, and retired scripts with each release.

b. The Contractor shall implement a continuous testing framework as part of the NPE testing environments for use during HART development and during subsequent maintenance and enhancement activities.

c. The Contractor shall establish a continuous integration capability and process that requires the integration of developed application code into a source code repository on a regularly scheduled basis and followed by verification of that code through an automated build.

d. HART shall implement and maintain a regression test suite that includes all test cases, data, code, scripts, anticipated results, instructions and other elements necessary for automated test execution through the test automation framework.

e. The Contractor shall deliver to the Government the tools and procedures necessary to operate and maintain the HART automated testing and continuous testing frameworks. The Contractor shall deliver five (5) license for each software tool- within those frameworks, procedures for utilizing those tools, and training in the operation and maintenance of that environment.

5.7 Project Management

HART effort shall be managed according to industry best practices in project and program management and in accordance with the DHS SELC, which is documented in DHS Guidebook 102-01-103-01 and the OBIM HART system SELC Tailoring Plan. The tailored SELC will allow for the accomplishment of the goals of formal SELC gate review events in the context of activities within agile methodologies.

a. The Contractor shall manage its operations and provide timely reporting on management, technical, and financial progress.

b. The Contractor shall develop and maintain an overall integrated schedule of its activities as well as schedules for individual project efforts that the Contractor finds necessary for HART development and implementation. These schedules shall be consistent with the HART contract line item number (CLIN) structure and the HART work breakdown structure (WBS).

c. The Contractor shall meet with the Government not later than 30 business days following contract award to conduct a baseline review addressing project cost/price, schedule and performance to establish common understanding and expectations for the execution of the contract. During the course of this review, the Contractor and the Government shall identify reasonable technical performance measures to be reported regularly to provide the Government with visibility into the Contractor's progress towards developing and delivering the expected capability.

d. The Contractor shall participate in weekly status meetings with representatives of the Government's Project Management Office to review overall progress and any current schedule or technical issues. The Contractor shall provide formal progress and financial reports on a regular basis but not less frequently than monthly to include reporting on the technical performance measures approved by the Government (see 5.7c above).

e. The Contractor shall develop and submit a complete and comprehensive integrated master schedule (IMS) that incorporates all projects, activities, and milestones necessary for the design, development and implementation of HART Increment 1, Increment 2, and optional tasks. Activities include, but are not limited to, major acquisition decision events, systems engineering lifecycle reviews, test events, security, training, etc. The IMS shall provide for regular delivery of configuration items, utilizing an iterative approach, to satisfy the requirements contained in this document. The schedule shall conform to the best practices set forth in the GAO Schedule Assessment Guide (GAO-16-89G) and to the structure of the HART work breakdown and CLIN structures set forth in this contract. The Contractor shall submit this comprehensive schedule and all schedule updates during the course of contract execution to the Government in an electronic format mutually agreed upon with the Government.

f. The initial IMS submission shall be required not later than 20 business days following contract award. All anticipated changes to the schedule baseline shall be communicated to the Contracting Officer's Representative (COR) within three (3) business days of identification; IMS updates shall be delivered bi-weekly. This notification shall include identified impact factors and potential recovery mechanisms. The contractor shall perform schedule risk assessments on the integrated technical and business schedules for all detailed schedules. The government will perform schedule integration within the OBIM Schedules. The contractor shall attend weekly Integrated Project Team (IPT) meetings to identify schedule risks and all known and anticipated schedule variances, to include any potential impacts to the schedule baseline.

g. The Contractor shall inform the Government of changes in schedules for its individual projects and of changes to the Contractor's overall integrated master schedule during the first weekly status meeting following identification of the need for the change.

h. The Contractor shall communicate schedule updates to the Government in an electronic format mutually agreed upon by the Contractor and the Government on a regular basis but not less frequently than monthly.

i. The Contractor shall support the Government's Project Management Office in stakeholder management, communications, outreach, onboarding new customers, and other Government project management office functions.

j. The Contractor shall meet the SELC requirements as specified in the HART SELC Tailoring Plan and shall support the HART Program Management Office in preparations for all gate, oversight, and governance reviews.

k. The Contractor shall present a quarterly In-Progress Review (IPR) briefing to OBIM and HART Program Management addressing program progress, cost/price, schedule, performance, risk, technical, and management issues.

5.8 Requirements Management

The HART development effort shall result in a documented record of functional and system requirements present in an OBIM document repository.

a. The Contractor shall validate and finalize draft HART functional requirements, business processes, and rules. The HART Contractor shall review any business process and

business rules documentation provided by OBIM and shall assess the functional requirements documented in the HART FRD and develop additional detail needed to proceed with system design and development. The Contractor may elect to review existing IDENT documentation, application design, and application source code and any other system documentation and specifications that the Contractor deems necessary to ensure that all business rules and workflows have been captured and migrated into HART.

b. The Contractor shall generate the system requirements necessary to support HART functional requirements and business processing.

c. The Contractor shall ensure traceability of requirements from the Mission Needs Statement, Concept of Operations Document, and Operational Requirements Document to the functional requirements, system requirements, and system design in the OBIM requirements repository tool – Serena Dimensions RM.

d. The Contractor shall manage existing requirements, updates to those requirements, and new requirements in the OBIM requirements management tool throughout the development and implementation of HART.

5.9 Site Coordination and Preparation

Depending upon system design and architecture, HART may include components provided as cloud-based services or as OBIM-owned components hosted in DHS Enterprise Data Centers or other data centers.

a. The Contractor shall coordinate the delivery and installation of HART computing, data storage, networking, and peripheral components required to be installed in DHS Enterprise Data Centers with the Enterprise Data Center support contractors. The Enterprise Data Center support contractors will receive and install HART components and provide continuing system management support for those components.

b. The Contractor shall coordinate the delivery and installation of HART computing, data storage, networking, and peripheral components required to be installed in an alternative data center with the management of that data center. The Contractor shall make provisions for data center management to receive and install HART components and provide continuing system management support for those components.

c. The Contractor shall contract for any cloud-based infrastructure services necessary for the implementation of the proposed HART system architecture and for all communications capabilities necessary to access those services.

d. The Contractor shall coordinate all necessary preparations for deploying OBIM-owned components of the HART production system, test systems, and Performance Test Environment with the management of the destination hosting or service provision environment.

e. The Contractor shall procure all equipment necessary, not reused from IDENT, for the HART infrastructure to be installed in any physical data centers. The Contractor shall be responsible for the provision of any cloud-based processing or storage capabilities included in the HART system architecture.

f. All additions to test and production environments hosted in data centers and to be delivered to OBIM shall be approved beforehand through the OBIM and DHS change management processes.

5.10 Infrastructure Delivery

The Contractor shall ensure the timely delivery of HART components to the physical locations where those components will be deployed. Delivery does not apply to cloud-based system components.

a. The Contractor shall ensure that hardware and infrastructure software procured as part of HART and intended to be installed in DHS Enterprise Data Centers are delivered to one or both of the DHS Enterprise Data Centers as required for installation by the DHS Enterprise Data Center support contractor.

b. The Contractor shall ensure that hardware and infrastructure software procured as part of HART and intended to be installed in alternative data centers are delivered to those data centers for installation in a timely manner according to the Contractor's proposed schedule. The Contractor shall make all arrangements necessary to ensure installation and continuing support of HART components in those data centers.

5.11 Change and Configuration Management

The HART program shall comply with the latest OBIM and DHS change management requirements and processes.

a. The HART Contractor shall either employ a government provided configuration management system or select and implement an equivalent alternative configuration management system for use in managing the configuration of all hardware, software, networking resources, documentation, policies, procedures, requirements, and other artifacts associated with the HART Program.
b. The HART Contractor shall transfer the content of its configuration management system to OBIM applications in use for configuration management:
    a. BMC Remedy – for hardware and software configurations and change request management;
    b. BMC Discovery – for automated IT infrastructure asset identification;
    c. Netbrain – for network topology mapping and configuration discovery;
    d. Serena Dimensions RM – for requirements management;
    e. Serena Dimensions CM – for software code management;
    f. Quality Center – for test management and as the testing repository; and
    g. SharePoint Controlled Document Library – for all HART documentation artifacts.
c. The Contractor shall submit all proposed implementations of and changes to HART environments to the OBIM change management process as specified in the OBIM Change Management Handbook and to the DHS change management process and DHS Infrastructure Change Control Board (ICCB) as specified in the DHS ICCB Process Handbook. The Contractor shall obtain approval prior to proceeding with those implementations and changes.

5.12 Software Delivery

HART software delivery will include the delivery of licenses and rights for non-developmental software products integrated into the HART solution; source code for applications, interfaces and tools custom-developed for HART; and licenses or rights for all design, development, and testing applications used to engineer the final HART application.

a. The delivery of HART shall include any COTS, GOTS, and open-source products that may have been integrated into the solution along with sufficient numbers of licenses for each product as necessary for the implementation of the full system design – production, testing, and Performance Test Environments - along with product keys, as applicable, for all licenses and documentation for each product.

b. Delivery shall also include the delivery of source code, executables, scripts, configuration files and documentation for any software developed as a part of HART. Source code delivery shall include the Contractor's software repository and loading delivered code into an OBIM source code management and control system and software repository.

c. For the purposes of this solicitation, developed software shall include all custom developed portions of HART as well as any auxiliary applications and tools developed to aid in development, testing, and data conversion associated with HART but are not part of the installed system. Delivery shall also include configuration specifications and parameters applicable to each component in HART.

d. The delivery of HART shall include the delivery of (licenses for) the tools used by the Contractor to design and specify the HART infrastructure and tools used to develop, integrate, and test the HART application software components.

e. The Contractor shall deliver to OBIM five (5) licenses for each tool used in the design, development and implementation of HART.

5.13 Knowledge Transfer

OBIM desires that system design and specifications be transferred to the Government formally in the formats specified. The Government also requires that the all designs, specifications, configurations, be transferred to the Government as source files compatible with the tools used to develop those designs, specifications, and configurations. In addition, the Government requires the delivery of licenses for each design and development tool used to implement HART.

a. The Contractor shall deliver all designs, specifications, configurations, logical and physical design views, data management specifications, and software architecture designs to the government both in the format required for formal delivery and in the source format for those design and development applications used to design, develop, and implement HART.

b. The Contractor shall deliver all development, testing, and operating procedures developed in association with HART in the format specified for formal delivery and, if different, as source files for the tools used to develop those procedures.

c. Knowledge transfer shall deliver tools and techniques used to design and document the system, develop the system, test the system, and convert and load data. Knowledge transfer shall also convey procedures used during system development, for operating the

production system, for transitioning from IDENT to HART, for installing releases of HART, and for maintaining HART once in production status.

d. The Contractor shall accomplish knowledge transfer on a “just-in-time” basis throughout the period of performance from the development Contractor to OBIM and to one or more OBIM-designated personnel or contractors.

6 HART Optional Efforts

HART includes six (6) optional efforts. HART Increment 2 will be implemented through the exercise of four of those options. The two other options represent development activities to address situations where OBIM customers do not upgrade to current IXM messaging standards or interface technologies.

- Increment 2 - HART Data Warehouse.
- HART Post-Deployment Support Period 1.
- HART Post-Deployment Support Period 2.
- Legacy Interface Development.
- IDENT Exchange Messages (IXM) Specification Version Translation.
- End of Contract Transition (Transition Out).

6.1 Increment 2 - HART Data Warehouse

HART Increment 2 shall implement OBIM's data warehousing capability. The HART data warehouse will consist of infrastructure that is separate from the HART production environment. This will address a continuing problem for the IDENT architecture in which data analysis and reporting takes place in and degrades the performance of the production environment.

a. In HART Option 2 the Contractor shall establish an analytical data warehouse with data storage hosted on storage devices that are separate from the production HART system data storage. This data warehouse shall enable the generation of data marts, subsets of the warehouse data, for focused analysis. The data warehouse shall allow data manipulation, reporting, and analytical processing to be performed concurrently with HART production processing without affecting the performance of the production HART system. OBIM is in the process of establishing ODS/ODR data warehouse using the Amazon Redshift database with the Birst business intelligence tool implemented on the Amazon GovCloud. The HART data warehouse may expand, enhance, or incorporate, the planned (or existing) ODS/ODR, replace it, or exist in parallel with it.

b. The Contractor shall implement one or more business intelligence tools to access and analyze data resident in the HART data warehouse and may elect to use the Birst business intelligence tool used with the ODR portion of ODS/ODR.

c. The Contractor shall develop a concept of operations for the data warehouse that includes the identification of data in the HART production environment, the continuing population of the data warehouse with HART data extracts from the production system, data cleansing operations, data storage, and data availability for analysis and reporting. The concept of operations shall also establish criteria for retaining data within the data warehouse, and for periodic removal of data no longer required for analytical purposes.

d. Contractor shall design the data warehouse and associated procedures to ensure the integrity of resident data and provide for the recovery of that data following failures of individual warehouse components or of the warehouse as a whole.

e. Contractor shall design and implement the infrastructure for the data warehouse. That infrastructure may consist of the necessary application and data servers, data storage devices, and software applications necessary to support the data warehouse.

f. If the data warehouse system in whole or in part is proposed for installation in DHS Enterprise Data Centers or in other data centers the Contractor shall acquire all infrastructure components necessary for the implementation of the warehouse to include all application and data management servers, data storage devices, communications equipment, and software. The Contractor shall ensure the delivery of those components to the destination data center.

g. If the data warehouse system in whole or in part is proposed to be provided as a cloud-based infrastructure service, the Contractor shall engage the necessary cloud-based services to supply the computing, data storage, and analytical services necessary for data warehouse operation.

h. The Contractor shall provide Level 2 and Level 3 support for Data Warehouse components installed in one or both of the DHS Enterprise Data Centers. The Contractor shall ensure the provision of the equivalent of Level 1, 2, and 3 support services for components installed in non-DHS data centers and for any Data Warehouse components implemented as cloud-based infrastructure services.

i. The Contractor shall select and implement software applications necessary to implement the data warehouse. Applications may include data warehouse management applications, analytical software separate from the data warehouse application, business intelligence, and ETL applications or equivalent for loading data from the production environment into the data warehousing environment. The Contractor shall also implement initial data warehouse-based analytical processing and reporting.

j. The Contractor shall design and implement the data structure for the data warehouse.

k. The Contractor shall import data residing in the existing ODS/ODR data warehouse, transform that data as necessary into HART data warehouse data structures, and load that data into the HART data warehouse.

l. The Contractor shall implement an ETL process to extract data from the HART production database and load that data into the HART data warehouse.

m. Note: The HART Data Warehouse will not be added to the Performance Test Environment.

n. The Contractor shall develop training in the operation and use of the HART data warehouse and its associated software for the following classes of HART data warehouse system users:

    1. System administration and operation personnel;
    2. System application maintenance and usage;
    3. Help desk;

4. OBIM data warehouse users; and
5. OBIM customer data warehouse users.

o. The Contractor shall develop and deliver training for each group in two modes: 1). Classroom with guided hands-on training; and 2). Web-accessible training available on a self-service basis. Web-based training shall comply with SCORM.

p. The Contractor shall conduct 2 sessions of ~~with~~ hands-on training for up to 20 attendees per session that shall cover at a minimum the following topics.
   i. HART data warehouse operation and maintenance
   ii. HART data warehouse system administration and management
   iii. HART data warehouse extract, translate, and load
   iv. Data mart generation
   v. Data warehouse and analytical and business intelligence tool operation to accomplish data query and data analytical operations.

q. The Contractor shall develop the training content and presentation and shall conduct or otherwise arrange for the conduct of the training. The Contractor shall also develop training presenting the same content in a recorded webinar format that can be viewed on a self-service basis.

r. The Contractor shall conduct training evaluations following completion of instruction and present the results to the HART Training Lead.

s. The Contractor shall conduct one (1) session of hands-on training for up to 20 help desk personnel. The Contractor shall also develop training presenting the same content in a recorded webinar format that can be viewed on a self-service basis.

t. The Contractor shall conduct two (2) sessions of hands-on training for up to 20 attendees for data warehouse system administration and operation and maintenance. The Contractor shall also develop training presenting the same content in a recorded webinar format that can be viewed on a self-service basis.

u. The Contractor shall conduct five (5) sessions of classroom training for up to 20 attendees each for end users of data warehouse reporting, query, and analytical capabilities.

v. The Contractor shall submit developed training for one OBIM instructional design review.

6.2 Post-Deployment Support Period 1

It is OBIM's intention to have the HART Contractor provide infrastructure and application support through the initial implementation of HART production processing and during the phased migration of all OBIM customers from IDENT to HART processing.

a. The HART system effort will include an optional period of 12 months of post-deployment support for HART application software and infrastructure implemented during Increment 1 and any HART Increment 2 software and infrastructure that is implemented during the period. The option will commence at the scheduled end of Increment 1 following the achievement of IOC and concurrent with the migration of the 1st OBIM customer to HART processing.

b. Post-deployment support shall also include the provision of Level 2 and Level 3 O&M support services (see Appendix C, *Definition*s) for components of HART installed in DHS Enterprise Data Centers. For HART components installed in non-DHS data centers or provided as cloud-based services, the Contractor shall ensure the provision of the equivalent of Level 1, Level 2, and Level 3 O&M support.

c. Post-deployment support shall include assuming responsibility for Level 2 and Level 3 O&M support for IDENT components retained and incorporated into the HART system architecture and for continuing to meet the SLAs for those components.

d. Post-deployment support shall include the resolution of help desk tickets related to problems with the HART system, generated by the OBIM help desk system.

e. Support under this option shall include fixes to developed portions of the HART application, enhancements to developed portions of the application, implementation of new releases of off-the-shelf applications integrated into the overall HART application, and ensuring maintenance and upgrade support for integrated applications.

f. The Contractor shall apply regular system patches and implement HART application upgrades, software patches, and application releases no less frequently than monthly.

g. The Contractor shall apply security patches within 20 business days from patch release or as directed by the Government.

h. Support under this option shall also include system performance monitoring, and performance tuning as necessary to achieve and sustain the required levels of performance and service delivery.

i. This support shall include performing impact analyses on proposed changes and assisting in prioritizing proposed modifications and planning the releases of new or modified system capabilities.

j. This support shall also include any necessary modifications to operating and administrative procedures discovered after system implementation.

k. Post deployment support shall include consulting with any 3rd party operations and maintenance contractor supporting any aspect of HART O&M to analyze and resolve any system performance and tuning issues. Any additional software capabilities added to the HART system during the support period shall be added to the scope of this support task.

6.3 Post-Deployment Support Period 2

The HART system effort will include a second optional period (Post-Deployment Support – Period 2) of 12 months of post-implementation support the HART application software and HART system infrastructure O&M. The description of this support is identical to the description of the support described for Post-Implementation Support – Period 1 and will initiate at the end of Post Deployment Period 1. The support scope of this support includes all HART software and infrastructure implemented during Increments 1 and 2.

6.4 IDENT Exchange Messages (IXM) Specification Version Translation

Some of OBIM's customers currently submit messages formatted using IXM version 5.0. For a variety of reasons, these customers have not upgraded their message submissions to IXM 6.0.x. In the event that these customers are unable to accomplish the upgrade to the current version of IXM in time for HART IOC implementation, a translation application will be required to ensure continued service delivery to these customers.

a. The Contractor shall develop a translation capability to translate incoming messages in IXM 5.0 format to the IXM 6.0.x format. This capability shall also translate HART responses to those incoming messages from the HART-generated IXM 6.0.x format response to the IXM 5.0 format readable by customer systems.

b. The Contractor shall test the translation application to ensure the proper operation.

c. The Contractor shall implement the translation application for each customer requiring IXM 5.0 message translation prior to that customer's processing being migrated from IDENT to HART.

6.5 Legacy Interface Development

OBIM has customers who currently communicate with IDENT using messages that do not comply with any IXM specification and which are not received on the Enterprise Service Bus. OBIM is currently advocating that each customer employing one of these interfaces upgrade to the use of the Enterprise Service Bus for interface communication and to the IXM specification for request message and response formats. In the event that one or more of these interfaces continue in use by OBIM customers, it will be necessary to continue to support those continuing interfaces both in message format and in communication mechanism.

There are currently twelve (12) such interfaces. See Table 2 for details on each interface.

- Message formats used include:
    - IXM 5.0. Six (6) interfaces use IXM 5.0 message formats.
    - IXM 6.0.x. One (1) interface uses IXM 6.0.x.
    - Non-IXM. Five (5) interfaces employ non-IXM message formats.
- Communication technologies used include:
    - Secure Hypertext Transmission Protocol (HTTPS).
    - IBM Message Queuing (MQ) via legacy propagation bus.
    - Oracle Advanced Queuing (AQ) via legacy propagation bus.
    - Simple Mail Transport Protocol (SMTP) for human-readable email.
    - SQL*NET.

For each remaining legacy interface:

a. The Contractor shall include in the system architecture a mechanism necessary for communicating through for each remaining legacy interface.

b. The Contractor shall develop an application that translates the customer's legacy request message format to IXM 6.0.x format and translates HART IXM 6.0.x responses to the customer's legacy response format.

c. The Contractor shall implement the architectural communications mechanism as part of HART IOC.

d. The Contractor shall implement the translation application for each legacy customer as that customer's processing is migrated from IDENT to HART.

Table 2 lists the specific legacy interfaces and associated technologies.

Table 2. Legacy Interfaces for Optional Development

ID	Customer Organization	Description	Stakeholder	Message Exchange Pattern	IXM	Non IXM Payload Type	Messaging Transport	OBIM BUS or ESB
1	DoJ:FBI:CJIS	EBTS Requests	IAFIS/NGI	Out-Only/In-Only		EBTS	SMTP	ESB
2	DHS:CBP	Data push to ADIS.	ADIS	In-Only/Out-Only	5.0		AQ	BUSPRD
3	DHS:CBP	IXM 5.0 MQ via legacy Propagation BUS.	LANDENTRY	In-Only/Out-Only	5.0		MQ	BUSPRD
4	DHS:USCG	IXM 5.0 (inbound), human- readable email (outbound), SMTP ESB. Currently sends IXM 5.0 request but receives custom email (non-IXM) response.	USCG-BASS	In-Only/Out-Only	5.0		SMTP	ESB
5	DoJ:FBI:CJIS	EFTS Requests	JABS	Out-Only/In-Only		EFTS	SMTP	JABS Gateway
6	DoS	IXM 5.0. AQ via legacy Propagation BUS.	CA	In-Only/Out-Only	5.0		AQ	BUSPRD
7	INTL:UKVISAS	IXM 5.0 AQ via legacy Propagation BUS	UK-Visas	In-Only/Out-Only	5.0		MQ	BUSPRD
8	DHS:ICE ENFORCE	Legacy – non IXM. ENFORCE sync process that copies IDENT data to ENFORCE. E3 handling IXM Services.	ENFORCE			SQL	SQL*NET	EID
9	DHS:CIS	Document Issuance	CIS LEGACY	In-Only/Out-Only	5.0		MQ	BUSPRD
10	DoJ:FBI:CJIS	EBTS Requests	IAFIS/NGI	In-Only/Out-Only	6.07		SMTP	ESB
11	DoJ:FBI:CJIS JABS	Legacy – non-IXM HTTPS between stakeholder and JABS Gateway; SMTP between JABS Gateway and JABS	JABS Client	In-Only/Out-Only		EFTS	HTTPS/HTTP	JABS Gateway
12	DoJ:FBI:CJIS	Legacy – non IXM. HTTPS between CJIS and OBIM Non-IXM interface currently used to receive daily ingest and updates to Wants and Warrants (W/W) and Foreign Special Interest (FSI) datasets.	IAFIS/NGI	In-Only/Out-Only		WList_RQS_WS_VIPS, WHit_RQS_WS_VIPS	HTTPS/HTTP	VIPS

6.6 End of Contract Transition (Transition Out)

The Contractor shall ensure a smooth handoff to the Government and to one or more successor contractors at the government's discretion.

a. The Contractor shall develop a plan for transferring responsibility for HART application and O&M support to the Government and to any successor contractors that the Government should designate.

b. The transition plan shall identify specific Contractor personnel participating in the transition and shall identify the duties of each.

c. The transition plan shall identify all application, management, and operational documentation and procedures necessary for the successful operation of the system.

d. The Contract shall develop a transition plan that identifies key training essential to the continued operations of the system and submit a list of training topics and proposed methods of delivery to the HART Program Manager or delegate for approval prior to

instruction development. The Contractor shall submit developed training for one (1) OBIM instructional design review after initial material development. The Contractor shall deliver that training to two (2) groups of thirty (30) or fewer attendees. Attendees will be a combination of Government and other contractor personnel.

e. The transition plan shall make provision for the cessation of any processing being performed outside of DHS Enterprise Data Centers in coordination with the Government's alternative arrangements for continuing operations.

f. The transition plan shall make provision for the return of any Government furnished equipment and for the return of any Government-owned HART software and data that may be in the Contractor's possession, hosted in non-DHS facilities, or otherwise under the Contractor's control.

g. The Contractor shall execute the transition plan including the return of any data and equipment, transfer of operations, training, general turnover of responsibilities, and cessation of service and operations required to completely close out HART support and related activity.

h. The Contractor shall familiarize successor contractor personnel with all aspects of HART design, operation, and implementation during a period of up to 30 business days while the respective contracts' periods of performance overlap.

i. The Contractor shall brief the Government and any contractors that the government may designate on current system status, performance, and operations and outstanding system issues at the transition point.

7 Deliverables

Production implementation of HART shall be preceded by the delivery of comprehensive procedures for system operation, system maintenance, system administration, data conversion, system transition and help desk support. Standard Operating Procedures (SOPs) for HART include disaster recovery procedures for recovering from the loss of a DHS Enterprise Data Center or other location hosting any portion of HART.

In addition to hardware, software, and services, the Government expects to receive deliverable artifacts that address the scope of deliverable categories listed in this section. Deliverables addressing the scope of each of the following categories of artifacts should be generated and delivered to the Government during the course of the HART design, development, test, installation, operation, and support efforts. Each individual deliverable should be complete, comprehensive, and of high quality. Table 3 lists the expected deliverables.

Each HART deliverable shall be delivered in the unlocked and modifiable electronic format of the application used to develop that deliverable and, where called for, hardcopy and searchable portable document format (.pdf) format. Hardcopy or .pdf formats unaccompanied by electronic formats shall be unacceptable as deliverables. Hardcopy or .pdf versions of deliverables may be submitted along with electronic deliveries to document the as-delivered state of a deliverable. Specific formats for each deliverable shall be specified at contract award.

The Contractor shall deliver to the Government five (5) licenses for each software tool used to develop HART design documentation. The Government may relax this requirement for widely-used software applications (e.g. Microsoft Office and Visio) on a case by case basis.

The Contractor shall submit draft deliverables (excluding weekly deliverables) for Government review five business days prior submission of the final deliverable. Government reserves the right to modify the format requirement for any deliverable. Any format change will be communicated to the contractor at least 10 business days prior to the due date.

Table 3. HART Deliverables

#	Format	Title	Due Date	Submit to:
1	MS Office & Searchable PDF	Project Management Plan (to include Risk Management Plan)	20 business days after contract award	COR, PM
2	MS Project	Integrated master schedule	20 business days after contract award	COR, PM
3	MS Project	Integrated master schedule updates	Bi-weekly	COR, PM
4	TBD at Contract Award	System requirements	TBD at Contract Award	COR, PM
5	TBD at Contract Award	Requirements Traceability Matrix	TBD at Contract Award	COR, PM
6	TBD at Contract Award	Requirements Traceability Matrix	TBD at Contract Award	COR, PM
7	TBD at Contract Award	HART System architecture design	TBD at Contract Award	COR, PM

#	Format	Title	Due Date	Submit to:
8	TBD at Contract Award	HART System architecture design	TBD at Contract Award	COR, PM
9	TBD at Contract Award	Application design for each custom software component	TBD at Contract Award	COR, PM
10	TBD at Contract Award	System testing infrastructure design	TBD at Contract Award	COR, PM
11	TBD at Contract Award	System production infrastructure design	TBD at Contract Award	COR, PM
12	TBD at Contract Award	Data architecture design for HART system identity and biometric image data storage	TBD at Contract Award	COR, PM
13	TBD at Contract Award	Logical data store and data file designs necessary to implement the HART system data architecture	TBD at Contract Award	COR, PM
14	TBD at Contract Award	Physical data store and data file designs necessary to implement the HART system data architecture.	TBD at Contract Award	COR, PM
15	TBD at Contract Award	Test system Bill of Materials	TBD at Contract Award	COR, PM
16	TBD at Contract Award	Production system Bill of Materials	TBD at Contract Award	COR, PM
17	TBD at Contract Award	Infrastructure equipment delivery to DHS Enterprise Data Centers	TBD at Contract Award	COR, PM
18	Licenses and Software	Software licenses for each COTS, GOTS, or open-source application necessary to provision each test and production environment.	TBD at Contract Award	COR, PM
19	Licenses and Software	Software licenses for all data and data store management software required to implement the HART system data architecture	TBD at Contract Award	COR, PM
20	Licenses and Software	Licenses for all software tools used to design and document the HART system – minimum of five (5) licenses per tool.	TBD at Contract Award	COR, PM
21	Licenses and Software	Licenses for each development tool used to develop the HART system application – minimum of five (5) licenses per tool.	TBD at Contract Award	COR, PM
22	Licenses and Software	Licenses for all testing tools introduced by the Contractor minimum of five (5) licenses per tool.	TBD at Contract Award	COR, PM
23	Licenses and Software	Licenses for biometric examination and other software tools introduced into the BSC to accommodate the full population of examiners (i.e. 64 for fingerprint and 15 for face and iris)	TBD at Contract Award	COR, PM

#	Format	Title	Due Date	Submit to:
24	TBD at Contract Award	Data definition code in editable electronic format for each HART system data store and data file necessary to implement the HART system data architecture	TBD at Contract Award	COR, PM
25	TBD at Contract Award	Source code in editable electronic format for all applications developed to integrate pre- existing applications into the HART and all stand-alone applications developed to fulfill requirements not addressed by pre-existing software	TBD at Contract Award	COR, PM
26	TBD at Contract Award	Executable modules for those applications developed using compiled development languages or executable load module generating tools	TBD at Contract Award	COR, PM
27	TBD at Contract Award	Software repository holding the developed HART application code	TBD at Contract Award	COR, PM
28	TBD at Contract Award	Configuration parameters and configuration data stores or files for each COTS, GOTS, or open-source application	TBD at Contract Award	COR, PM
29	TBD at Contract Award	IDENT to HART User Migration Plan	TBD at Contract Award	COR, PM
30	TBD at Contract Award	IDENT to HART Data Store Migration and Conversion Plan	TBD at Contract Award	COR, PM
31	TBD at Contract Award	All files and data stores holding the data used by the software tools used to design and document the HART system	TBD at Contract Award	COR, PM
32	TBD at Contract Award	HART biometric matcher interface specification	TBD at Contract Award	COR, PM
33	TBD at Contract Award	Test Plans for conducting each level of testing specified in the TEMP	TBD at Contract Award	COR, PM
34	TBD at Contract Award	Developmental Test Plan	TBD at Contract Award	COR, PM
35	TBD at Contract Award	Test cases for each level of testing specified in the TEMP	TBD at Contract Award	COR, PM
36	TBD at Contract Award	Test procedures for each test to be conducted	TBD at Contract Award	COR, PM
37	TBD at Contract Award	Test problem reports generated during each test	TBD at Contract Award	COR, PM
38	TBD at Contract Award	Regression test suites for use during testing	TBD at Contract Award	COR, PM

#	Format	Title	Due Date	Submit to:
39	TBD at Contract Award	Summary reports summarizing each phase of testing	TBD at Contract Award	COR, PM
40	TBD at Contract Award	Procedures for system installation and configuration	TBD at Contract Award	COR, PM
41	TBD at Contract Award	Procedures for system operation	TBD at Contract Award	COR, PM
42	TBD at Contract Award	Procedures for system application maintenance and enhancement	TBD at Contract Award	COR, PM
43	TBD at Contract Award	Procedures for help desk personnel providing telephone support for the system	TBD at Contract Award	COR, PM
44	TBD at Contract Award	Security Authorization Process and Security Accreditation documentation as required by the *DHS Security Authorization Process Guide* Version 11.1 including	TBD at Contract Award	COR, PM
45	TBD at Contract Award	- Security Plan	TBD at Contract Award	COR, PM
46	TBD at Contract Award	- Contingency Plan	TBD at Contract Award	COR, PM
47	TBD at Contract Award	- Contingency Plan Test Results	TBD at Contract Award	COR, PM
48	TBD at Contract Award	- Configuration Management Plan	TBD at Contract Award	COR, PM
49	TBD at Contract Award	- Security Assessment Plan	TBD at Contract Award	COR, PM
50	TBD at Contract Award	- Security Assessment Report	TBD at Contract Award	COR, PM
51	TBD at Contract Award	- Authorization to Operate Letter	TBD at Contract Award	COR, PM
52	TBD at Contract Award	- Plan(s) of Action and Milestones	TBD at Contract Award	COR, PM
53	TBD at Contract Award	- Interconnection Security Agreement(s)	TBD at Contract Award	COR, PM
54	TBD at Contract Award	Training documentation, manuals, and training presentations.	TBD at Contract Award	COR, PM
55	TBD at Contract Award	Training documentation, manuals, and training presentations.	TBD at Contract Award	COR, PM
56	TBD at Contract Award	Classroom training, as specified	TBD at Contract Award	COR, PM
57	TBD at Contract Award	Self-service training, as specified	TBD at Contract Award	COR, PM
58	MS Project	Project schedules	TBD at Contract Award	COR, PM

#	Format	Title	Due Date	Submit to:
59	TBD at Contract Award	Automated Biometric Identification System (IDENT) Exchange Messages (IXM) Specification, Version 6.1	TBD at Contract Award	COR, PM
60	TBD at Contract Award	Automated Biometric Identification System (IDENT) Exchange Messages (IXM) Specification, Version 6.2	TBD at Contract Award	COR, PM
61	TBD at Contract Award	Technical progress reports	TBD at Contract Award	COR, PM
62	TBD at Contract Award	Financial progress reports	TBD at Contract Award	COR, PM
63	TBD at Contract Award	Task order status reports	As directed by Gov't	COR, PM
64	TBD at Contract Award	Transition Out Plan	As directed by Gov't	COR, PM
65	TBD at Contract Award	Transition Out Training	As directed by Gov't	COR, PM
66	TBD at Contract Award	Deployment and site preparation plans for each test and production system installation	TBD at Contract Award	COR, PM
67	TBD at Contract Award	SELC review presentations and required artifacts for each SELC gate review required by the final HART SELC Tailoring Plan	TBD at Contract Award	COR, PM
68	TBD at Contract Award	Operations manuals	TBD at Contract Award	COR, PM
69	TBD at Contract Award	User manuals	TBD at Contract Award	COR, PM
70	TBD at Contract Award	Maintenance manuals	TBD at Contract Award	COR, PM
71	TBD at Contract Award	As-Built designs of each test and production installation	TBD at Contract Award	COR, PM
72	TBD at Contract Award	Business continuity plans and updates	TBD at Contract Award	COR, PM
73	TBD at Contract Award	Disaster recovery plans and updates	TBD at Contract Award	COR, PM
74	TBD at Contract Award	Technology insertion packages for hardware or software to be added to the DHS Technical Reference Model (TRM)	TBD at Contract Award	COR, PM
75	TBD at Contract Award	End of contract Transition-Out Plan	TBD at Contract Award	COR, PM

#	Format	Title	Due Date	Submit to:
76	TBD at Contract Award	End of Contract transition schedule	TBD at Contract Award	COR, PM
77	TBD at Contract Award	Monthly Asset Report	10th business day of each month	COR, PM
78	TBD at Contract Award	Annual Inventory Report	12 months after award date	COR, PM

8 Guidelines, Constraints, and Performance Targets

The following are guidelines to be considered and constraints to be observed in responding to this solicitation.

8.1 Guidelines

The HART Contractor should be guided by the following when responding to and performing the work specified in this document.

Hosting Environments. HART production and test system components including data storage, data warehousing, fingerprint matching, and latent print management subsystems may be hosted in any one or combination of several different environments. Preference should be given to environments and infrastructure solutions that allow maximum flexibility, ease and speed of deployment, and on-demand scalability. All HART hosting environments shall be Federal Risk and Authorization Management Program (FedRAMP) and Federal Information Security Management Act (FISMA) compliant, as appropriate. The potential hosting environment include:

- Cloud-based environments providing infrastructure services for HART;
- Non-DHS data center environments, which may be either Government-owned or commercial data center environments, hosting OBIM-owned HART infrastructure components;
- DHS Enterprise Data Center environments; and
- Hybrid environments hosting HART components in any combination of the above types of environments.

IDENT Reuse. The proposed HART architecture may retain, re-use, repurpose, or dispose of any hardware or software components currently present in the IDENT system. Reuse of existing IDENT components is encouraged where practicable and financially advantageous, but not required. However, OBIM requires the redesign and replacement, not the reuse, of the existing Transaction Manager application. Any proposed component reuse shall not affect the availability of the IDENT system, the integrity of IDENT data, or degrade IDENT system performance in any way. The HART Contractor shall take no action during the development and deployment of HART that affects IDENT performance or availability until such time as all customer service request processing has been successfully transitioned from IDENT to HART.

Licenses and maintenance. The Government will not provide licenses or maintenance for software applications necessary to implement HART or for hardware that the Offeror acquires for HART. For existing IDENT components that the Offeror chooses to incorporate into HART rather than replace, the Government will continue to provide the hardware maintenance for the incorporated system.

Off-the-Shelf Software. OBIM prefers system design proposals for HART that incorporate loosely coupled, off-the-shelf or non-developmental software applications for performing the majority of key system functions. These applications may be COTS, GOTS, or open-source. Functions that may be candidates for performance by off-the-shelf products include but are not limited to: messaging, workflow management, business rules management, business rules

execution, transaction volume management, transaction priority management, biometric matching, multimodal biometric matching and fusion, biographic matching, data store and file access, system monitoring, and security access control, authentication, and authorization. HART design should deliver major portions of its functionality through those COTS, GOTS, or open-source products integrated into the system. If significant customization would be required to COTS or GOTS solutions, purpose-built functionality on open-source frameworks can be considered.

The Government envisions the delivered solution to be a framework of loosely-coupled off-the-shelf components augmented by custom-developed components to assure system adaptability and flexibility.

Off-the-Shelf Application Utilization. OBIM prefers that HART utilize a majority of the functionality of those off-the-shelf applications incorporated into the HART solution. If significant customization would be required to COTS or GOTS solutions, purpose-built functionality on open-source frameworks can be considered.

Functionality as Services. HART should implement a substantial portion of the functionality it delivers as callable services through the integration of COTS, GOTS, or open-source products. Services provided by individual products should be available for orchestration with services from other products and with those provided by any custom-developed applications to fulfill HART functional processing requirements.

Data Management Systems. OBIM currently employs the Oracle relational database for managing IDENT data. Where the need for a data management system arises in HART, OBIM requires that the data management solution proposed support continuous availability and scalability both vertically and horizontally – that is scaling of the capacity of the storage hardware and the ability to expand the overall capacity of data under management by implementing additional, potentially heterogeneous, storage devices under management by the data management solution.

Operations and Maintenance Cost Minimization. The Government has an objective to minimize O&M costs for the HART system. The Government encourages system proposals that offer opportunities to control and reduce continuing O&M costs.

8.2 Mandatory Constraints and Restrictions

The following constraints and restrictions shall be observed in designing HART system solution.

Standards Compliance. HART shall comply with all applicable DHS, NIST, and Federal Standards.

Change Management. HART shall be subject to and comply with all DHS and OBIM change management policies and procedures.

Section 508 Compliance. All components of HART shall comply with Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220). Section 508 requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities.

Design Deliverables File Formats. The Contractor shall provide all deliverables in the native electronic format of the software tool used to develop that deliverable. In addition to any other specification of formats for system design, architectural drawing, network diagram, schematics, and any other technical design deliverables, the HART Contractor shall deliver those artifacts in the electronic file format produced by the design tool or tools used to develop those deliverables. Hardcopy and portable document formats alone are unacceptable. Electronic deliverables shall be unlocked and modifiable so that OBIM can update and maintain those design-related artifacts as the system evolves over time. The Contractor shall also deliver five (5) licenses for each application used to generate those HART system design artifacts.

Documentation Delivery. The Contractor shall place all documentation products to be delivered to the Government under configuration control and shall maintain currency of each document. All documents, both electronic and hardcopy, shall be current and up-to-date at time of delivery.

Electronic Biometric Transmission Specification Compatibility (EBTS). HART shall support the current interoperability with the FBI NGI system which includes generating outbound transmissions of EBTS messages to NGI. HART shall provide EBTS support as follows:

- HART shall be able to initiate outbound queries of NGI in EBTS format and receive the resulting responses from NGI in EBTS format.
- HART shall only accept inbound EBTS messages for automated Latent print search requests.

IDENT Exchange Message (IXM) Version Support. IXM 6.0.9 is the current version at the time of this procurement. Versions 6.0.4 and 6.0.7 are in use by OBIM customers. IXM version 6.0.9 implements a 1:N face matching capability to IXM along with other minor updates. HART Increments 1 and 2 shall support IXM 6.0.4, 6.0.7, 6.0.8, and 6.0.9, which are backward compatible with each other. IXM 6.0.x data elements are based on NIEM attributes. Future versions of IXM should continue to be based on NIEM constructs where applicable.

Hardware Installation. Installation of HART infrastructure hardware in the DHS Enterprise Data Centers, whether for test or production environments, shall be handled by the DHS Data Center Support contractors. The HART Contractor shall be responsible for ensuring that the installation of HART infrastructure in any hosting environment other that the DHS Enterprise Data Centers occurs in a technically correct and timely manner.

Operations and Maintenance. In DHS Enterprise Data Centers, Level 1 operations and maintenance support for HART components will be performed by the DHS Enterprise Data Center Support contractors. This contractor will provide the data center operating environment, hardware maintenance, operating system and utility infrastructure software maintenance. This support will commence when equipment is delivered to the Enterprise Data Centers for installation. Level 2 and Level 3 support will be provided by the HART Contractor. For any cloud-based system components or components hosted in a non-DHS data center, the HART Contractor is responsible ensuring that the equivalent of Level 1, Level 3, and Level 3 support is provided for those components.

Government Ownership. Government ownership rights shall in accordance with the relevant clauses in Part 4 of the RFP.

Data Ownership. All data loaded into test environments for purposes of testing the HART system during development shall be the property of the government. All data loaded into the production HART system implementations at the DHS Enterprise Data Centers or other locations shall be the property of the government. All intermediate versions of data created as part of conversion efforts from IDENT data formats and storage organization to HART data formats and storage shall be the property of the Government. When no longer needed for their original purpose, any intermediate data versions that have been created shall, at the Government's direction, either be returned to the Government or destroyed.

Multiple Biometric Modalities and Matching Technologies. HART shall be designed to accommodate multiple biometric modalities, multiple biometric matching technologies for each modality, incorporation of additional biometric matching technologies for each modality, and removal or retirement of biometric matching technologies.

Remote Access. Contractor access to any HART test environments installed in DHS Enterprise Data Centers shall be remote. The Contractor shall use only approved mechanisms to access HART test environments. Any development or other work done in HART test environments installed in the DHS Enterprise Data Centers shall be done remotely from the Contractor's own facilities.

Development Languages. For new systems development (i.e. coding) undertaken for HART, the Contractor shall design and produce the software using one of the following languages: Java, C#, JavaScript, Python, Ruby, or Go. Contractor shall request approval from the Contracting Officer prior to use of any other language for coding.

Legacy Interface Compatibility. HART shall support the legacy interfaces in place with OBIM's customers and their systems. HART shall support all legacy communications mechanisms employed to communicate between OBIM and its customers.

Information Assurance. Information Assurance (IA) shall be considered a requirement for all systems used to input, process, store, display, or transmit sensitive or national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated COTS IA and IA-enabled IT products. These products shall provide for the availability of systems. The products also shall ensure the integrity and confidentiality of information and the authentication and nonrepudiation of parties in electronic transactions.

Technical Reference Model (TRM) Compliance. All products, both hardware and software, integrated into HART shall either reside in the TRM or be capable of qualifying for addition to the TRM. The Contractor shall identify any products included in the HART system solution that are not currently on the TRM and shall coordinate with OBIM to follow the DHS Technology Insertion protocol to secure approval for those products and their addition to the TRM.

9 Applicable Documents

9.1 Compliance Documents

The following documents provide specifications, standards, and guidelines with which compliance is required in order to meet the requirements of this contract. The HART system shall comply with the following:

- American National Standards Institute (ANSI)/NIST Information Technology Laboratory (ITL) (ANSI/NIST-ITL) 1-2011 Update 2013, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information Part 1*.
- ANSI/NIST-ITL 2-2008, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information Part 2: XML Version, August 2008*.
- ISO/IEC JTC 1/SC 37, *Biometric Data Format and Related Standards.*
- FIPS Publication 199, *Standards for Security Categorization of Federal Information Processing Systems*, February 2004.
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
- NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.
- DHS Sensitive Systems Policy Directive 4300A, Version 12.01, February 2016.
- DHS Security Authorization Process Guide Version 11.1 March 16, 2015.
- DHS Homeland Security Enterprise Architecture Interoperability Standards.
- DHS Guidebook 102-01-103-01, Systems Engineering Life Cycle Guidebook, April 2016.
- DHS Privacy Policy Guidance Memorandum 2011-02: Roles & Responsibilities for Shared IT Services, June 30, 2011.
- U.S. Government Accountability Office Schedule Assessment Guide, GAO-16-89G, December 22, 2015.
- OBIM Change Management Handbook Version 2.3
- DHS Infrastructure Change Control Board (ICCB) Process Handbook Version 14.0, October 26,2015
- OBIM Data Modeling Methodology Standards, January 14, 2016 (for all relational data models)
- HART Biometric System Operational Requirements Document (ORD), Version 1.0, November 16, 2015.

9.2 Reference Documents

The following documents will provide necessary information for the Contractor in performing the work described in this document:

- Replacement Biometric System Concept of Operations (CONOPS), Version 1.0, June 24, 2015.

- HART System Test and Evaluation Master Plan (TEMP). Version 1.0, November 30, 2014.
- Replacement Biometric System Mission Needs Statement (MNS). Version 1.0, December 14, 2014
- HART Systems Engineering Lifecycle (SELC) Tailoring Plan, December 9, 2015.
- Department of Justice Electronic Biometric Transmission Specification Version 10.0.5, June 13, 2013; https://www.fbispect.cjis.gov/ebts/Approved.
- Automated Biometric Identification System (IDENT) Exchange Messages (IXM) Specification, Version 6.0.7.
- Automated Biometric Identification System (IDENT) Exchange Messages (IXM) Specification, Version 6.0.
- Automated Biometric Identification System (IDENT) Exchange Messages (IXM) Specification, Version 5.0.
- Federal Bureau of Investigation Electronic Biometric Transmission Specification, https://www.fbibiospecs.org/, Version 10.0.2 Final, June 2014.
- DHS Information Security Performance Plan.
- DHS Management Directive 140-01, Information Technology System Security, July 31, 2007.
- Instruction Manual 102-01-004-01, DHS Agile Development and Delivery for Information Technology Guidebook.
- Enterprise Data Management – Data Modeling Methodology Guidelines, November 10, 2009.
- Federal Enterprise Architecture Business Reference Model (BRM) Version 3.1, May 2013, under the Border and Transportation Security BRM Service.
- Handbook for Safeguarding Sensitive Personally Identifiable Information, March 2012.
- DHS/NPPD-004 – DHS Automated Biometric Identification System (IDENT) SORN June 5, 2007, 72 FR 31080.
- DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) Privacy Impact Assessment, December,7, 2012.
- National Information Exchange Model (NIEM) Version 3.2, June 2016.
- National Institute of Standards and Technology (NIST) Fingerprint Image Quality 2.0.
- National Institute of Standards and Technology (NIST) SP 500-290 Version 2 (2013), *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information.*
- US-VISIT Configuration Management Plan.
- HART Data Management Plan.
- HART Information Technology (IT) Configuration Plan.
- DHS/NPPD-004 – DHS Automated Biometric Identification System (IDENT) System of Records Notification (SORN). https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system.

- DHS/NPPD/PIA-002 Automated Biometric Identification System Privacy Impact Assessment, https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system.
- HART Risk Management Plan.
- HART Quality Assurance Plan.
- HART Training Plan.
- Architecture Guide, Release 5.4 Volume 2: Current Architecture, June 28, 2015.
- US-VISIT Automated Biometric Identification System C++ Coding Standards, April 4, 2006.
- US-VISIT Automated Biometric Identification System JAVA Coding Standards, July 27, 2006.
- OBIM Data Quality Guidance, January 14, 2016

Appendix A HART Performance Requirements

HART shall meet the performance requirements established in the *HART Operational Requirements Document (ORD).* Table 4 in this appendix lists the performance requirements to be met by HART. Measures of Performance (MOPs) in Table 4 originate in the HART ORD Table 9, Measures of Performance. Key Performance Parameters (KPPs) in Table 4 are sourced from ORD Table 25, OBIM Key Performance Parameters.

The "Threshold" column in Table 4 indicates the minimum performance requirement for each performance measure. The "Objective" column indicates the desired performance objective. The "Source" column lists the origin of each performance measure and whether that measure is a KPP or MOP. KPPs are more general performance requirements; MOPs are more specific requirements.

Table 4. HART Performance Requirements

Performance Measure	Threshold	Objective	Source
Availability. HART shall provide the availability of:	≥ 99.7%	≥ 99.95%	ORD KPP** #1
Biometric Identification Service. HART shall provide a fingerprint biometric identification service that meets approved customer service level agreements (SLAs) for an aggregated percentage of customer requests:	≥ 95%	≥ 99%	ORD KPP #2
*Multimodal Biometric Search Response time.** For DHS customers for law enforcement purposes, HART shall provide a percentage of multimodal full gallery searches completed within 2 minutes or fewer for any given hour of the day:	≥ 95%	≥ 99%	ORD KPP #3
Multimodal Biometric Verification Service. HART shall provide a multimodal biometric verification service that meets approved customer SLAs for an aggregated percentage of customer requests:	≥ 95%	≥ 99%	ORD KPP #4
Multimodal Biometric Verification Accuracy. HART shall provide an average Travelers Inconvenienced Due to False-Positive Matches multimodal rate of:	≤ 0.02%	≤ 0.01%	ORD KPP #5

Performance Measure	Threshold	Objective	Source
Interoperability. HART shall provide an average response time to process full gallery multimodal biometric search requests received from DOJ's NGI for criminal and civil fingerprint submissions:	≤ 15 minutes	≤ 10 minutes	ORD KPP #6
Availability: HART shall have an overall availability threshold of 99.70% with an objective of 99.95%, which includes both scheduled and unscheduled downtime.	≥ 99.7%	≥ 99.95%	ORD MOP***#1
Mean Time Between Failures. HART shall have a Mean Time between Failures (MTBF) for the overall system at a threshold greater than or equal to 50 days with an objective greater than or equal to 365 days.	≥ 50 days	≥ 365 days	ORD MOP-2
Mean Time to Repair. HART shall have a Mean Time to Repair (MTTR) for the overall system at a threshold less than or equal to 3.6 hours with an objective less than or equal to 3.6 hours.	≤ 3.6 Hours	≤ 3.6 hours	ORD MOP-3
BioVisa Response. HART shall have a search and response time for DOS BioVisa of less than or equal to 15 minutes with a threshold of greater than or equal to 95% of all requests, and an objective of greater than or equal to 98% of all requests.	≥ 95%	≥ 98%	ORD MOP-4
Customs and Border Protection (CBP) Port of Entry (POE) Response. HART shall have a full-gallery search and response time for CBP POE at Primary Inspection of less than or equal to 10 seconds with a threshold of greater than or equal to 95% of all requests and an objective of greater than or equal to 98% of all fingerprint requests.	≥ 95%	≥ 98%	ORD MOP-5

Performance Measure	Threshold	Objective	Source
Law Enforcement Response. HART shall have a search and response time for DHS customers for law enforcement purposes [United States Coast Guard, CBP / Border Patrol and Office of Field Operations (OFO), and Immigration and Customs Enforcement (ICE)] of less than or equal to 2 minutes with a threshold of greater than or equal to 95% of all requests and an objective of greater than or equal to 98% of all fingerprint requests.	≥ 95%	≥ 98%	ORD MOP-6
Department of Justice (DOJ) Response. HART shall have a search and response time for DOJ of less than or equal to 15 minutes with a threshold of greater than or equal to 95% of all requests and an objective of greater than or equal to 98% of all fingerprint requests.	≥ 95%	≥ 98%	ORD MOP-7a
Federal Emergency Management Administration (FEMA) Response. HART shall have a search and response time for FEMA of less than or equal to 24 hours with a threshold of greater than or equal to 95% of all requests and an objective of greater than or equal to 98% of all requests.	≥ 95%	≥ 98%	ORD MOP-7b
Transportation Security Administration (TSA) Response. HART shall have a search and response time for TSA of less than or equal to 24 hours with a threshold of greater than or equal to 95% of all requests and an objective of greater than or equal to 98% of all requests.	≥ 95%	≥ 98%	ORD MOP-7c
United States Citizenship and Immigration Services (USCIS) Field Office Successful Verification Response. HART shall have a verification and response time for USCIS field office verifications of less than 10 seconds for successful verifications with a threshold of greater than or equal to 95% of all requests and an objective of greater than or equal to 98% of all requests.	≥ 95%	≥ 98%	ORD MOP-7d

Performance Measure	Threshold	Objective	Source
USCIS Verification Mismatch Full Gallery Response. HART shall have a verification and response time for USCIS field office verifications of less than or equal to 10 minutes, for mismatches with Biometric Support Center (BSC) review with full gallery search and response, with a threshold of greater than or equal to 95% of all requests and an objective of greater than or equal to 98% of all requests.	≥ 95%	≥ 98%	ORD MOP-7e
USCIS Enrollment Search and Response. HART shall have a search and response time for USCIS application support center enrollments of less than or equal to 24 hours with a threshold of greater than or equal to 95% of all requests and an objective of greater than or equal to 98% of all requests.	≥ 95%	≥ 98%	ORD MOP-7f
CBP Biometric Exit Response. HART shall have a response time for CBP Biometric Exit Verification (1:1 requests) of less than or equal to 3 seconds with a threshold of greater than or equal to 95% of all requests and an objective of greater than or equal to 98% of all requests.	≥ 95%	≥ 98%	ORD MOP-7g
Fingerprint Verification Accuracy. HART shall support a threshold and objective of greater than or equal to 99.5% Target or True Acceptance Rate (TAR) at less than or equal to 0.008% False Acceptance Rate (FAR) for fingerprint verification accuracy (1:1 comparisons).	TAR ≥ 99.5% at FAR ≤ .008%	TAR ≥ 99.5% at FAR ≤ .008%	ORD MOP-8
Biometric Transactions Referred to BSC. HART shall support a less than or equal to 0.6% threshold and less than or equal to 0.5% objective for biometric Identification (1:N) transactions sent to BSC (“gray-area hit”) for fingerprint evaluation.	≤ 0.6%	≤ 0.5%	ORD-MOP 9

Performance Measure	Threshold	Objective	Source
Simultaneous Biometric Modalities Matched. HART shall support a threshold of two and an objective of three simultaneously matched biometric modalities during multimodal fusion.	2	3	ORD-MOP 10
Fingerprint Identification Accuracy. HART shall support a threshold and objective of greater than or equal to 99.5% TAR at less than or equal to 0.008% FAR for fingerprint identification accuracy (1:N comparisons) of match subsystem.	TAR ≥ 99.5% at FAR ≤ .008%	TAR ≥ 99.5% at FAR ≤ .008%	ORD MOP-11
Face Verification Accuracy. HART shall support a threshold and objective of greater than or equal to 95% TAR at less than or equal to 0.1% FAR for face verification accuracy (1:1 comparisons) of match subsystem. This requirement applies to identities and/or face images that OBIM determines to be of sufficient quality for matching. OBIM will consider input and analysis from the vendor when determining what is to be measured as matchable.	TAR ≥ 95.0% and FAR ≤ .010%	TAR ≥ 95.0% and FAR ≤ .010%	ORD MOP -12
Iris Identification Accuracy. HART shall support a threshold and objective of greater than or equal to 98% TAR at less than or equal to 0.0080% FAR for iris (dual) identification accuracy (one-to-many comparisons) of match subsystem.	TAR ≥ 98% and FAR ≤ .0080%	TAR ≥ 98% and FAR ≤ .0080%	ORD MOP-13
Iris Verification Accuracy. HART shall support a threshold and objective of greater than or equal to 98% TAR at less than or equal to 0.01% FAR for iris (dual) identification accuracy (one-to-many comparisons) of match subsystem.	TAR ≥ 98.0% and FAR ≤ .010%	TAR ≥ 98.0% and FAR ≤ .010%	Planned Addition to ORD

Performance Measure	Threshold	Objective	Source
Fusion Accuracy. HART shall support a threshold and objective of greater than or equal to 99.9% TAR at less than or equal to 0.008% FAR for fusion accuracy of match subsystem.[1]	TAR ≥ 99.9% and FAR ≤ .008%	TAR ≥ 99.9% and FAR ≤ .008%	ORD MOP-15

* Response times are measured from the time OBIM systems receive an in-bound request to the time OBIM systems make an out-bound response available to the requesting system.

** Key Performance Parameter (KPP) – *HART Operational Requirements Document (ORD)*, Table 25, Key Performance Parameters.

*** Measures of Performance (MOP) – *HART Operational Requirements Document (ORD)*, Table 9, Measures of Performance.

[1] OBIM expects fusion to improve overall system biometric matching accuracy to meet the stated threshold, encompassing both identification and verification matching scenarios.

Appendix B HART Sizing Information

This appendix contains selected extracts from information sources present in the HART Reading Room that potential growth in the number of identities, encounters, and transactions that HART must address. It also contains the current matching and storage capacity utilization report for the existing IDENT system.

Table 5 shows the anticipated growth in overall OBIM sizing parameters for three years beyond the implementation of HART Increment 1 assuming a January 2017 start to HART development and completion of Increment 1 in July of 2018 (18 months).

Table 5. Projected Growth: Three Years Beyond Increment 1 Completion (July 2018 – July 2021)

Scalability Factors	Volume at End of Increment 1 - July 2018 (in Millions)	Volume 3 Years After Increment 1 (July 2021) (in Millions)
Unique Identities[2]. Growth in the cumulative number of unique identities stored in OBIM databases.	225	261
Encounters[3]. Growth in the number of cumulative encounters recorded in OBIM databases.	893	1,196
Biometric Images[4]. Growth in the aggregate number of biometric images stored in OBIM databases (Fingerprint, Iris, and Face combined).	3,703	4,891
Transaction Growth[5]. Growth in the total number of transactions processed shall accommodate the daily transaction growth over time while still satisfying the response times and SLA requirements.	1.099	1.414

[2] IDENT _UniqueEncounters_TrendAnalysis.xlsx, IDENT Encounters Tab, HART Reading Room EXCEL Workbook

[3] Ibid.

[4] IDENT _UniqueEncounters_TrendAnalysis.xlsx, Images Historical Tab, HART Reading Room EXCEL Workbook

[5] Daily Revised Transaction Forecast – Reading Room EXCEL Workbook – Generated December 12, 2016

Table 6 shows the projected cumulative number of enrollments expected in OBIM's biometric matching galleries for fingerprint, iris, and face images. The projections in Table 6 are anticipated year end totals. Fingerprint biometrics include 10-print and 2-print sets; iris biometrics are iris pairs.

Table 6. Projected Matching Gallery Cumulative Enrollments

Projected Gallery Enrollments (in Millions)			
Year	Fingerprint[6]	Face	Iris (Pairs)
2016	201.4	0	0.3
2017	214.9	300	5.5
2018	228.5	500	6.1
2019	242.0	700	7.6
2020	255.6	1,000	9.1
2021	269.1	1,300	10.6
2022	282.6	1,600	12.0

Table 7 shows the estimated number of Iris and Face Identification transactions projected for 7 years. Both daily and annual estimates are shown.

Table 7. Iris and Face Identification Transaction Projections

Projected Iris and Face Identification (1:N) Transactions (in Thousands)				
Year	**Face Daily**	**Iris Daily**	**Face Annual**	**Iris Annual**
2017	50.2	9.7	18,323	3,538
2018	69.2	11.7	25,259	4,283
2019	92.7	16.8	33,844	6,142
2020	96.3	31.7	35,145	11,555
2021	100.0	44.6	36,499	16,272
2022	103.9	58.5	37,906	21,359

Table 8 shows the estimated number of Iris and face Verification transaction projected for 6 years. Both daily and annual estimates are shown.

[6] IDENT_UniqueEncounters_TrendAnalysis.xlsx, IDENT Encounters Tab, HART Reading Room EXCEL Workbook

Table 8. Iris and Face Verification Transaction Projections

Projected Iris and Face Verification (1:1) Transactions (in Thousands)				
Year	**Face Daily**	**Iris Daily**	**Face Annual**	**Iris Annual**
2017	8.2	0.9	2,993	329
2018	26.5	1.9	9,673	694
2019	44.5	4.9	16,243	1,789
2020	77.0	5.1	28,105	1,862
2021	90.0	5.5	32,850	1,935
2022	100.0	58.5	36,500	2,008

Tables 9 and 10 show projected Daily and Annual transaction rates respectively for four types of fingerprint processing transactions: Identify, Verify, Pre-Verify, and Retrieve Identity.

Table 9. Daily Transaction Rates – Current and Projected - Fingerprint[7]

Daily Transaction Rates – Current and Projected				
Transaction Type:	**Identify**	**Verify**	**Pre-Verify**	**Retrieve Identity**
Current Transaction Rates (in Thousands)				
Average Per Day	133.9	136.8	637.82	75.3
Peak Hour	5.6	12.2	36.1	4.3
Projected Transaction Rates per Day (in Thousands)				
2017	144.0	148.5	637.9	78.4
2018	155.0	161.2	698.9	81.6
2019	166.9	175.0	765.8	84.9
2020	179.9	190.0	839.1	88.4
2021	194.0	206.5	919.4	92.0

[7] Daily_Revised_Transaction Forecast - Reading Room EXCEL Workbook – Generated December 12, 2016

Table 10. Projected Annual Transaction Rates - Fingerprint[8]

Projected Annual Transaction Rates (in Millions)				
Transaction Type:	**Identify**	**Verify**	**Pre-Verify**	**Retrieve Identity**
2017	52.6	54.2	232.8	28.6
2018	56.6	58.8	255.1	29.8
2019	60.9	63.9	279.5	31.0
2020	65.7	69.4	306.3	32.3
2021	70.8	75.4	335.6	33.6

Tables 11 and 12 contain the Weekly IDENT Capacity Management report for September 30, 2016 for organic matcher gallery growth and storage, respectively.

[8] Ibid.

Table 11. Weekly IDENT Capacity Report – September 30, 2016 – Gallery Organic Growth

	Forecasted Organic Growth - 09/30/2016									
	Matcher Gallery									
	10-PRINT				2-PRINT		LATENT			
	IDENT 10P WL (10P) - Elite V	IDENT 10P WL (2P/4P) - Elite V Lite	IDENT 10P VST (10P) - Elite V	IDENT 10P VST (2P/4P) - Elite V Lite	IDENT 2P VF - Elite IV	IDENT 2P VM - Elite IV	Latent 10P WL - Elite II	Latent 10P VST - Elite II	Latent 2P VF & VM - Elite II	Unresolved Latent - Elite II
Total PMA Capacity	40,000,000	10,000,000	200,000,000	10,000,000	32,000,000	32,000,000	40,000,000	200,000,000	50,000,000	1,000,000
PMA Capacity Used	9,339,105	1,517,971	158,851,211	95,368	17,993,291	18,338,577	14,404,217	158,946,579	36,331,868	273,686
PMA Capacity Used (%)	23.3%	15.2%	79.4%	1.0%	56.2%	57.3%	36.0%	79.5%	72.7%	27.4%
Expected Date for 95% PMA Capacity Threshold	> 5 Years	N/A	Aug-2018	N/A	> 5 Years	> 5 Years	> 5 Years	Aug-2018	> 5 Years	> 5 Years
Expected Date for 100% PMA Capacity Depletion	> 5 Years	N/A	Apr-2019	N/A	> 5 Years	> 5 Years	> 5 Years	Apr-2019	> 5 Years	> 5 Years
Throughput < 95th Percentile Peak Hour Workload	Jun-2019		Oct-2018		> 5 Years	> 5 Years	N/A			
Throughput < Avg. Peak Hour Workload	Aug-2021		Feb-2021		> 5 Years	> 5 Years	N/A			

Table 12. Weekly IDENT Capacity Report – September 30, 2016 - Storage

Storage – 09/30/2016										
	DC1 (Primary)						DC2 (Backup)			
		IDENT IMAGEDG	IDENT DATADG	ESB	Matcher			IDENT IMAGEDG	IDENT DATADG	Matcher
Current Storage Capacity Used		88.1%	79.9%	18.7%	55.7%	Current Storage Capacity Used		88.1%	79.9%	77.9%
Total (TB)		675.0	71.9	22.0	80.8	Total (TB)		675.0	71.9	59.9
Free (TB)		80.3	14.4	17.9	35.8	Free(TB)		80.3	14.4	13.3
Used (TB)		594.7	57.5	4.1	45.1	Used (TB)		594.7	57.5	46.7
Expected Date for 80% Capacity Threshold		Jul-16	Oct-16	Sep-23	Jan-20	Expected Date for 80% Capacity Threshold		Jul-16	Oct-16	Dec-16
Expected Date for 100% Capacity Depletion		Sep-17	Aug-19	Sep-23	Sep-22	Expected Date for 100% Capacity Depletion		Sep-17	Aug-19	Dec-18

Table 13 contains sizing metrics for the Secondary Inspection Tool (SIT). SIT is a Java application. These metrics were generated using the Serena Dimensions source code management tool.

Table 13. Secondary Inspection Tool Lines of Java Code Analysis[9]

Symbol	Quantitative Measure	Description
Files and directories		
Source Files	338	Source Files
Directories	97	Directories
Source Lines of Code		
BLOC	13,529	Blank Source Lines of Code
SLOC-P	46,535	Physical Executable Source Lines of Java Code
CLOC	23,388	Comment Only Source Lines of Code
TOTAL	83,452	Total Source Lines of Code
Additional Descriptive Metrics		
SLOC-L	32,316	Logical Executable Lines of Code
MVG	5,396	McCabe Cyclometric Complexity
C&CLOC	604	Code and Comment Lines of Code
CWORD	124,150	Commentary Words
HCLOC	541	Header Comment Lines of Code
HCWORD	2,196	Header Commentary Words

[9] Analysis generated using Serena Dimensions, November 18, 2016

Appendix C Definitions

1:N Match. A 1:N (one-to all) biometric match is a search of all individual biometrics stored in the full biometric repository, for example, a search of all fingerprints on file, seeking a match to the to the submitted biometric modalities.

1:1 Match. A 1:1 (one-to-one) match is a biometric identity verification search matching attempting to match modalities submitted with a biometric verification request to a single identity record retrieved from the biometric repository by a document-based or unique identifier-based search.

Biometric Support Center (BSC). The Biometric Support Center (BSC) has two locations – one in the Washington DC metropolitan area and the other in the San Diego area – currently staffed by expert fingerprint examiners. These examiners are supported by the 3M Cogent Automated Biometric Information System (CABIS) system for latent fingerprint management as well as custom-developed tools for use in fingerprint examination and accessing and updating the current IDENT system. The custom developed tools are the Candidate Verification Tool (CVT) and Secondary Inspection Tool (SIT). Examiners also have access to tools developed by other DHS components for access to the IDENT system and associated data.

Biometric Matching Subsystem. A biometric matching subsystem is a vendor-specific configuration of application servers, database servers, data storage, and software that enrolls biometric images in its gallery and conducts searches of that gallery to verify an identity or find an identity that matches a biometric.

Biometric Matching Subsystem Interface. This interface is a standard interface through which all biometric matching subsystems will connect to the HART core application. This interface will implement an application programming interface that will be the standard for interfacing biometric matching subsystems to the HART core application.

Customer. A customer is any government agency whether federal, state, domestic, or foreign, civilian, law enforcement, or military that accesses OBIM identity services, provides identity information to OBIM, or exchanges identity information with OBIM.

Enrollment. The process of adding an instance of a biometric modality (i.e. fingerprint set, iris pair, or facial image) to a biometric matching gallery and generating templates from incoming biometric modality images and loading those templates into the matching gallery.

False Acceptance Rate (FAR). A statistic used to measure biometric performance when performing verification tasks. FAR is expressed as a percentage and is a measure of the frequency with which the system produces a false acceptance which occurs when a submitted biometric sample is incorrectly matched to another individual's existing biometric.

Full Gallery Search. Multimodal Full Gallery Search. A full gallery search is a search of all biometric images enrolled in a single biometric gallery. A multimodal full gallery search is a search of the entire biometric gallery for each of the biometric

modalities submitted with a search request. For example, if an identification search request is submitted with both fingerprint and iris modalities, then a multimodal full gallery search would involve searching the entire fingerprint gallery and the entire iris gallery for a match.

Full Operating Capability (FOC). FOC is the point at which all of the functionality developed by a program has been successfully installed for production processing and is actively processing production workloads.

Fusion. "Fusion" is general term used to represent the techniques used to make a final determination of identity match when more than one modality has been submitted for identity verification through separate matching technologies, when more than one algorithm has been used to match an incoming modality, or when both conditions apply.

Gallery. A biometric matching subsystem's database, or set of known identities, for a specific modality (e.g. fingerprint, iris, or face).

Identification. An operation during which a biometric matching subsystem searches its database or gallery for a reference matching a submitted biometric modality sample and if found returns a corresponding identity.

Identity database. The term "identity database" is used to refer to all non-image identity data received and stored by OBIM systems.

Images. For the purposes of this SOO, the term "image" refers to any of the following: scanned fingerprint images, scanned iris images, scanned images of other biometric modalities, facial photographs, scanned facial photographs, other photographs, scanned images of biometric image hardcopies, scanned signature images, generic images of scanned documents, video recordings, and voice recordings.

Initial Operating Capability (IOC). IOC is a program milestone selected and defined by the program office that corresponds to that point on the schedule where all system capabilities included within the scope of program Increment 1 have been fielded to one or more locations and when those Increment 1 capabilities are processing the production workload for at least one (1) OBIM customer.

Latent Fingerprint. A fingerprint image, full or partial, left on a surface touched by an individual and submitted by a law enforcement agency.

Level 1 Operations & Maintenance Support – Basic Level Service. Basic Level Service (Level 1) is a hosting service that includes hardware maintenance and network monitoring for equipment. All services provided shall be consistent with the Uptime Institute's TIER III data center classification. The service includes monitoring system viability (also known as ping); monitoring all facilities services (known as power); and monitoring all network services (also known as pipe). The Contractor shall install equipment in the data center and bring it up to an operational state and provide limited O&M support. Basic Level Service provides basic facility services such as space, power, and security. It includes network connectivity from the servers to the wide area network (WAN) for all systems hosted in the environment. The Contractor shall provide

personnel, processes, and technology to support hosting services for DHS systems and applications. Level 1 service includes:

- Acquisition - The Contractor shall acquire server, software, storage, and General Support Systems (GSS) assets as required
- Installation - The Contractor shall install, configure, test and document the basic system including, but not limited to, racks, cabinets, servers, storage/backup, and network systems and shall coordinate all installation configurations.
- Hardware Maintenance – The Contractor shall maintain all contractor furnished equipment (CFE) and Government furnished equipment (GFE) to meet SLAs.
- Hardware/System Configuration - The Contractor shall configure the hardware systems based on DHS and OBIM (if it does not contradict DHS) - provided configuration guidelines, document and deliver updates to the as-built documentation to the HART Program Manager for incorporation into the system master baseline, and maintain configuration information resulting from maintenance or change implementations.
- Project Management - The Contractor shall provide project management support and logistics and oversight support including points of contact and project management for basic level services to support HART systems and services. The Contractor shall implement its production integration process for all workload migrations into the DHS Enterprise Data Centers.
- Accounting and Chargeback – The Contractor shall provide financial management services including but not limited to cost estimates, monthly and annual billing, and support for government auditing.
- Inventory Control – The Contractor shall maintain and update asset inventory information, perform physical audits, inventories, and inspections, provide inventory reports, provide audit reports, provide inventory management, ensure the configuration management database is accurate and in accord with SLAs, manage removal and replacement of defective parts under warranty, and manage the production software library.
- Incident Management – The Contractor shall monitor equipment from its operations center and in the event of an incident open a ticket for the designated service desk and perform touch labor tasks to assist remote staff in incident resolution.
- Decommissioning - The Contractor shall provide decommissioning services as requested. The Contractor shall start the decommissioning process after notification by the Government. The images, settings and data from the device shall be retained until the supported project is no longer in use or when there is written permission to delete/dispose of the data from the Government.

Level 2 Operations & Maintenance Support - Managed Level Service. Managed level service includes all Basic Level Services plus system administration, operations, database, and middleware services. The Contractor shall provide managed level service for both government-furnished and contractor-furnished systems. Level 2 service includes:

- Operating System Installation, Configuration, and Management - The Contractor shall install and configure platform operating system and utility programs.
- Patch Management - The Contractor shall maintain patch release services and provide patch management in order to maintain operational functionality of new releases, service, and compliance with the configuration management processes and procedures, including, but not limited to, patch application, patch testing, installation and deployment, configuration management database updates, and support and implementation of DHS Data Center Service Resource Management Process.
- Storage Management - The Contractor shall provide storage services and utility offerings. These offerings include the ability for the customer to receive management of /or consume storage in accordance with Task Orders. The Contractor shall install and configure all Storage Area Network (SAN) and Network Attached Storage (NAS), including any management software, and manage the allocation and retraction of storage in a dedicated and/or virtualized storage environment.
- Backup and Restore - The Contractor shall perform backup and restore services to include incremental backups daily and full backups weekly and manage backup scripts to backup critical operating system and system data files including all system batch processes. The Contractor shall restore operating systems according to the Component Disaster Recovery plan.
- Database Support - The Contractor shall provide database support services to manage, configure and maintain database servers for hosting and application support services.
- Middleware Support - The Contractor shall provide middleware support services to manage, configure and maintain middleware servers and software for hosting and application support services.
- Monitoring - The Contractor shall provide monitoring of hardware and Level 2 processes for availability, performance, and degradations.
- Services Normally Provided in a Managed Service Environment - The Contractor shall perform other tasks that it normally provides in a managed service environment. These tasks shall include services such as but not limited to the following:
    - o Mainframe operation and maintenance;
    - o Software license management for IBM and independent software vendor products and applications;
    - o Maintaining mainframe networks;
    - o Production batch job scheduling and production control;
    - o Server operation and maintenance;
    - o Software license management;
    - o Maintenance changes;
    - o Software installation;
    - o Performance reporting;
    - o Interfacing with application Contractor support as required for other included functions;

o Running and maintaining audit tools;
o Production Operations;
o Automation Services; and
o Tape handling, including rotation of backup tapes to and from an off-site storage facility.

Level 3 Operations & Maintenance Support – Application Level Service. At Level 3 the Contractor shall provide personnel, processes and technology to support application support services. Level 3 service includes, but is not limited to, application monitoring, initial application baselining; application changes; porting; quality assurance; system assurance; installation; integration; end user training; application code testing; application migration; database support; application C&A support. Level 3 service includes:

- Application Monitoring - The Contractor shall manage and monitor application performance and degradation and provide fault prevention capabilities for data center operations and system metrics to mitigate potential problems. The Contractor shall integrate the application into monitoring systems as a project, and then provide the actual monitoring as a regular part of O&M.
- Initial Application Baselining - The Contractor shall provide initial application baselining services. This applies to, but is not limited to, data center tools, application tools, and functional applications.
- Application Changes - The Contractor shall provide Application Change Services per industry best practices.
- Application Porting - The Contractor shall provide Application Porting Services. Application Porting includes, but is not limited to:
    - Revision of applications for a new system or operating system.
    - Validation and verification for all newly ported applications before entering the production environment. This includes migration and integration
    - Stringent testing to meet DHS security standards
- Quality Control - The Contractor shall provide Application Quality Control services in order to maintain application integrity. Application Quality Control shall meet the quality standards as set forth by DHS Quality Assurance guidelines for Application Management Services. The Contractor shall manage Quality Control according to industry best practices, for example, with processes and staff that are functionally and administratively independent from the product lines and the services delivered to the HART customer. The Contractor shall detect and report quality problems per the SLAs and maintain a Quality Control Plan. The Contractor shall support DHS IV&V activities.
- System Assurance - The Contractor shall provide support to System Assurance services. System assurance provides certifiable operational capability in a 24x7x365(366) environment.

- Application Installation and Test - The Contractor shall provide application installation and testing services in order to ensure proper functionality of applications.
- Application Integration - The Contractor shall provide Application Integration services. Application integration includes, but is not limited to, verification and validation testing.
- End User Training - The Contractor shall provide Application End User Training. This consists of all training necessary to provide staff with needed resources to execute full functionality of applications and effectively support the application.
- Application Code Testing - The Contractor shall provide Application Code Testing services for all applications undergoing application testing. All code shall undergo proper change management and code release procedures. Code testing shall be done on non-production machines and shall undergo thorough test and evaluation procedures.
- Application Migration - The Contractor shall provide application code release and migration services that provide application code release management and migration support to migrate application code onto new platforms without disrupting data center functionality.
- Application Component and Database Maintenance - The Contractor shall support application databases and provide maintenance on all managed applications, databases, web servers, and other application components to assure optimal application performance.

Matcher. "Matcher" is the generic term used to refer to the implemented capability to compare an incoming biometric image to those images previously enrolled in the matching sub-system galleries to determine whether the incoming image has been previously enrolled. Matchers may be hardware or software based. Software matchers consist of software algorithms hosted on application servers that compare templates generated for incoming images against images already resident in the matching sub-system galleries. Hardware matchers perform the same function as their software counterparts with the exception that the hardware matchers are high speed blade computers designed specifically for high-speed match performance.

Matching sub-system. The Matching Sub-system is the component of the system architecture that consists of the applications, servers, and data storage that enroll biometric images in template galleries and execute matching operations for incoming biometric images against those already enrolled in the biometric template galleries. In Increment 1 of the HART system, the matching sub-system will be limited to fingerprint capabilities. In Increment 2, the necessary applications and infrastructure will be added to the matching subsystem to enroll iris and facial images and to match incoming images against the matching sub-system galleries corresponding to the type of incoming image.

Multimodal Bridge Subsystem (MMBS). OBIM's Identity Technology Division has established a small processing capability, the Multimodal Bridge System, for matching face and iris modalities. This system:

- Lacks the capacity for processing full production transaction volumes requiring face and iris matching.
- Does not automatically forward indeterminate matches to the Biometric Support Center for resolution.
- Returns only the raw match results for each modality (i.e. iris and face) and makes no attempt to improve accuracy by leveraging (i.e. fusing) match results from multiple modalities.

This subsystem will not be modified during HART Increment 1. It will connect to the HART core application through the HART multimodal matching subsystem interface.

Multimodal full gallery search. Multimodal full gallery searches are searches of the multiple modality galleries attempting to find a match to more than one biometric modality. These searches are intended to search the "full gallery" – that is all of the enrolled biometrics for each modality – and generate a match or no-match result for each modality searched.

Redress. Redress is the process of removing or correcting derogatory information associated with an identity at the request of the identity's owner.

Response time. Response time for HART transactions shall be the elapsed time from the point where an incoming transaction is received to the point where HART releases the response. The elapsed time will be the sum of the elapsed time for HART core application processing added to the time for biometric matching subsystem operation,

Sizing timeframe. All projections for sizing will assume a timeframe of three (3) years past the end of HART Program Increment 1. OBIM requires that the delivered system infrastructure installed in DHS or other data centers be capable of processing the business volume growth forecast over the 3 elapsed years following the end of Increment 1 without the need for a capacity upgrade.

Target (True) Acceptance Rate (TAR). TAR is expressed as a percent and reflects the percentage of times a system correctly verifies a true claim of identity.

Template (biometric template). A template is a digital reference of distinct characteristics that have been extracted from a biometric modality image and stored in a matching subsystem for use in subsequent biometric matching and authentication processes.

Verification. An operation during which a biometric matching subsystem retrieves a reference from its gallery corresponding to a specific identity and verifies whether the biometrics submitted with the request match the biometrics on file for that identity.

List of Acronyms

Acronym	Definition
ABIS	DoD Automated Biometric Identification System
ANSI	American National Standards Institute
AO	Authorizing Official
AoA	Analysis of Alternatives
AQ	ORACLE Advanced Queuing
ATO	Authority to Operate
AWS	Amazon Web Services
BLOC	Blank Lines of Code
BPO	Baseline Performance Objectives
BRM	Business Reference Model
BSC	Biometric Support Center
C&A	Certification and Accreditation – Superseded by Security Authorization Process
CABIS	Cogent Automated Biometric Identification System
CBP	Customs and Border Protection
CFE	Contractor Furnished Equipment
CIA	Confidentiality, Integrity, and Availability
CJIS	Department of Justice Criminal Justice Information Services
CLIN	Contract Line Item Number
CLOC	Comment Only Lines of Code
CONOPS	Concept of Operations
COR	Contracting Officer's Representative
COTS	Commercial Off the Shelf
CVT	Candidate Verification Tool
CWORD	Commentary Words
DHS	Department of Homeland Security
DoD	Department of Defense

Acronym	Definition
DOJ	Department of Justice
DOS	Department of State
EBTS	Electronic Biometric Transmission Specification
EIT	Electronic Information Technology
ESB	Enterprise Service Bus
ETL	Extract, Translate, and Load
FAR	False Acceptance Rate
FAR	Federal Acquisition Regulations
FBI	Federal Bureau of Investigation
FedRAMP	Federal Risk and Authorization Management Program
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOC	Full Operating Capability
FRD	Homeland Advanced Recognition Technology Functional Requirements Document Increments 1 and 2
GAO	U.S. Government Accountability Office
GFE	Government Furnished Equipment
GOTS	Government Off the Shelf
GSS	General Support Systems
HART	Homeland Advanced Recognition Technology
HCLOC	Header Comment Lines of Code
HCWORD	Header Commentary Words
HSPD	Homeland Security Presidential Directive
HTTPS	Secure Hypertext Transfer Protocol
IA	Information Assurance
IACS	DHS Information Assurance Compliance System
ICAM	Identity, Credential, and Access Management
ICCB	DHS Infrastructure Change Control Board

Acronym	Definition
ICE	Immigration and Customs Enforcement
IDENT	Automated Biometric Identification System
IOC	Initial Operating Capability
INS	Immigration and Naturalization Service
INTERPOL	International Criminal Police Organization
IPR	In-Progress Review
IT	Information Technology
ITL	Information Technology Laboratory
IV&V	Independent Verification and Validation
IXM	IDENT Exchange Messages Specification
KPP	Key Performance Parameter
KST	Known or Suspected Terrorist
MIS	Matcher Interface Service
MMBS	Multimodal Bridge Solution
MNS	Mission Needs Statement
MOP	Measure of Performance
MQ	IBM Message Que
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
MVG	McCabe Cyclometric Complexity
NAS	Network Attached Storage
NCR	National Capital Region
NGI	Next Generation Identification System
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NPE	Non Production Environment
NPPD	National Protection and Programs Directorate
NST	National Security Threat

Acronym	Definition
O&M	Operations and Maintenance
OBIM	Office of Biometric Identity Management
ODS/ODR	Operational Data Store / Operational Data Repository
OFO	Customs and Border Protection Office of Field Operations
OLAP	Online Analytical Processing
ORD	Operational Requirements Document
OTA	Operational Test Agent
PICS	Password Issuance Control System
PMA	Programmable Matching Accelerator
POE	Port of Entry
PSPO	Customs and Border Protection Passenger Systems Program Office
S3	Amazon Simple Storage Service
SAN	Storage Area Network
SCORM	Sharable Content Object Reference Model
SELC	Systems Engineering Life Cycle
SIT	Secondary Inspection Tool
SLA	Service Level Agreement
SLOC-P	Source Lines of Code - Physical
SMTP	Simple Mail Transfer Protocol
SOC	Security Operations Center
SOP	Standard Operating Procedure
SORN	System of Records Notification
SP	Special Publication
TAR	Target Acceptance Rate
TBD	To Be Determined
TEMP	Test and Evaluation Master Plan
TRM	Technical Resource Model
TSA	Transportation Security Administration

Acronym	Definition
ULF	Unsolved Latent File
USCIS	United States Citizenship and Immigration Services
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
WAN	Wide Area Network
WBS	Work Breakdown Structure

PART 3. SPECIAL CONTRACT REQUIREMENTS

3.1 Organizational Conflict of Interest Notice

(a) Offerors should be aware that they may be deemed ineligible to participate in this acquisition by reason of an organizational conflict of interest (OCI) (see FAR 9.5, Organizational and Consultant Conflicts of Interest). Offerors should carefully examine and comply with HSAR 3052.209-72, Organizational Conflict of Interest, found in Section 4 of this solicitation. An offeror's eligibility or ineligibility to participate in the current acquisition is determined by the contracting officer.

(b) Offerors should be aware that the type of work required by this acquisition may give rise to an OCI that may restrict the offeror's ability to compete for follow-on work. These types of OCI do not generally lend themselves to successful mitigation (see FAR 9.5, Organizational and Consultant Conflicts of Interest). Offerors should carefully examine and comply with HSAR 3052.209 73, Limitation of Future Contracting, found in Section 4 of this solicitation. An offeror's eligibility or ineligibility to participate in a future acquisition is determined by the contracting officer.

3.2 Contract Incentives (Fixed Price Incentives – Award Fee)

Incentives (award-fee) under this task order are designed to promote efficiency and quality performance in the execution of the work to be delivered and performed. The basis for the incentives is some element of superior cost, schedule and performance. The incentive percentage under this task order is a maximum [**TBD**] percent of the negotiated fixed price on each of the key CLINs referenced below. The contractor, when exceeding the stated criteria in the contract as specified, has the opportunity to receive a maximum of [**TBD**] percent above the negotiated CLIN price for each of the referenced CLINs. The fixed price award fee CLINs are as follows:

CLIN 0001 Phase I, Increment 1, Core Biometric Management System
CLIN 0008 Post IOC Customer Migration

Incentives are applicable only on the above referenced CLINS and are not applicable to any other task order CLIN. The contractor will be assessed and paid, as applicable, after the final completion of each increment (i.e., after the final delivery and acceptance of CLINs 0001 and 0008). There is no incentive attached to the Hardware/Software CLIN for Increments 1, which is FFP.

NOTE: The award-fee amount and the award-fee determination methodology are unilateral decisions made solely at the discretion of the Government.

3.2.1 Incentive Increases/Decreases during Performance

Increases or decreases in the total maximum incentive fee available under the task order may result from changes to the requirement during performance which result in an increase or decrease in the total price under the affected key CLINs referenced in the above paragraph. However, such incentive fee increases or decreases shall be limited to additions or deletions of work formally directed or accepted by the Government in writing that exceed or vary from the original scope negotiated at the time of award. Not applicable for incentive adjustment are changes limited to Government caused delays (see 3.2.2 below for time adjustments). Any incentive increase or decrease shall be accompanied by a formally signed modification by the Contracting Officer and reflect a within scope change in the work originally planned at the time of award.

3.2.2 Adjustments for Time (Schedule)

Two types of time adjustments are envisioned under this task order. They are adjustments resulting from the addition of work scope under the task order and Government caused delays. The contractor shall not be negatively impacted in incentive determinations based on *schedule* in either of these situations. Any schedule change shall be incorporated in the task order by a formal modification. In the event of

Government caused delays, compensation to the contractor, if appropriate, is limited to an equitable

adjustment for proven costs incurred. Such an increase in CLIN price shall not result in any adjustment to the maximum incentive fee attainable.

3.2.3 Basis for Incentive Fee Payment

Incentive fees are payable only on the CLINS identified as (FPAF) in the payment schedule and shall not exceed [**TBD**] percent of the negotiated price for successfully meeting the related CLIN requirement objectives. Incentive fee is based on predetermined achievement goals in schedule and/or performance that exceed selected objectives set in the Baseline Performance Objectives and defined in Attachment 7.2, Award-Fee Plan.

3.3 Travel

The Contractor travel may be required to support this requirement. All travel required by the Government outside the local commuting area (National Capital Region) will be reimbursed to the Contractor in accordance with the Federal Travel Regulations **(no local travel will be reimbursed under this task order)**. All travel shall be requested in advance and be approved by the COR in writing prior to the travel dates. No travel is authorized unless sufficient funds for travel are available on the contract. Travel is reimbursable at cost. Payment of fees or other charges is not applicable to travel. Travel shall be in accordance with FAR 31.205-46.

3.4 Purchasing Hardware and Software under the Task Order (CPFF)

The Contractor shall submit requests for hardware/software purchases for Government review and written approval prior to the purchase. For changes to a previously approved Government Bill of Materials (BOM), the Contractor shall provide written notification including a rational basis for the change in hardware/software simultaneously to the COR and Contracting Officer at least seven days prior to the intended purchase. In addition, notifications shall include a list of the required equipment to be purchased and the corresponding deleted items, if appropriate, with estimated costs and quantities for each new and substituted item. Changes to HW/SW on the approved BOM resulting in no additional costs to the Government (i.e., substitutions or deletions of items of equal or less value) may be approved by the COR after proper technical vetting of the proposed change by the Government. Changes or additions to HW/SW on the approved BOM resulting in increased net costs of the BOM estimate require written approval by the Contracting Officer after proper technical vetting of the proposed change by the Government. Purchasing hardware/software in advance of proper written Government approval of the purchase may result in non-payment of the Contractor's invoice for those purchases. All purchases of material under this contract shall be in accordance with a Government approved Purchasing system.

The Contractor is required to track all changes to the BOM and shall provide written notification of all changes in a clear, logical, and legible format to the COR and the Contracting Officer.

Payment for hardware and software will be made incrementally based on delivery and Government acceptance of completed deliverables in accordance with the delivery schedule.

The Fixed Fee for all hardware/software purchases under this task order shall not exceed the lesser of 1 percent of estimated HW/SW costs for each increment or $500,000.

3.5 As-Builts and Hardware/Software Inventory

Within 30 days after the completion by the Contractor and acceptance by the Government of each Increment, the contractor shall deliver to the COR, a hard and electronic copy of the system "as-built" drawings and a complete inventory list of all hardware and software delivered to the Government. In addition, the Contractor shall amend and update such drawings and inventory lists to record and capture any changes or corrections, as necessary, during the life of the task order.

3.6 Exercise of Phase II/Increment 2

Phase IIa, Increment 2, Production-Scaled Multimodal Modality Matching and Fusion is one of two parts of Phase

II of the HART system development under the task order and will not be funded at the time of award (subject to the availability of funds in accordance with FAR 52.232.-18) and is dependent on the Government's acceptance and approval of the Systems Engineering Life Cycle (SELC) Critical Design Review. Phase IIb, Increment 2, Data Warehouse is an Optional CLIN and will be exercised at the sole discretion of the Government.

3.7 Government as Co-Licensee

Any software license proposed or issued by the Contractor in the performance of this contract shall include the Government as a co-licensee and provision the license for substitution of a successor contractor. To accomplish this, some negotiation by the contractor of the commercial terms may be required prior to Government acceptance of the software. To facilitate the process of license acceptance, the contractor shall provide written notification and a copy of the commercial license to the Contracting Officer as soon as practicable for Government review and comment prior to the purchase of the license. Any additional costs resulting from the contractor's failure to notify the Government of potentially unacceptable software licensing terms in a timely manner shall be borne by the contractor.

3.8 Substitution of Software

The Government may, in its sole discretion, provide as Government Furnished Software the same software proposed by the Contractor in place of software that would otherwise be provided under license to the Contractor.

3.9 No Private Use of Data First Produced

Pursuant to subparagraph (d)(2) of the Rights in Data-General clause of this task order, the contractor may not use any data first produced in the performance of this task order for any purpose other than the performance of this task order without the prior, written permission of the Contracting Officer.

3.10 Contractor Identification

Contractor employees shall identify themselves as contractors along with their company name at/in all meetings/functions/e-mails related to performance under this contract.

3.11 Integrated Master Schedule

The Contractor shall develop and submit a complete and comprehensive integrated master schedule (IMS) that incorporates all projects, activities, and milestones necessary for the design, development and implementation of HART Increment 1, Increment 2, and optional tasks. Activities include, but are not limited to, major acquisition decision events, systems engineering lifecycle reviews, test events, security, training, etc. The IMS shall provide for regular delivery of configuration items, utilizing an iterative approach, to satisfy the requirements contained in the BPO. The schedule shall conform to the best practices set forth in the GAO Schedule Assessment Guide (GAO-16-89G) and to the structure of the HART work breakdown and CLIN structures set forth in this contract. The Contractor shall submit this comprehensive schedule and all schedule updates during the course of contract execution to the Government in an electronic format mutually agreed upon with the Government.

The initial IMS submission shall be required not later than 20 business days following contract award. All anticipated changes to the schedule baseline shall be communicated to the Contracting Officer's Representative (COR) within three (3) business days. This notification shall include identified impact factors and potential recovery mechanisms. The contractor shall perform schedule risk assessments on the integrated technical and business schedules for all detailed schedules. The government will perform schedule integration within the OBIM Schedules. The contractor shall attend weekly Integrated Project Team (IPT) meetings to identify schedule risks and all known and anticipated schedule variances, to include any potential impacts to the schedule baseline.

3.12 Software Deliverables for Use under Government Contracts or Interagency Agreements

Definitions.

a. "Open Source Software" for the purpose of this statement of work means computer software that is made generally available under a copyright license in which the user is granted the rights to use, copy, modify, prepare derivative works and distribute, in source code or other format, the software, in original or modified form and derivative works thereof without remuneration of any kind.

b. "Server" means a computer system designed to provide the capability of use by multiple users. A server may be the combined operation of hardware and software or software only. This contract [interagency agreement] either requires the contractor to first produce computer software or the first production of computer software will be integral to the performance of the contract.

1. Design of Computer Software. The Contractor will design the computer software under the following bases:

a. Computer Language. The Contractor shall design and produce the software using one of the following languages: Java, C#, JavaScript, Python, Ruby or Go. If the Contractor recommends the use of any other language, it may request the permission of the Contracting Officer.

b. Open Source Software Components. To the extent that the Contractor intends to incorporate open source content into the computer software, it may use open source content subject to an open source license that either requires only acknowledgement of the source or the source and a disclaimer of liability. Prior to incorporating open source content subject to any other license conditions, the Contractor must request and receive the prior written approval of the Contracting Officer.

c. Commercial or Proprietary Software Components. The Contractor shall not incorporate into the computer software content that is subject to either commercial or proprietary license conditions without the prior approval of the Contracting Officer.

d. Server Compatibility. To the extent that the computer software is to be designed for loading on a server, the Contractor shall design the computer software to be operated on at least one of the following server operating systems: Linux (Kernel version 4+), Microsoft Windows (version 2012+ for server software, version 10+ for client software), or Unix-based operating systems (e.g., AIX).

2. Computer Software Deliverables. Upon conclusion of contract performance and at any times specified by the contract during contract performance, the Contractor shall provide the following deliverables associated with that computer software.

a. Operable Source Code. The Contractor shall deliver at the conclusion of contract performance one computer disc containing the complete, compilable, and operable source code in the DHS approved language.

b. Executable Code. The Contractor will deliver at the conclusion of contract performance one computer disc containing the complete and operable executable code.

c. Software Documentation. The Contractor shall create and deliver software documentation, containing any programmer notes and describing the software, its operation, its organization, and any significant characteristics of its design so that a computer programmer skilled in the art of programming according to the approved language may operate, maintain, update, modify, and perform all operations necessary to perpetuate the utility of the computer software.

d. Description of Third Party Licenses Used. To the extent that the Contractor has included in the computer software either DHS approved open source content or software content subject to proprietary licenses, the Contractor shall provide each of those licenses and incorporate those licenses in a text file in the discs delivered.

3. Independence of Cloud Based Software. The Contractor must insure that cloud based software is capable of running on non-Contractor based servers. Any cloud based software must be capable of running on equivalent

DHS or third party servers. This attribute must be an aspect of the software's underling design.

4. Interoperability of Related Data. Data derived from the created software must be capable of being transferred to other software in a machine legible format with a minimal level of outside intervention when consistent with standard industry practice. This attribute must be part of the software's underlying design. The Contractor shall not develop software or use COTS that store OBIM business data using methods and/or data structures that are wholly proprietary or that otherwise would require OBIM to exert undue effort or expense to extract/re-use its own data.

5. Testing of Software.

(1) *Software Testing Required*. Any software created under interagency agreement or contract prior to delivery must undergo software testing. Software testing must be conducted using industry standard tools.

(2) *Timing of Software Testing*. Software testing should occur once executable software has been created.

(3) *Software Testing Requirements*. Software testing should determine the following:

(a)That the software is capable of serving the purpose of its creation and meets the requirements.
(b) That the software is stable and performs correctly to all inputted information.
(c) The software is usable and performs its functions within a time frame appropriate for the nature of the operation.

(4) *Installation Testing*. Installation testing that identifies what will be necessary for a user to install and successfully run the software will be required prior to delivery.

3.13 Invoicing Instructions

A. 52.232-1 Payments. In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

1) Cover sheet identifying DHS;
2) Task Order Number;
3) Modification Number, if any;
4) DUNS Number;
5) TINS Number; and
6) Month services provided or date deliverables completed
7) Contract Line Item Number (CLIN) for each billed item.

B. The contractor shall submit an electronic copy to email address: nppdinvoice.consolidation@dhs.gov.

C. Simultaneously provide an electronic copy of the invoice to the following individuals at the addresses below:

Robert Degnan, Contracting Officer
Robert.Degnan@hq.dhs.gov; 202-447-5576

Shannon Ozoria, Contracting Specialist
Shannon.Ozoria@hq.dhs.gov; 202-447-0230

Abe Jacob, Contracting Officer Representative
Abe.Jacob@ice.dhs.gov;202-295-0787

The contractor shall submit invoices to the email address above. Additionally, the contractor shall prepare and submit a sufficient and procurement regulatory compliant invoice and receiving report for technical certification of inspection/acceptance of services and approval for payment. The contractor shall attach back up information to the invoices and receiving reports substantiating all costs for services performed. The receiving agency's written or

electronic acceptance by the COR and date of acceptance shall be included as part of the backup documentation.

Payment for Increments 1 and 2 shall be based on the delivery to, and acceptance by the Government of product deliverables in accordance with task order schedule. Deliverables rejected by the Government for non-performance or deficiencies shall be corrected by the contractor at no additional cost to the Government prior to payment for that deliverable. Final payment for each Increment shall be withheld until a determination of acceptance can be made by the Government based on a fully operational system meeting all Performance Work Statement (PWS) requirements, as tested and verified by a qualified independent party chosen by the Government.

3.14 Performance and Acceptance Criteria

The following criteria will serve as the basis to evaluate the contractor on providing timely and high quality performance during execution of the contract. The criteria are broken into the following performance based elements: Code Quality and SELC Deliverable Quality. Each performance element is independent and evaluated throughout contract execution.

Element 1: Code Quality

Application of the code quality analysis tools shall be performed by the contractor using CAST AIP or equivalent static or dynamic code analysis tools. Code quality analysis tools, their configurations, rule settings, or other tool operational parameters will be available for review, verification. And validation by the Government or its representative, and the tool settings used shall be subject to configuration management. All code quality analysis tools results shall be made available to designated government representatives. The code quality tools shall comply with software industry rules, standards, and best practices. Deviations from the rules shall be logged as critical violation and posted to the tool's dashboard portal.

Element 2: Deliverable Quality

The government will evaluate the quality of the contract deliverables to ensure documentation quality. The contractor shall be responsible for ensuring the timeliness, quality, and completeness of each documentation deliverable. Criteria that will be used to evaluate the documentation will result in three major categories of comments: Critical Issues, Important Clarifications, and Editorial Recommendations. All critical issues and important clarifications must be addressed with the final submission.

3.15 Security of Deliverables and Information

All document deliverables of the contractor shall remain categorized as, and shall be clearly labeled as "For Official Use Only". The release of any portion of the deliverable beyond contractor personnel working on the contract with a need to know the information contained therein to perform under this contract must be authorized in writing by the Government.

In accordance with DHS 4300A, email transmissions of all official correspondence specifically For Official Use Only (FOUO) or Sensitive PII classifications being sent/received outside of DHS domains will be protected by encryption or transmitted within secure communications systems (e.g., government email). For added security, when transmitting FOUO/SPII over a regular email channel, the information will be included as a password protected attachment with the password provided under separate cover. FOUO designated information shall not be sent to personal email accounts. Email containing FOUO will contain (U) in the subject line and CLASSIFICATION: UNCLASSIFIED//FOUO Caveats: None or Law Enforcement Sensitive at the beginning and end of email body. Where the sensitivity of the information material warrants additional access and dissemination restrictions, the originator may cite a WARNING: This email contains FOR OFFICIAL USE ONLY (FOUO) OR PRIVACY DATA. It may contain information exempt from public release under the Freedom of Information Act (5 U.S.C. 552). The information contained herein must be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO/PII information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. The contractor is responsible for practicing sound operations security (OPSEC) and ensuring other personnel have a valid "need to know". Digital Signature or Other Electronic Signature Methods shall be used whenever practical, except where handwritten signatures are required by law, regulation, Executive Order, or other agency requirement.

Digital Signature or Other Electronic Signature Methods, when properly executed, shall be accepted to the maximum extent practicable.

3.16 Company Information Review/ Acquisition Risk

During the period of performance of the contract, the Contractor is under a continuing obligation to ensure that all responses to the acquisition risk questions remain complete, accurate, and up-to-date. The Contractor shall promptly notify and submit updated responses to the CO when any change in circumstances of the Contractor or subcontractors warrants a change in the Contractor's or subcontractor's responses to the acquisition risk questions. In addition, the Contractor is under a continuing obligation to promptly disclose to the CO any proposed additional or replacement subcontractors. Failure to comply with these continuing obligations may be grounds for termination for default under the termination clause of this contract.

The government reserves the right to prohibit individuals who are not U.S. citizens from performing services or delivering goods under this contract.

PART 4. SOLICITATION PROVISIONS AND CONTRACT CLAUSES

4.1. PROVISIONS AND CLAUSES INCORPORATED BY REFERENCE

FAR 52.203-18	Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements – Representation (JAN 2017)
FAR 52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017)
FAR 52.216-7	Allowable Cost and Payment (JUN 2013)
FAR 52.216-8	Fixed Fee (JUN 2011)
FAR 52.216-29	Time-and-Materials/ Labor-Hour Proposal Requirements - Non-Commercial Item Acquisition with Adequate Price Competition (FEB 2007)
FAR 52.223-15	Energy Efficiency in Energy-Consuming Products (DEC 2007)
FAR 52.227-9	Refund of Royalties (APR 1984)
FAR 52.227-16	Additional Data Requirements (JUN 1987)
FAR 52.232-1	Payments (APR 1984)
FAR 52.232-18	Availability of Funds (APR 1984)
FAR 52.237-3	Continuity of Services (JAN 1991)
FAR 52.232-39	Unenforceability of Unauthorized Obligations (JUN 2013)
FAR 52.239-1	Privacy or Security Safeguards (AUG 1996)
FAR 52.245-1	Government Property (APR 2012)
FAR 52.246-2	Inspection of Supplies – Fixed Price (AUG 1996)
FAR 52.246-6	Inspection – Time and Material and Labor Hour (MAY 2001)
HSAR 3052.219.70	Small Business Subcontracting Plan Reporting (JUN 2006)
HSAR 3052.242-72	Contracting Officer's Technical Representative (DEC 2003)

4.2. PROVISIONS AND CLAUSES INCORPORATED BY FULL TEXT

FAR 52.217-5, Evaluation of Options (JUL 1990)

Except when it is determined in accordance with FAR 17.206(b) not to be in the Government's best interests, the Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. Evaluation of options will not obligate the Government to exercise the option(s).

The following two Option clauses are applicable to Post Deployment Support Services periods only.

FAR 52.217-8, Option to Extend Services (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within *10 days* prior to the end of the contract period.

FAR 52.217-9, Option to Extend the Term of the contract (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 15 days prior to the end of the contract period; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least *30 days* before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed *24 months* after deployment of Increment 1.

The following clause will apply to all data first produced in the performance of the contract and to any devices that originate in the performance of the contract.

FAR 52.227-1, Authorization and Consent (DEC 2007)

(a) The Government authorizes and consents to all use and manufacture, in performing this contract or any subcontract at any tier, of any invention described in and covered by a United States patent—

(1) Embodied in the structure or composition of any article the delivery of which is accepted by the Government under this contract; or

(2) Used in machinery, tools, or methods whose use necessarily results from compliance by the Contractor or a subcontractor with (i) specifications or written provisions forming a part of this contract or (ii) specific written instructions given by the Contracting Officer directing the manner of performance. the entire liability to the Government for infringement of a United States patent shall be determined solely by the provisions of the indemnity clause, if any, included in this contract or any subcontract hereunder (including any lower-tier subcontract), and the Government assumes liability for all other infringement to the extent of the authorization and consent hereinabove granted.

(b) The Contractor shall include the substance of this clause, including this paragraph (b), in all subcontracts that are expected to exceed the simplified acquisition threshold. However, omission of this clause from any subcontract, including those at or below the simplified acquisition threshold, does not affect this authorization and consent.

FAR 52.227-2, Notice and Assistance Regarding Patent and Copyright Infringement (DEC 2007)

(a) The Contractor shall report to the Contracting Officer, promptly and in reasonable written detail, each notice or claim of patent or copyright infringement based on the performance of this contract of which the Contractor has knowledge.

(b) In the event of any claim or suit against the Government on account of any alleged patent or copyright infringement arising out of the performance of this contract or out of the use of any supplies furnished or work or services performed under this contract, the Contractor shall furnish to the Government, when requested by the Contracting Officer, all evidence and information in the Contractor's possession pertaining to such claim or suit. Such evidence and information shall be furnished at the expense of the Government except where the Contractor has agreed to indemnify the Government.

(c) The Contractor shall include the substance of this clause, including this paragraph (c), in all subcontracts that are expected to exceed the simplified acquisition threshold.

FAR 52.227-6, Royalty Information (APR 1984)

(a) Cost or charges for royalties. When the response to this solicitation contains costs or charges for royalties totaling more than $250, the following information shall be included in the response relating to each separate item of royalty or license fee:

(1) Name and address of licensor.
(2) Date of license agreement.
(3) Patent numbers, patent application serial numbers, or other basis on which the royalty is payable.
(4) Brief description, including any part or model numbers of each contract item or component on which the royalty is payable.
(5) Percentage or dollar rate of royalty per unit.
(6) Unit price of contract item.
(7) Number of units.
(8) Total dollar amount of royalties.

(b) Copies of current licenses. In addition, if specifically requested by the Contracting Officer before execution of the contract, the offeror shall furnish a copy of the current license agreement and an identification of applicable claims of specific patents.

The following clause will apply to any data, devices, or equipment that are not first produced in the performance of the contract in the form that they existed at the time of award of the task order.

FAR 52.227-3, Patent Indemnity (APR 1984)

(a) The Contractor shall indemnify the Government and its officers, agents, and employees against liability, including costs, for infringement of any United States patent (except a patent issued upon an application that is now or may hereafter be withheld from issue pursuant to a Secrecy Order under 35 U.S.C. 181) arising out of the manufacture or delivery of supplies, the performance of services, or the construction, alteration, modification, or repair of real property (hereinafter referred to as "construction work") under this contract, or out of the use or disposal by or for the account of the Government of such supplies or construction work.

(b) This indemnity shall not apply unless the Contractor shall have been informed as soon as practicable by the Government of the suit or action alleging such infringement and shall have been given such opportunity as is afforded by applicable laws, rules, or regulations to participate in its defense. Further, this indemnity shall not apply to—

(1) An infringement resulting from compliance with specific written instructions of the Contracting Officer directing a change in the supplies to be delivered or in the materials or equipment to be used, or directing a manner of performance of the contract not normally used by the Contractor;
(2) An infringement resulting from addition to or change in supplies or components furnished or construction work performed that was made subsequent to delivery or performance; or
(3) A claimed infringement that is unreasonably settled without the consent of the Contractor, unless required by final decree of a court of competent jurisdiction.

FAR 52.227-14, Rights in Data -- General (MAY 2014), Alternate II (DEC 2007) and Alternate III (DEC 2007) (DEVIATION)

(a) Definitions. As used in this clause—

"Computer database" or "database" means a collection of recorded information in a form capable of, and for the purpose of, being stored in, processed, and operated on by a computer. The term does not include computer software.

"Computer software"—

(1) Means

(i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and

(ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

(2) Does not include computer databases or computer software documentation.

"Computer software documentation" means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.

"Data" means recorded information, regardless of form or the media on which it may be recorded. The term

includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

“Form, fit, and function data” means data relating to items, components, or processes that are sufficient to enable physical and functional interchangeability, and data identifying source, size, configuration, mating, and attachment characteristics, functional characteristics, and performance requirements. For computer software it means data identifying source, functional characteristics, and performance requirements but specifically excludes the source code, algorithms, processes, formulas, and flow charts of the software.

“Limited rights” means the rights of the Government in limited rights data as set forth in the Limited Rights Notice of subparagraph (g)(2) if included in this clause.

“Limited rights data” means data, other than computer software, that embody trade secrets or are commercial or financial and confidential or privileged, to the extent that such data pertain to items, components, or processes developed at private expense, including minor modifications.

”Restricted computer software” means computer software developed at private expense and that is a trade secret; is commercial or financial and is confidential or privileged; or is copyrighted computer software, including minor modifications of the computer software.

“Restricted rights,” as used in this clause, means the rights of the Government in restricted computer software, as set forth in a Restricted Rights Notice of paragraph (g) if included in this clause, or as otherwise may be provided in a collateral agreement incorporated in and made part of this contract, including minor modifications of such computer software.

“Technical data” means recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer databases and computer software documentation). This term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration. The term includes recorded information of a scientific or technical nature that is included in computer databases (See 41 U.S.C. 116).

“Unlimited rights” means the right of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.

(b) *Allocation of rights.*

(1) Except as provided in paragraph (c) of this clause, the Government shall have—

(i) Unlimited rights in:

(A) Data first produced in the performance of this contract;

(B) Form, fit, and function data delivered under this contract;

(C) Data delivered under this contract (except for restricted computer software) that constitute manuals or instructional and training material for installation, operation, or routine maintenance and repair of items, components, or processes delivered or furnished for use under this contract;

(D) All other data delivered under this contract unless provided otherwise for limited rights data or restricted computer software in accordance with paragraph (g) of this clause; and

(ii) The right to limit the Contractor’s assertion of copyright in data first produced in the performance of this contract, and to obtain assignment of copyright in that data, in

accordance with paragraph (c)(1) of this clause.

(2) The Contractor shall have the right to—

(i) Assert copyright in data first produced in the performance of this contract to the extent provided in paragraph (c)(1) of this clause;

(ii) Use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, unless provided otherwise in paragraph
(d) of this clause;

(iii) Substantiate use of, add or correct limited rights, restricted rights, or copyright notices and to take other appropriate action, in accordance with paragraphs (e) and (f) of this clause; and

(iv) Protect from unauthorized disclosure and use those data that are limited rights data or restricted computer software to the extent provided in paragraph (g) of this clause.

(c) *Copyright—*

(1) *Data first produced in the performance of this contract*.

(i) Unless provided otherwise in paragraph (d) of this clause, the Contractor may establish, without prior approval of the Contracting Officer, claim to copyright in scientific and technical articles based on or containing data first produced in the performance of this contract and published in academic, technical or professional journals, symposia proceedings or similar works. The prior, express written permission of the Contracting Officer is required to assert copyright in all other data first produced in the performance of this contract.

(ii) If the Government desires to obtain copyright in data first produced in the performance of this contract and permission has not been granted as set forth in paragraph (c)(1)(i) of this clause, the Contracting Officer shall direct the Contractor to assign (with or without registration), or obtain the assignment of, the copyright to the Government or its designated assignee.

(iii) When authorized to assert copyright to the data, the Contractor shall affix the applicable copyright notices of 17 U.S.C. 401 or 402, and acknowledgment of Government sponsorship (including contract number).

(iv) When authorized to assert copyright to the data, for data other than computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable worldwide license in such copyrighted data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government. For computer software, the Contractor grants to the Government and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in such copyrighted computer software to reproduce, prepare derivative works, and perform publicly and display publicly (but not to distribute copies to the public) by or on behalf of the Government.

(2) *Data not first produced in the performance of this contract.* The Contractor shall not, without prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract unless the Contractor—

(i) Identifies the data; and

(ii) Grants to the Government, or acquires on its behalf, a license of the same scope as set forth in subparagraph (c)(1) of this clause or; if such data are restricted computer software, the

Government shall acquire a copyright license as set forth in subparagraph (g)(4) of this clause (if included in this contract) or as otherwise provided in a collateral agreement incorporated in or made part of this contract.

(3) *Removal of copyright notices*. The Government will not remove any authorized copyright notices placed on data pursuant to this paragraph (c), and will include such notices on all reproductions of the data.

(d) *Release, publication and use of data*. The Contractor shall have the right to use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, except—

(1) As prohibited by Federal law or regulation (*e.g.*, export control or national security laws or regulations);

(2) As expressly set forth in this contract; or

(3) If the Contractor receives or is given access to data necessary for the performance of this contract which contain restrictive markings, the Contractor shall treat the data in accordance with such markings unless otherwise specifically authorized otherwise in writing by the Contracting Officer.

(e) *Unauthorized marking of data*.

(1) Notwithstanding any other provisions of this contract concerning inspection or acceptance, if any data delivered under this contract are marked with the notices specified in paragraph (g)(3) or (g)(4) of this clause and use of the notices is not authorized by this clause, or if such data bears any other restrictive or limiting markings not authorized by this contract, the Contracting Officer may at any time either return the data to the Contractor, or cancel or ignore the markings. However, pursuant to 41 U.S.C. 4703, the following procedures shall apply prior to canceling or ignoring the markings.

(i) The Contracting Officer will make written inquiry to the Contractor affording the Contractor 60 days from receipt of the inquiry to provide written justification to substantiate the propriety of the markings;

(ii) If the Contractor fails to respond or fails to provide written justification to substantiate the propriety of the markings within the 60-day period (or a longer time approved in writing by the Contracting Officer for good cause shown), the Government shall have the right to cancel or ignore the markings at any time after said period and the data will no longer be made subject to any disclosure prohibitions.

(iii) If the Contractor provides written justification to substantiate the propriety of the markings within the period set in subdivision (e)(1)(i) of this clause, the Contracting Officer will consider such written justification and determine whether or not the markings are to be canceled or ignored. If the Contracting Officer determines that the markings are authorized, the Contractor will be so notified in writing. If the Contracting Officer determines, with concurrence of the head of the contracting activity, that the markings are not authorized, the Contracting Officer will furnish the Contractor a written determination, which determination shall become the final agency decision regarding the appropriateness of the markings unless the Contractor files suit in a court of competent jurisdiction within 90 days of receipt of the Contracting Officer's decision. The Government shall continue to abide by the markings under this paragraph (e)(1)(iii) until final resolution of the matter either by the Contracting Officer's determination becoming final (in which instance the Government will thereafter have the right to cancel or ignore the markings at any time and the data will no longer be made subject to any disclosure prohibitions), or by final disposition of the matter by court decision if suit is filed.

(2) The time limits in the procedures set forth in subparagraph (e)(1) of this clause may be modified in accordance with agency regulations implementing the Freedom of Information Act (5 U.S.C.

552) if necessary to respond to a request thereunder.

(3) Except to the extent the Government's action occurs as the result of final disposition of the matter by a court of competent jurisdiction, the Contractor is not precluded by paragraph (e) of this clause from brining a claim, in accordance with the Disputes clause of this contract, that may arise as a result of the Government removing or ignoring authorized markings on data delivered under this contract.

(f) *Omitted or incorrect markings*.

(1) Data delivered to the Government without any restrictive markings shall be deemed to have been furnished with unlimited rights. The Government is not liable for the disclosure, use, or reproduction of such data.

(2) If the unmarked data has not been disclosed without restriction outside the Government, the Contractor may request, within 6 months (or a longer time approved by the Contracting Officer in writing for good cause shown) after delivery of such data, permission to have authorized notices placed on qualifying data at the Contractor's expense, and the Contracting Officer may agree to do so if the Contractor—

(i) Identifies the data to which the omitted notice is to be applied;

(ii) Demonstrates that the omission of the notice was inadvertent;

(iii) Establishes that the use of the proposed notice is authorized; and

(iv) Acknowledges that the Government has no liability for the disclosure, use, or reproduction of any data made prior to the addition of the notice or resulting from the omission of the notice.

(3) If data has been marked with an incorrect notice, the Contracting Officer may—

(i) Permit correction of the notice at the Contractor's expense if the Contractor identifies the data and demonstrates that the correct notice is authorized, or

(ii) Correct any incorrect notices.

(g) *Protection of limited rights data and restricted computer software.*

(1) The Contractor may withhold from delivery qualifying limited rights data or restricted computer software that are not data identified in paragraphs (b)(1)(i), (ii), and (iii) of this clause. As a condition to this withholding, the Contractor shall—

(i) Identify the data being withheld; and

(ii) Furnish form, fit, and function data instead.

(2) Limited rights data that are formatted as a computer database for delivery to the Government shall be treated as limited rights data and not restricted computer software.

(3) Notwithstanding paragraph (g)(1) of this clause, the contract may identify and specify the delivery of limited rights data, or the Contracting Officer may require by written request the delivery of limited rights data that has been withheld or would otherwise be entitled to be withheld. If delivery of that data is required, the Contractor shall affix the following "Limited Rights Notice" to the data and the Government will treat the data, subject to the provisions of paragraphs (e) and (f) of this clause, in accordance with the notice:

Limited Rights Notice (Dec 2007)

(a) These data are submitted with limited rights under Government Contract No._____(and subcontract ___, if appropriate). These data may be reproduced and used by the Government with the express limitation that they will not, without written permission of the Contractor, be used for purposes of manufacture nor disclosed outside the Government; except that the Government may disclose these data outside the Government for the following purposes, if any; provided that the Government makes such disclosure subject to prohibition against further use and disclosure: *[Agencies may list additional purposes as set forth in 27.404(c)(1) or if none, so state.]*

(i) Use (except for manufacture) by support service contractors.

(ii) Evaluation by nongovernment evaluators.

(iii) Use (except for manufacture) by other contractors participating in the Government's program of which the specific contract is a part.

(iv) Emergency repair or overhaul work.

(v) Release to a foreign government, or its instrumentalities, if required to serve the interests of the U.S. Government, for information or evaluation, or for emergency repair or overhaul work by the foreign government.

(b) This Notice shall be marked on any reproduction of these data, in whole or in part. (4)

(i) Notwithstanding paragraph (g)(1) of this clause, the contract may identify and specify the delivery of restricted computer software, or the Contracting Officer may require by written request the delivery of restricted computer software that has been withheld or would otherwise be entitled to be withheld. If delivery of that computer software is required, the Contractor shall affix the following "Restricted Rights Notice" to the computer software and the Government will treat the computer software, subject to paragraphs (e) and (f) of this clause, in accordance with the notice:

Restricted Rights Notice (Dec 2007)

(a) This computer software is submitted with restricted rights under Government Contract No._____(and subcontract_____, if appropriate). It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b) of this notice or as otherwise expressly stated in the contract.

(b) This computer software may be—

(1) Used or copied for use in or with the computer(s) for which it was acquired, including use at any Government installation to which such computer(s) may be transferred;

(2) Used or copied for use in a backup computer if any computer for which it was acquired is inoperative;

(3) Reproduced for safekeeping (archives) or backup purposes;

(4) Modified, adapted, or combined with other computer software, *provided* that the modified, adapted, or combined portions of the derivative software incorporating any of the delivered, restricted computer software shall be subject to the same restricted rights;

(5) Disclosed to and reproduced for use by support service Contractors or their subcontractors in accordance with paragraphs (b)(1) through (4) of this notice; and

(6) Used or copied for use in or transferred to a replacement computer.

(c) Notwithstanding the foregoing, if this computer software is copyrighted computer software, it is licensed to the Government with the minimum rights set forth in paragraph (b) of this notice.

(d) Any other rights or limitations regarding the use, duplication, or disclosure of this computer software are to be expressly stated in, or incorporated in, the contract.

(e) This Notice shall be marked on any reproduction of this computer software, in whole or in part.

(End of notice)

(ii) Where it is impractical to include the Restricted Rights Notice on restricted computer software, the following short-form Notice may be used instead:

Restricted Rights Notice Short Form (Jun 1987)

Use, reproduction, or disclosure is subject to restrictions set forth in Contract No. _____(and subcontract, if appropriate) with _____(name of Contractor and subcontractor).

(End of notice)

(iii) If restricted computer software is delivered with the copyright notice of 17 U.S.C. 401, it will be presumed to be licensed to the Government without disclosure prohibitions, with the minimum rights set forth in paragraph (b) of this clause.

(h) *Subcontracting*. The Contractor shall obtain from its subcontractors all data and rights therein necessary to fulfill the Contractor's obligations to the Government under this contract. If a subcontractor refuses to accept terms affording the Government such rights, the Contractor shall promptly notify the Contracting Officer of the refusal and shall not proceed with the subcontract award without authorization in writing from the Contracting Officer.

(i) *Relationship to patents or other rights*. Nothing contained in this clause shall imply a license to the Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the Government.

FAR 52.227-15, Representation of Limited Rights Data and Restricted Computer Software (DEC 2007)

(a) This solicitation sets forth the Government's known delivery requirements for data (as defined in the clause at 52.227-14, Rights in Data--General). Any resulting contract may also provide the Government the option to order additional data under the Additional Data Requirements clause at 52.227-16, if included in the contract. Any data delivered under the resulting contract will be subject to the Rights in Data--General clause at 52.227-14 included in this contract. Under the latter clause, a Contractor may withhold from delivery data that qualify as limited rights data or restricted computer software, and deliver form, fit, and function data instead. The latter clause also may be used with its Alternates II and/or III to obtain delivery of limited rights data or restricted computer software, marked with limited rights or restricted rights notices, as appropriate. In addition, use of Alternate V with this latter clause provides the Government the right to inspect such data at the Contractor's facility.

(b) By completing the remainder of this paragraph, the offeror represents that it has reviewed the requirements for the delivery of technical data or computer software and states [offeror check appropriate block]—

[ ] (1) None of the data proposed for fulfilling the data delivery requirements qualifies as limited rights data or restricted computer software; or

[ ] (2) Data proposed for fulfilling the data delivery requirements qualify as limited rights data or restricted computer software and are identified as follows:

_____
_____
_____

(c) Any identification of limited rights data or restricted computer software in the offeror's response is not determinative of the status of the data should a contract be awarded to the offeror.

FAR 52.252-1, Solicitation Provisions Incorporated by Reference (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es): http://farsite.hill.af.mil/.

FAR 52.252-2, Clauses Incorporated by Reference (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): http://farsite.hill.af.mil/.

HSAR 3052.204-71, Contractor Employee Access (SEP 2012)

(a) Sensitive Information, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

HSAR 3052.209-72, Organizational Conflict of Interest (JUN 2006)

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting is that: (1) Potential offerors may have had access to non-public Government information that would provide an unfair competitive advantage under the present solicitation, (2) Potential offerors may have an unfair competitive advantage because they developed or established the ground rules for the present solicitation, or (3) Potential offerors may have an actual conflict of interest if the contractor currently has a contract supporting the legacy system Automated Biometric Identification System (IDENT) or the future HART system.

(b) If any such conflict of interest is found to exist, the Contracting Officer may (1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded. After discussion with the offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

(c) Disclosure: The offeror hereby represents, to the best of its knowledge that:

___(1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or

___(2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included a mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes the conflict can be avoided, neutralized, or mitigated, the offeror shall submit a mitigation plan to the Government for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan.

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the offeror. The Contracting Officer will use all information submitted by the offeror, and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful offeror shall inform the Contracting Officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestitures that may affect this provision.

(g) Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

HSAR 3052.209-73, Limitation on Future Contracting (JUN 2006)

(a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective offerors is invited to FAR Subpart 9.5— Organizational Conflicts of Interest.

(b) The nature of this conflict is that: (1) The contractor may gain access to non-public Government information that would provide an unfair competitive advantage under a future acquisition, or (2) The contractor may gain an unfair competitive advantage because it developed or established the ground rules for a future acquisition.

(c) The restrictions upon future contracting are as follows:

(1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing DHS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract). DHS shall not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.

(2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

HSAR 3052.209-70, Prohibition on Contracts with Corporate Expatriates (JUN 2006)

(a) Prohibitions.

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(b) Definitions. As used in this clause:

Expanded Affiliated Group means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting `more than 50 percent' for `at least 80 percent' each place it appears.

Foreign Incorporated Entity means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

Inverted Domestic Corporation. A foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—

(1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;

(2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—

(i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or

(ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and

(3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

Person, domestic, and foreign have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

(c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

(1) Certain stock disregarded. For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:

(i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or

(ii) Stock of such entity which is sold in a public offering related to an acquisition described in section 835(b)(1) of the Homeland Security Act, 6 U.S.C. 395(b)(1).

(2) Plan deemed in certain cases. If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.

(3) Certain transfers disregarded. The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) Special rule for related partnerships. For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395(b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(e) Treatment of Certain Rights.

(1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:

(i) warrants;
(ii) options;
(iii) contracts to acquire stock;
(iv) convertible debt instruments; and
(v) others similar interests.

(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of Section 835.

(f) Disclosure. The offeror under this solicitation represents that [Check one]:

__ it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003;

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it has submitted a request for waiver pursuant to 3009.108-7004, which has not been denied; or

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it plans to submit a request for waiver pursuant to 3009.108-7004.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

HSAR 3052.215-70, Key Personnel or Facilities (DEC 2003) *(Applicable to Post Deployment Periods 1 and 2)*

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel or Facilities under this Contract: *TBD 60 days prior to start of Post Deployment Period 1*

HSAR 3052.216-71, Determination of Award-Fee (SEP 2012)

(a) The Government shall evaluate contractor performance at the end of each specified evaluation period(s) to determine the amount of award. The contractor agrees that the amount of award and the award fee methodology are unilateral decisions to be made at the sole discretion of the Government.

(b) Contractor performance shall be evaluated according to a Performance Evaluation Plan. The contractor shall be periodically informed of the quality of its performance and areas in which improvements are expected.

(c) The contractor shall be promptly advised, in writing, of the determination and reasons why the award fee was or was not earned. The contractor may submit a performance self-evaluation for each evaluation period. The amount of award is at the sole discretion of the Government but any self-evaluation received within 10 business days after the

end of the current evaluation period will be given such consideration, as may be deemed appropriate by the Government.

HSAR 3052.216-72, Performance Evaluation Plan (DEC 2003)

(a) A Performance Evaluation Plan shall be unilaterally established by the Government based on the criteria stated in the contract and used for the determination of award fee. This plan shall include the criteria used to evaluate each area and the percentage of award fee (if any) available for each area. A copy of the plan shall be provided to the contractor 21 business days prior to the start of the first evaluation period.

(b) The criteria contained within the Performance Evaluation Plan may relate to: (1) Technical (including schedule) requirements if appropriate; (2) Management; and (3) Cost.

(c) The Performance Evaluation Plan may, consistent with the contract, be revised unilaterally by the Government at any time during the period of performance. Notification of such changes shall be provided to the contractor 21 calendar days prior to the start of the evaluation period to which the change will apply.

HSAR 3052.216-73, Distribution of Award-Fee (DEC 2003)

(a) The total amount of award fee available under this contract is assigned according to the following evaluation periods and amounts:

Evaluation Period: Phase I/Increment 1 and Post IOC Customer Migration

Available Award Fee: TBD

(b) Payment of the award fee shall be made, provided that after payment of 85 percent of the potential award fee, the Government may withhold further payment of the award fee until a reserve is set aside in an amount that the Government considers necessary to protect its interest. This reserve shall not exceed 15 percent of the total potential award fee or $100,000, whichever is less.

(c) In the event of contract termination, either in whole or in part, the amount of award fee available shall represent a pro rata distribution associated with evaluation period activities or events as determined by the Government.

(d) The Government will promptly make payment of any award fee upon the submission by the contractor to the contracting officer's authorized representative, of a public voucher or invoice in the amount of the total fee earned for the period evaluated. Payment will be made by issuing a contract modification.

HSAR Deviation 15-01, Information Technology Security and Privacy Training (MAR 2015)

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements*.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty
(30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for

each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) Privacy Training Requirements. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors.

Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award.

Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The email notification shall state the required training has been completed for all Contractor and subcontractor employees.

HSAR Deviation 15-01, Safeguarding Sensitive Information (MAR 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b)*Definitions.* As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static

Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

- Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
- Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
- Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and (4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities*. The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

- DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
- DHS Sensitive Systems Policy Directive 4300A
- DHS 4300A Sensitive Systems Handbook and Attachments
- DHS Security Authorization Process Guide
- DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
- DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
- DHS Information Security Performance Plan (current fiscal year)
- DHS Privacy Incident Handling Guidance
- Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
- NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

- Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

- The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

- All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

- The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or

Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review*. The Government may elect to conduct random periodic reviews to ensure that the security

requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information.

These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US- CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(xv) Inspections,
(xvi) Investigations,
(xvii) Forensic reviews, and
(xviii) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) *Additional PII and/or SPII Notification Requirements*.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall

include:

(xix) A brief description of the incident;
(xx) A description of the types of PII and SPII involved;
(xxi) A statement as to whether the PII or SPII was encrypted or protected by other means;
(xxii) Steps individuals may take to protect themselves;
(xxiii) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(xxiv) Information identifying who individuals may contact for additional information.
(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

4.3. OTHER TERMS AND CONDITIONS

DHS Enterprise Architecture Compliance Terms and Conditions

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.

- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.

- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

- Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.

- Applicability of Internet Protocol Version 6 (IPv6) to DRS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the US. Government Version 6 (USGv6) Profile National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

DHS Geospatial Information System Terms and Conditions

All implementations including geospatial data, information, and services shall comply with the policies and requirements set forth in the DHS Geospatial Information Infrastructure (GII), including (but not limited to) the following:

- All data built to the GII, whether adopted or developed, shall be submitted to the government for review and insertion into the DHS Data Reference Model.

- All software built to the GII, whether adopted or developed, shall be submitted to the government for review and insertion into the DHS Technical Reference Model.

Accessibility Requirements (Section 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public. All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

Section 508 Applicable EIT Accessibility Standards
36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.24 Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

36 CFR 1194.26 Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All

EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Section 508 Applicable Exceptions
Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements
36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

All tasks for testing of functional and/or technical requirements must include specific testing for Section 508 compliance, and must use DHS Office of Accessible Systems and Technology approved testing methods and tools. For information about approved testing methods and tools send an email to accessibility@dhs.gov.

Energy Star Standards

All hardware procured directly or in support of this action must meet applicable and appropriate EPEAT and ENERGY Star standards.

Government-Furnished Equipment (GFE), Government-Furnished Property (GFP) and Contractor Acquired Property (CAP)

If the proposed solution requires the use of GFP/GFE/CAP to be provided then the contractor shall maintain accounting and inventory documentation regarding the issuance of GFP/GFE/CAP to all program contractor employees or subcontractors in accordance with FAR Part 45, FAR 52.245-1and FAR 52.245-9. Also the contractor shall be responsible in identifying, tracking, conducting 100% physical inventories and maintaining control of all Government-Furnished Property, Government-Furnished Equipment, and Contractor-Acquired Property (GFP/GFE/CAP) in its possession including subcontractors and that all physical inventory reporting and property reporting requirements are met. The contractor shall possess an established, government-approved property control system to identify every item providing complete, current, auditable records of all transactions.

The contractor shall coordinate and obtain OBIM Asset Management approval prior to transferring/moving any government property, including disposal or exchanges. The contractor shall provide a Monthly Property Management Report of all GFE/GFP/CAP on hand to the government as specified under the Deliverable table. Any

specific documentation/information needed to complete this effort will be provided by the government at the time of award. The contractor shall perform an annual 100% physical inventory consisting of all GFE/GFP/CAP in the custody of the contractor on hand as specified in the deliverable table.

Property Inventory
Contractor will ensure personnel apply a DHS-supplied barcode to all property purchased for NPPD. Contractor must establish and maintain an accurate master inventory of all property purchase for NPPD under this [Contract/IAA].

Notification of Property Receipt
Contractor will confirm receipt of NPPD property purchased under this SOW with the assigned NPPD Accountable Property Officer within 5 business days of receipt.

Monthly Asset Management Report
Contractor will ensure personnel prepare a monthly Asset Management Report, which contains accurate information for all NPPD property located at their facility. At a minimum, this report must include:

- DHS Barcode
- Acquisition Date
- Acquisition Status
- Asset Condition
- Manufacturer Name
- Manufacturer Model
- Asset Description
- Serial Number
- Asset Cost
- Location

Invoice/Receipts
Contractor will ensure copies of all invoices/packing slips/receipts for property purchased for NPPD accompanies the Monthly Asset Management Report.

Company Information Review Provision

Due to the sensitive nature of the requirements in this solicitation, and the Counterintelligence efforts to support mitigation of the foreign intelligence threat to the Department's supply chain by obtaining a CIR, the Government intends to procure services or supplies from Contractors that are not a national security acquisition risk. The Government reserves the right to award a contract to an offeror that presents a level of acquisition risk, under appropriate arrangements, when the government determines that awarding such a contract is in the Government's interest.

Accordingly, all offerors responding to this solicitation are required to answer the acquisition risk questions located in PART 7, Attachment 7.8. All answers must reference the parent and subsidiary entities of the offeror. In addition, offerors are required to request, collect, and submit to the Government answers to Attachment 7.8 acquisition risk questions for all subcontractors performing services or supplying goods under the awarded contract. Offerors are responsible for the accuracy and completeness of each subcontractor's submission.

After award of the contract, during the period of performance the selected Contractor is under a continuing obligation to ensure that all responses to the acquisition risk questions remain complete, accurate, and up-to-date. The Contractor shall promptly notify and submit updated responses to the CO when any change in circumstances of the Contractor or subcontractors warrants a change in the Contractor's or subcontractor's responses to the acquisition risk questions. In addition, the selected Contractor is under a continuing obligation to promptly disclose to the CO any proposed additional or replacement subcontractors. Failure to comply with these continuing obligations may be grounds for termination for default under the termination clause of this contract.

The Government reserves the right to prohibit individuals who are not U.S. citizens from performing services or

delivering goods under this contract.

Any Offeror who submits a proposal to this RFP acknowledges the Government's requirement for secure services or supplies and the need to assess the offeror's acquisition risk posture. The offeror understands and agrees that the Government retains the right to reject the offeror's proposal, if the Government determines that awarding a contract to that offeror presents an unacceptable risk to national security.

PART 5. INSTRUCTIONS TO OFFERORS

This acquisition will be conducted under the auspices of the DHS Procurement Innovation Lab (PIL). The PIL is a virtual lab that experiments with innovative techniques for increasing efficiencies in the procurement process and institutionalizing best practices. There is nothing you need to do differently for this requirement. The PIL project team may reach out to successful and unsuccessful offerors to assess effectiveness of the procurement process and the innovative techniques applied. The anonymous feedback will be used to further refine DHS procurement practices. Additional information on the PIL may be found here-- https://www.dhs.gov/publication/acquisition-innovations-motion.

5.1 GENERAL INSTRUCTIONS

This RFP is issued under the DHS EAGLE II Strategic Sourcing Contract Vehicles, Functional Category 1 (Unrestricted). Only prime contractors under Functional Category 1 may submit an offer for this requirement. This procurement will be conducted in accordance with FAR 16.505.

The Government intends to break down the proposal process into the following two steps (Paras. 5.1.1 and 5.1.2).

Vendor questions regarding the RFP must be received no later than February 14, 2017 at 5PM ET. Please submit any RFP questions as follows:

- Forward email to: HARTProposalSubmission@hq.dhs.gov. Include "**Vendor Questions**" in the Subject line.

Responses to vendor questions will be released to all EAGLE II, FC 1 vendors on or about February 17, 2017.

5.1.1 STEP 1 – Oral Presentations:

Orals shall begin approximately two weeks after release of the RFP and will conclude based on the number of offers received. The CO will determine the order in which Offerors are scheduled through a random selection process. Requests to reschedule will be at the discretion of the CO. **An Offeror must notify DHS of its intent to submit an offer within two work days after formal release of the RFP (DUE Date/Time, Tuesday, 2/14/17, 5PM ET)**. All notifications of an Offeror's intent to submit an offer shall be accomplished as follows:

i. Offeror shall forward email to: HARTProposalSubmission@hq.dhs.gov. Include **"Intent Notification"** in the Subject line.
ii. Offeror shall provide Name of Offeror, address, and point of contact (email and phone number) with whom you wish DHS to coordinate the oral presentation schedule.

Within one work day of the notification of intent deadline, the Contracting Officer or Contract Specialist will contact the Offeror's POC to provide the schedule date and time of the oral presentation. Subsequently, DHS will provide written confirmation of the schedule in an email to the POC. Location and building access instructions will be provided at that time. Oral presentations will be held in person at a specified location in the Washington, DC metropolitan area.

After the conclusion of the oral presentations, Offerors will receive an advisory notification. Some Offerors determined to have strong oral presentations will receive a notice to proceed with the written proposal. Some Offerors may be advised not to submit a written proposal if it is determined from the oral presentations that the chance for an award is fairly low. The intent of this distinction is to minimize proposal development costs for those Offerors with little or no chance of receiving an award. This will be a recommendation only and discontinuing the pursuit of the requirement following the notification is voluntary. However, in making a decision to proceed regardless of being advised not to continue, an Offeror should note that the Oral Presentation is the most important factor in the overall evaluation (See Part 6.1 Evaluation Factors). Note: If requested, details regarding the basis for the recommendation will not be provided until after award.

Note: Failure to participate in the Oral Presentation precludes further consideration of an Offeror. Written proposals will not be accepted from Offerors who have not completed an Oral Presentation.

5.1.2 STEP 2 – Written Proposals:

For the written part, Offerors are required to submit **two separate volumes** in response to this solicitation: a *Technical Volume* and a *Business Volume* in accordance with the instructions below.

All **written** offers shall be submitted electronically by the date, time and to the email address, below:

Proposal Due Date: Approximately four (4) weeks after an advisory notification (*actual due date will be provided in advisory notification*).
Deliver to: HartProposalSubmission@hq.dhs.gov

In the "Subject" line for the written proposal, include the **Solicitation HSHQDC-16-R-00080**. For proposals exceeding 7 MB, it is recommended that the Offeror submit multiple emails. When submitting multiple emails, Offerors shall identify the number of emails following the solicitation number in the "Subject" line as follows: Email 1 of 3, Email 2 of 3, etc.

In the *Body* of the email, Offerors shall include the following:

- Name of Offeror
- Email contents/list of attachments
- Offeror Point of Contact (name, phone number and email address) for any questions regarding submission.

The Government is not obligated to review or evaluate any offer due to the Offeror's failure to submit an offer to the appropriate email address and/or by the date and time specified above. An offer determined to be late may be eliminated from further consideration.

The government will not be obligated to pay any pre-award costs incurred by the offeror in preparing a response to this solicitation.

Marking Proprietary Information: Any proprietary data included in Offerors' proposals shall be clearly identified. Each page that contains proprietary data shall be marked CONTRACTOR PROPRIETARY at the bottom of the page. The title page of each proposal volume that contains proprietary data shall also be marked CONTRACTOR PROPRIETARY.

Proposal Formatting/ Print Size: Computer-generated pages shall use Arial or Times New Roman Fonts at twelve points or larger; 10 point Times New Roman Font may be used in presenting tables where the data would otherwise not easily fit onto the page width; and 9 point Times New Roman Font may be used in embedded graphics. Proposal page size shall not exceed 8 1/2" by 11". A page is defined as one printed side of one 8 1/2" by 11" sheet of paper. Drawings may be depicted on a page size of up to 11" by 17" if needed (drawings only). All pages shall be numbered at the bottom of each page *"Page <X> of <Total>"* including appendices and any drawings. All files shall be in Adobe PDF with the exception of the WBS. Offerors must complete the WBS using the template in Attachment 7.3.1 and provide as an .xlsx file.

5.2 FACTOR 1 - Oral Presentation (Step 1)

Through the Oral Presentations, the Government intends to understand the Offeror's proposed solution and its capabilities as it relates to the Government's performance objectives for the new system. Further, these presentations will be used as an opportunity to assess the viability of an Offeror to successfully deliver the HART solution.

Travel costs for the presentation will not be reimbursed.

5.2.1 Oral Presentation Process/ Format/ Instructions:

The Offeror shall arrive at least 20 minutes before the assigned scheduled time for processing and accessing the building. A DHS representative will escort the presenters to the appropriate location. Presentations will begin promptly at the appointed time.

5.2.1.1 Presenters: The Offeror's presentation team is limited to five (5) employees of the Prime Contractor only. Sub-contractors or consultants are not authorized to participate in the oral presentation. The Government requires at least one of the persons in the oral presentation to have a major functional role in the execution of the technical solution being proposed. Each presenter is required to carry and present a valid Government issued ID (e.g., driver's license, passport, etc.).

5.2.1.2 Presentation: Each Offeror will be provided two sets of questions: (1) The first set of questions are contained within the RFP below (see 6.1); and, (2) the second set of questions will be provided the day of the oral presentation. The answers to both sets of the questions will serve as the basis of the Offeror's presentation. Questions in the RFP will allow Offerors to prepare responses in advance of the presentation. For those questions received the day of the presentation, Offerors will be given one hour of preparation time prior to the start of the formal oral presentation.

Oral presentations will be limited to 3 hours, broken down as follows:

a) Preparation (60 minutes) - In addition to pre-released questions, the Government will provide a second set of prepared questions. The presenters will have 60 minutes to prepare.
b) Presentation (90 minutes) – The Offerors will have 90 uninterrupted minutes to conduct a presentation on both the advance questions and those received the day of the presentation.
c) Q&A (up to 30 minutes) – After the 90 minute presentation, the Government will caucus for up to 15 minutes to identify any clarifications it may require to understand the presentations. If needed, the Government will ask any clarification questions of the offering contractor.
d) No exchanges or discussions between evaluators and presenters will be permitted during the preparation and presentation times.

5.2.1.3 Oral Presentation Rules of Engagement –

- Presenter names and their roles in the HART project shall be submitted to the specified Government Point of Contact (POC) at least three (3) business days in advance of the offeror's scheduled oral presentation date (Government will provide POC during presentation scheduling). The presentation team shall be knowledgeable and well versed in all aspects of the Offeror's proposed solution and be able to address all presented material independently of other sources.
- The presentation team may not reach back to any other personnel for assistance during the oral presentation.
- The presentation team may bring no more than four (4) pre-drawn flipcharts (max 27"x34") to use as visual aid to assist its presentation.
- Presenters shall not bring and, are forbidden to use, electronic equipment of any kind after arriving at the presentation site (no laptops, tablets, phones, etc.). The Government will provide secure storage of Offeror's electronic equipment during the preparation, presentation and Q&A times, as well as personal belongings such as handbags, briefcases, etc.
- Offerors shall submit their final presentation reference material (e.g., slides, charts, graphs, diagrams, etc.) in .PDF format via email to both Shannon Ozoria at Shannon.Ozoria@hq.dhs.gov, **and** Robert Degnan at Robert.Degnan@hq.dhs.gov, within 10 business days after release of the RFP for distribution to the Government evaluators and Offeror's presenters on the day of the oral presentation. Submitted presentation reference material is limited to addressing advance questions; each page must clearly indicate which advance question is being addressed. Each presentation package shall include no more than 15 pages total. Each page must be printable on 11"x17" paper or smaller. Each page must be legible. The

Government will provide 5 copies to Offeror's presenters for use during the presentation. There will be no capability to photocopy materials at the oral presentation.

- The Government will provide flipcharts, paper, and writing materials, which may be used as needed, during the presentation. There will be no capability to photocopy at the oral presentation. The Government plans to project the submitted final presentation material on a projection screen.
- All presentation materials will be collected after each oral presentation.
- The Government will provide a conference room and a table of sufficient size to accommodate the Offeror's five personnel.
- Up to two oral presentations will be scheduled per day; one in the morning and one in the afternoon.

Note: The confidence rating earned for the presentation will be based on the oral part of the presentations as well as the submitted reference material, with the oral part of the presentations given significantly more importance than written. The Government reserves the right to, and may video record the oral presentations.

5.3 FACTORS 2, 3, 4, 5 and 6 - Written Proposals (Step 2)

Written proposals shall have a *Technical Volume* and a *Business Volume* in accordance with the instructions below:

5.3.1 Technical Volume Requirements:

The Technical Volume is written and includes documentation required for Factors 2, 3, 4 and 5. The written technical volume shall include the following (page limitations referenced below):

5.3.1.1 FACTOR 2 - System Development and Execution

a) Performance Work Statement (PWS) – Proposed tasks and deliverables in response to the Baseline Performance Objectives (BPO) attached to this RFP. (limit 100 pages)
b) Schedule (limit 5 pages) - A complete and comprehensive schedule that incorporates activities and milestones necessary for the design, development and implementation of Increment 1, Increment 2, and option periods. The activities include, but are not limited to, major acquisition decision events, systems engineering lifecycle reviews, test events, security, training, etc. The project schedule provides for regular delivery of configuration items, utilizing an iterative approach, to satisfy the requirements contained in the BPO.
c) Diagrams (Architecture/Drawings) (limit 10 pages)
d) Management Approach – How the execution of tasks will be managed (limit 5 pages)
e) Quality Assurance Surveillance Plan (QASP) (limit 10 pages)
f) Bill of Materials (pricing not required with technical volume – see BOM requirements for Business Volume, Section 5.3.2, below) (no page limit)

Note: If cloud services are proposed to support your solution, the Offeror shall clearly establish which hardware/software is to be purchased under the proposed BOM and which hardware/software is proposed through a cloud service provider.

5.3.1.2 FACTOR 3 - Resource Analysis

a) Life Cycle Cost WBS Elements (Attachment 7.3.1) – must use WBS template and must return in Excel format (no page limit)
b) Long Term O&M Supplemental Questions (Attachment 7.4) - Response to Questions, limit 10 pages

5.3.1.3 FACTOR 4 - Staffing

a) Staffing Plan (limit 3 pages) - A high level composition of the proposed team, which includes an estimated number of personnel and labor categories. Include brief summary of team(s) and the team(s) relationships and responsibilities in the execution of the planned work.

5.3.1.4 FACTOR 5 – Past Performance

a) Past Performance citations (limit 3 pages) - Provide up to three (3) relevant projects of similar size, scope and complexity to the proposed HART effort within the last five (5) years from the date of this solicitation; either executory or completed. The projects may be of the prime or a key prime subcontractor, but must clearly identify the owner of the project experience. If the reference refers to a subcontractor's experience, a letter of commitment to team with the prime on the subcontractor's letterhead, signed by an individual of the subcontractor's firm authorized to make such a commitment, shall be submitted along with the Past Performance citations. At a minimum, each reference shall include:

- Name of project, duration, and dollar value.
- Client Agency or Company for whom work was performed
- Brief description of project (sufficient to establish relevance of experience to the HART project), and role of prime or subcontractor which clearly identifies the level and type of services performed under the contract.
- Point of Contact (Name, title, current phone number, and current email) familiar with the project and can confirm level and quality of referenced experience and work.

Note: Offerors with no Past Performance of similar size, scope and complexity will receive a "neutral" rating for this factor.

5.3.1.5 Technical Volume File Breakdown:

When submitting the Technical Volume, at a minimum, it is requested that the volume be broken down into separate electronic files within the major headings as follows:

Factor 2 - System Development and Execution
- PWS/ Schedule /Diagrams
- Management Approach
- Bill of Materials
- QASP

Factor 3 - Resource Analysis
- Life Cycle Cost WBS
- Long Term O&M Supplemental Questions

Factor 4 – Staffing
- Staffing Plan

Factor 5 – Past Performance
- Past Performance

5.3.2 Business Volume Requirements:

5.3.2.1 FACTOR 6 – Price

Offerors are required to submit pricing (Factor 6) in accordance with the instructions below. Note that the Government intends to award a hybrid type task order which will include Fixed Price Award Fee (FPAF), Firm Fixed Price (FFP), Time and Materials (T&M) and Cost Reimbursement (CR) CLINS.

5.3.2.2 Pricing Logic

CLIN Structure – The CLIN structure for this requirement is developed to logically parse the cost elements into a

logical framework to manage costs, incentivize performance, and provide a reasonable method to pay for completed work.

There are two FPAF CLINS:

CLIN 0001, Core Biometric Management System, Phase 1, Increment 1, and
CLIN 0008, Post IOC Customer Migration

CLIN 0001 primarily encompasses costs for product development (comprised mostly of labor, but payable based on a successfully completed deliverable), yet the hardware and software used in the product development are payable under a separate CPFF CLIN (HW/SW CLIN 0001B). There is no incentive for the purchase of the equipment associated with the deliverable achieved under CLIN 0001.

CLIN 0008 Post IOC Customer Migration is a fixed price award fee (FPAF) CLIN and is payable upon completion of full customer migration to the HART system (estimated period of performance is 6 months). This migration will coincide with the commencement of Post Deployment Period 1.

CLINS 0001A and 0008A are CLINS set up to accommodate award fee amounts for the corresponding FPAF CLINS (CLIN 0001 and 0008). Offerors may propose an award fee percentage and include the amount on CLINS 0001A and 0008A. The award fee percentage shall be applied to FPAF CLINS, 0001 and 0008, only. Note: Proposed award fees are subject to Government review and acceptance prior to award.

CLIN 0002, Phase IIa, Increment 2 - Production-Scale Multimodal Modality Matching and Fusion is FFP. Similar to CLIN 0001, it primarily encompasses costs for product development (comprised mostly of labor, but payable based on a successfully completed deliverable). CLIN 0002B is HW/SW for Phase IIa, Increment 2 (Production-Scale Multimodal Modality Matching and Fusion) used in the product development and is CPFF.

CLIN 0003 (*Optional CLIN*), Phase IIb, Increment 2, Data Warehouse, is set up similarly to CLINS 0001 and 0002 in that it is comprised mostly of labor. It is also an FFP CLIN. Hardware and software for Phase IIb, Increment 2 is on a separate CPFF CLIN (0003B).

Hardware and software (CLINS 0001B, 0002B and 0003B) is cost plus fixed fee payable at completion and acceptance of an associated deliverable. In other words, multiple separate payments for hardware and software may be proposed by the Offeror, as further explained in the paragraphs below. Hardware and software purchased under this task order under the hardware and software CLINS will be Government owned equipment after the delivery and Government acceptance of the product. To leverage enterprise IDENT software applications, Offerors are to negotiate with licensors directly to obtain the best pricing/terms for such licenses on the open market and include those costs in your proposed cost estimate. However, post-award, the Government reserves the right to substitute any existing enterprise license(s) in lieu of any proposed open-market license on an exact product for product basis.

CLIN 000#C is for hosting and support services provided by the contractor during the phased development and implementation of the related Increments. The Offeror has one of two pricing options for hosting and support services. If it is the intent of the Offeror to propose using the *DHS Data Center* for its hosting solution, the Offeror must complete its pricing on 000#C.**1**. Level 1 services using the DHS Data Center will be provided by a separate DHS contractor, but the Offeror will need to price Level 2 and Level 3 support services under CLIN 000#C.**1**.

If the Offeror proposes Non-DHS hosting, either in a *cloud or a non-DHS data center*, the Offeror shall price and complete CLIN 000#C.2, which requires the Offeror to support Levels 1, 2 and 3 services. This separate CLIN category, 000#C, exists for the Increment development and implementation period only. Further, the Offeror is required to estimate the number of months the service is required and provide a firm fixed monthly price for those services in its offer (FFP CLIN). Once a completed Increment is received and accepted by the Government, the cost of non DHS hosting services shall be included in the Post Deployment CLINS (Periods 1 and 2). If DHS hosting services are proposed as part of the solution, the Offeror shall NOT include a price for the Level 1 support services under CLINS 000#C.1 or the Post Deployment CLINs 1001A.1, 2001A.1, or 2001B.1.

Other ODC's associated with development of Increments 1 and 2 and **not** characterized as hardware/software or

hosting and support services shall be included with the CLINS that include labor calculations and will be paid in accordance with the accepted deliverables.

Post-Deployment Period 1 and Period 2 (Option CLINS – 1001A.1, 1001A.2, 2001A.1, 2001A.2, 2001B.1 and 2001B.2) are firm fixed price (FFP) and payable on a monthly basis. Pricing for these CLINS shall include all costs of maintaining and operating a fully operational Increment(s) in accordance with requirement descriptions of the BPO for the Post Deployment periods, based on the Offerors' proposed hosting approach. CLINS #001A.1 and B.1 shall be completed when the Offeror proposes to utilize DHS hosting services for Level 1 support. CLINS #001.A2 and B.2 shall be completed when the Offeror proposes to host Level 1 services either in the cloud or at a non-DHS data center. Note: It is expected that only Increment 1 will be operational in Post-Deployment Period 1. However, it is expected that both Increments 1 and 2 will be fully operational by the start of Post- Deployment 2.

CLINS 2001B.1 and 2001B.2 Post Deployment 2 for **Data Warehouse,** hosted either in a DHS Data Center or in a Non-DHS Data Center or the cloud**,** are FFP Optional CLINS. In the event that Phase IIb, Increment 2 (CLIN 0003) and one of the optional hosting CLINS 0003C.1 or 0003C.2 are exercised, there will be a need for Data Warehouse Hosting and Support Services during the Post Deployment 2 period. The Offeror shall submit a price with its offer for one of the Data Warehouse Hosting and Support Services CLINS based on the hosting approach the Offeror proposes.

Transition-out (Optional CLIN 0005) is FFP and payable in a one-time lump sum amount and related to the cost of transitioning operations to a succeeding contractor in accordance with the requirements of the BPO.

Legacy Interface Development (Optional CLIN 0006) is a T&M CLIN and payable based on the labor rates and the actual level of effort performed on an individual monthly basis. Total estimated hours for this CLIN is 3,304. This CLIN requires the Offeror to submit backup detail (labor mix and hourly rates for each proposed labor category) on its proposed not-to exceed amount based on a level of effort of 3,304 hours, as provided herein by the Government. Labor rates shall not exceed those approved under the EAGLE II IDIQ contract. Discounted rates are encouraged.

IXM Specification Version Translation (Optional CLIN 0007) is an FFP CLIN and payable in a one-time lump sum amount.

Travel CLINS are Cost Reimbursement CLINS in which authorized travel is reimbursed at cost. Fees, or other charges, are not applicable to this CLIN. For purposes of this solicitation, the Government provides an estimated amount for travel.

NOTE: The Offeror has a number of hosting options for its proposed HART solution in accordance with BPO. The proposed solution may include the use of the DHS data center (a hosting cost that is separate from the proposed task order award amount), commercial cloud services, or a commercial data center (i.e. non-DHS data center). These diverse choices can result in significant variances of the total evaluated prices of the various proposed solutions. As such, to normalize the comparison of prices from one proposed solution to another, DHS will adjust prices based on Offeror's proposed hosting choices. To account for the associated cost of DHS data center hosting and Level 1 managed services, the Government will add an amount of up to $16.2 million per year to the prices proposed in the following CLINS: 0001C.1, 0002C.1, 0003C.1, 1001A.1, 2001A.1 and 2001B.1 to reflect the current estimated yearly cost incurred by the Government for these data center services. This represents up to an additional $1.35 million per month to the monthly price quoted on a prorated basis, proportional to the proposed DHS data center footprint. The referenced CLIN prices will be adjusted by the Government upon review of hosting choices made by the Offeror and the estimated hidden hosting costs of the proposed approach.

5.3.2.3 Individual CLIN Requirements for Submission

A pricing schedule (i.e. SF18) is included in this RFP for key CLINS in the execution of all tasks under the task order. Offerors may provide a further break down of the DHS CLIN structure into sub CLINS in their proposals for CLINS 0001, 0002 and 0003, Phase I/Increment1 and Phase II/Increment 2 (Phases IIa and b). This "sub CLIN" structure shall be based on critical sub component development and deliverable milestones in the overall completion of these major CLIN requirements. These sub CLINS should be non-severable deliverables that can be

validated or tested to prove functionality of the component segment, and as development progresses, collectively with other completed component segments for which they interrelate. Payment for each sub CLIN will be based on proven successful functionality of its operational purpose.

NOTE: All sub CLINS under a particular Increment shall add up to the Increment price on the Pricing Schedule. A separate percentage for award fee is applicable on the FPAF CLINS, 0001 and 0008. The Award Fee CLINS are identified as CLIN *0001**A*** and *0008**A***, accordingly, on the pricing schedule.

Similarly, the Offeror may provide a further break down of Hardware and Software CLINS 0001B, 0002B and 0003B into sub CLINS to parallel the sub CLINS identified by the Offeror as Increment 1 and Increment 2 deliverables. That is, the proposed prices for the hardware and software required to achieve the functionality of the Increment 1 and Increment 2 sub CLINS may be billed accordingly with the sub-increment deliverable schedule. Payment of the CPFF HW/SW sub CLINS will be based on proven successful functionality of associated Increments 1 and 2 deliverables.

CLIN	Type	Description
0001	FPAF	Phase I/Increment 1 Core Biometric Management System: Provide total dollar amount in Price Schedule for all costs associated with the successful completion of Phase I/Increment 1 with the exception of the costs for hardware/software (See CLIN 0001B for Phase I hardware/software). When creating sub CLINS for Increment 1, all sub CLIN prices, when totaled, must equal the total dollar amount in the Price Schedule for Phase I/Increment 1. Provide breakout attachment for all sub CLINS proposed. Include description and pricing for each sub CLIN.
0001A	(Fee)	Phase I/Increment 1 Award Fee (Offeror may propose percentage)
0001B	CPFF	Hardware/Software Phase I/Increment 1: Provide total price in Price Schedule for all costs for hardware/software for this phase. In addition, provide a detailed Bill of Materials (BOM) breakdown for all proposed hardware/software. When creating sub CLINS for HW/SW for Increment 1, all sub CLIN prices, when totaled, must equal the total dollar amount in the Price Schedule for HW/SW for Phase I/Increment 1. Provide breakout attachment for all sub CLINS proposed. Include description and pricing for each sub CLIN.
0001C.1	FFP	Phase I/Increment 1: DHS Hosting and Support Services in DHS Data Center (Levels 2 and 3 Services for portion of solution in the DHS Data Center) - Provide per month cost and estimated number of months for all support services to cover service costs through Increment 1 development period in the DHS Data Center, if applicable.
0001C.2	FFP	Phase I/Increment 1: Non-DHS Hosting and Support Services (Levels 1, 2 and 3 Support) - Provide per month cost and estimated number of months of Non-DHS Hosting Services to cover service costs through Increment 1 development period, if applicable.
0002	FFP	Phase IIa/Increment 2 Production-Scale Multimodal Modality Matching and Fusion: Format instructions are the same as those for Phase I/Increment 1.
0002A		Skip
0002B	CPFF	Hardware/Software Phase IIa/Increment 2: Format instructions are the same as those for HW/SW Phase I/Increment 1.
0002C.1	FFP	Phase IIa/Increment 2: DHS Hosting and Support Services in DHS Data Center (Levels 2 and 3 Services for portion of solution in the DHS Data Center) - Provide per month cost and estimated number of months for all support services to cover service costs through Phase IIa, Increment 2 development period in the DHS Data Center, if applicable.
0002C.2	FFP	Phase IIa/Increment 2: Non-DHS Hosting and Support Services (Levels 1, 2 and 3 Support) Provide per month cost and estimated number of months of Non-DHS Hosting Services to cover service costs through Phase IIa, Increment 2 development period, if applicable.

0003	FFP	Phase IIb/Increment 2 Data Warehouse *Optional CLIN*: Format instructions are the same as those for Phase I/Increment 1.
0003A		Skip
0003B	CPFF	Hardware/Software Phase IIb/Increment 2 Data Warehouse *Optional CLIN*: Format instructions are the same as those for HW/SW Phase I/Increment 1.
0003C.1	FFP	Phase IIb/Increment 2 Data Warehouse *Optional CLIN*: DHS Hosting and Support Services in DHS Data Center (Levels 2 and 3 Services for portion of solution in the DHS Data Center) - Provide per month cost and estimated number of months for all support services to cover service costs through Phase IIb, Increment 2 development period in the DHS Data Center, if applicable.
0003C.2	FFP	Phase IIb/Increment 2 Data Warehouse *Optional CLIN*: Non-DHS Hosting and Support Services (Levels 1, 2 and 3 Support) Provide per month cost and estimated number of months of Non-DHS Hosting Services to cover service costs through Phase IIb, Increment 2 development period, if applicable.
0004	CR	Travel Increments 1 and 2: NTE $305,000
0005	FFP	Transition-Out (*Optional CLIN*)
0006	T&M	Legacy Interface Development (*Optional CLIN*)
0007	FFP	IXM Specification Version Translation (*Optional CLIN*)
0008	FPAF	Post IOC Customer Migration
0008A	(Fee)	POST IOC Customer Migration Award Fee (Offeror may propose percentage)
1001A.1	FFP	Option 1 Post Deployment Period 1: DHS Hosting and Support Services in DHS Data Center Price per month (all labor, service and hosting charges and materials included) (12 months) – Does not include non-DHS hosting services.
1001A.2	FFP	Option 1 Post Deployment Period 1: Non-DHS Hosting Services *(Optional CLIN)*: Price per month (All costs non-DHS hosting services only) (12 months)
1002	CR	Option 1Travel: NTE $150,000
2001A.1	FFP	Option 2 Post Deployment Period 2: DHS Hosting and Support Services in DHS Data Center Price per month (all labor, service charges and materials included) (12 months) – Does not include Data Warehouse DHS hosting services (See 2001B.1)
2001A.2	FFP	Option 2 Post Deployment Period 2: Non-DHS Hosting and Support Services for Data Warehouse *(Optional CLIN)*: Price per month (12 months) - Does not include Data Warehouse non-DHS hosting services (See 2001B.2).
2001B.1	FFP	Option 2 Post Deployment Period 2: DHS Hosting and Support Services in DHS Data Center for Data Warehouse *(Optional CLIN)* - Price per month (All labor, service charges and materials costs for Data Warehouse only) included) (12 months).
2001B.2	FFP	Option 2 Post Deployment Period 2 Non-DHS Hosting and Support Services for Data Warehouse *(Optional CLIN)*: Price per month (All labor, service charges, and materials for Data Warehouse non-DHS hosting services only) (12 months).
2002	CR	Option 2 Travel: NTE $150,000

5.3.2.4 Other Business Volume Submissions

- *Subcontracting Plan* (Large Businesses Only): Large businesses responding to this RFP are required to submit a Subcontracting Plan with their proposals. Subcontracting requirements and goals are applicable for this task order in accordance with the controlling IDIQ (Small Business Subcontracting Goal 40%).

A large business which fails to submit an acceptable subcontracting plan with its proposal may be eliminated from further consideration for award. (See 3052.219-70, Small Business Subcontracting Plan Reporting)

- *Organizational Conflict of Interest*: Complete and return Provision HSAR 3052.209-72, Organizational Conflict of Interest (see Part 4 of the RFP). Provide any additional required documentation related to this issue, as deemed necessary.

- *Data Rights Notices:* In accordance with Data Rights clause FAR 52.227-14- Rights in Data (See Part 4 of the RFP).

- *Data Rights Representation*: In accordance with Data Rights provision FAR 52.227-15, Representation of Limited Rights Data and Restricted Computer Software (See Part 4 of the RFP).

- *Government Approved Purchasing and Accounting Systems:* Provide evidence of Government approved purchasing and accounting systems. If you have an approved purchasing system, provide the POC information of the representative at your Cognizant DCMA or Cognizant Federal Agency (CFA) that determined approval; and a copy of the Contractor Purchasing System Review (CPSR) report, if available, and/or a copy of the official letter from DCMA or CFA verifying the approval of the purchasing system.

- *Negotiated Licenses Terms and Conditions for Proposed Software*: For any software proposed for use within the offeror's solution, the offeror shall provide an accompanying software license agreement. Any software license agreements provided with the offeror's proposal as required by this RFP must not contain any terms and conditions that are contrary to federal law or are not in the best interest of the Government. While the Government has highlighted 10 common areas that the Government cannot agree to, other terms and conditions that may be problematic may exist (See Attachment 7.5). Therefore, it is incumbent upon the offeror to negotiate those terms and conditions changes with the software provider prior to the submission of the offeror's written proposal. The Government will not advise offerors on what terms and conditions must be changed in each license prior to the submission of written proposals. The Government suggests that offerors consult with their legal counsel to ensure that any terms and conditions contained in the required license agreements do not contain terms and conditions that are contrary to federal law.

- *Company to Company NDA:* Proprietary Information: The Government will be utilizing non-federal employees for administrative and/or technical assistance. All contractor support will sign non-disclosures with the Government. All Offerors planning on submitting a proposal to this solicitation are required to submit a completed company-to-company agreement. The Offeror shall provide copies of completed "company-to-company" NDA agreements with MITRE and Tecolote to be forwarded with the Offeror's written proposal in the Business Volume. A copy of the company-to-company agreement and instructions on how to fill out the form can be directly obtained from the Government support service provider. The firm and a POC is identified below:

  Name of Company: MITRE
  Company POC: Wendell "Delle" Wright or September O'Brien
  Address: MITRE 1 Building, 7525 Colshire Drive, McLean, VA 22102-7539
  Tel. No. 703-983-0090 (Mr. Wright) or 703-983-5184 (Ms. O'Brien)
  Email: wwright@mitre.org or slobrien@mitre.org

  Name of Company: Tecolote Research, Inc.
  Company POC: Elizabeth Hawes
  Address: 420 S. Fairview Ave, Suite 201, Goleta, CA 93117
  Tel. No.805-571-6336 x126
  Email: ehawes@tecolote.com

- *Acquisition Risk Questions:* Provide completed Acquisition Risk Question form(s) (See Attachment 7.8)

- *Proposal Point of Contact* (name, title, phone number, email).

5.3.2.5 Business Volume Instructions (No page limit):

Offerors shall:

- Complete and submit enclosed Pricing Schedule (i.e. SF18) and provide backup information in accordance with individual CLIN instructions in the table above.
- Submit BOM with pricing for each item in clear, legible format.
- Complete and return Offeror's response to Provision HSAR 3052.209-72, Organizational Conflict of Interest (See Part 4 of the RFP).
- Submit Subcontracting Plan (Large businesses only).
- Submit Data Rights Notices, as required.
- Submit Negotiated License Terms and Conditions for Proposed Software (See Attachment 7.5)
- Provide proposal Point of Contact (name, title, phone number, and email).
- Provide copies of "*company to company*" non-disclosure agreements (See 5.3.2.7, Contractor Support (Company to Company) below)

5.3.2.6 Business Volume File Breakdown:

When submitting the Business Volume, it is requested that the volume be broken down into separate electronic files as follows:

- Pricing information (Pricing schedule and backup, BOM, OCI response, company to company NDA, POC).
- Subcontracting Plan, if required.
- Data Rights Notices, if required.
- Negotiated License Terms and Conditions for Proposed Software

PART 6. EVALUATION FACTORS AND BASIS OF AWARD

6.1 EVALUATION FACTORS

The evaluation will be based on an integrated assessment of the information submitted in the Offeror's proposal and other evaluation information available to the Government. The integrated assessment of proposals will include a risk assessment of the overall proposal.

Award will be made on a determination of Best Value. The non-Price Factors, when combined, are significantly more important than the Price Factor. Factors 1, 2, 3, 4 and 5 are in descending order of importance.

6.1.1 FACTOR 1 – Oral Presentation (Only advance questions are identified below. On-the-spot questions will be provided on the day of the scheduled presentation.)

Offerors will be evaluated on a confidence scale based on responses to the following advanced questions as well as the on-the-spot questions.

- Discuss the major tradeoffs that had to be resolved in coming up with your specific proposal, including consideration and value proposition for innovations. Do not simply discuss general engineering tradeoffs.
- Discuss your proposal's approach to biometric matching and how that approach will facilitate the implementation of future advances in biometric matching technology.
- Describe the overall technical solution. Please describe how the solution components will work together, how the key HART business capabilities will be executed by the solution, and how the transition from IDENT to HART will occur.
- Given your proposed technical solution, how will it reduce long-term system operations and maintenance cost growth.

6.1.2 FACTOR 2 – System Development and Execution

- Architecture Principles - Does the proposed system architecture avoid dispersing business rules processing among multiple components? Has the offeror achieved an optimal distribution of functionality between COTS/GOTS open source and customer development components? To what degree of viability does the offeror demonstrate that the architecture will leverage new approaches to ensure system scalability and performance in a cost effective way? To what degree of viability does the offeror demonstrate that the architecture will facilitate the insertion of new technologies, designed to improve the accuracy, reliability and cost effectiveness of biometric and biographic services? Will this enhance the ability to provide new and/or improved capabilities to its customer base in a timely manner? Is separation of concerns and abstraction applied to apportion system functionality in a way that minimizes the impact of system changes? Will the system be flexible enough to operate in an environment with changing customer requirements (post-HART deployment)? To what degree does the offeror show that, because of this modular design, a new customer/stakeholder could be on-boarded relatively quickly and that SLA business rule settings would not require extensive testing and configurations throughout the HART system? Are all components and their internal and external interfaces identified and described appropriately. Does the architectural approach minimize unnecessary complexity? Has the offeror provided specifications that allow to determine whether desired performance and capacity objectives can be obtained? To what degree of viability does the offeror demonstrate that the architecture will enable the correlation of facts and encounter information that pertain to a biometric identity? To what degree of viability does the offeror demonstrate that the architecture will virtually eliminate scheduled and unscheduled downtime? To what degree of viability does the offeror demonstrate that the systems and components are arranged into a layered architecture with each layer providing specific functional software, partitioned to achieve operational capabilities based on services? Does the architectural approach standardize hardware and software to the maximum extent? Does the proposal describe all architectural/design tradeoffs?
- Data Management - To what degree of viability does the offeror provide both proactive and reactive data quality controls to identify bad data and remediate it? Does the proposal explain how data will be

partitioned to enhance application's performance, manageability and availability? Does the proposal contain a model driven database development approach? Does the proposal address data retention objectives in a way that minimizes ad-hoc processing? Does the proposal show how to maintain the integrity of the relationship between biometric templates and the images from which they derive? Does the proposal provide a front-end solution for browsing, querying and reporting warehouse data that include display interfaces, analysis tools and query functionalities? Does the proposal provide for data integration, ETL functionality, data quality checks, metadata management and Data Warehouse administration?

- Biometric Matching - To what degree of viability does the offeror demonstrate the matching subsystem will achieve accuracy levels in matching biometric modalities listed in BPO? To what degree does the offeror demonstrate their understanding of the integration required to continue operations of existing fingerprint comparison software and workflows? To what degree does the offeror demonstrate their understanding of the integration required to continue operations of the latent sub-system? To what degree does the offeror demonstrate their understanding of the integration required to continue operations of the Secondary Inspection Tool? To what degree does the offeror demonstrate a willingness to leverage multiple modalities to ensure the highest accuracy possible given the varied quality of both the submitted biometric images and the enrolled galleries? To what degree does the offeror demonstrate a willingness to apply fusion techniques within a single modality? Is the proposed matcher interface flexible enough to allow integration of a new matcher subsystems or algorithm with minimal impact on the biometric integration tier? To what degree of viability does the offeror demonstrate that the infrastructure proposed for the matching tier will meet performance and maintenance requirements in a cost-effective way? Will the matching subsystem scale both horizontally to gallery size and vertically to service requests? To what degree of viability does the offeror demonstrate the matching tier provides specific functionality, e.g., quality checking, segmentation, template conversion, enrollment, identification, verification, single modality fusion, and multiple modality fusion? To what degree does the offeror minimize the use of proprietary information or values to allow for future integration or migration to/from different matching vendors?
- Performance Test Environment - Has the Offeror demonstrated the proposed performance test environment design achieves the objectives and requirements as stated in the Baseline Performance Objectives (BPO) and Functional Requirements Document (FRD)? Does the proposed solution utilize a highly virtualized system infrastructure in order to reduce foot print and overall operational costs? Is the proposed solution de-coupled from the production environment and does it duplicate its architecture? To what degree does the offeror demonstrate an understanding of the need for a Performance Test Environment (PTE) to evaluate the throughput and accuracy of the system? Is there a plan to combine real matching capability with simulated matching to deliver a cost effective PTE solution? To what degree does the offeror propose a PTE with the flexibility to both replicate the production system and also test new thresholds, matcher configurations and vendors?
- Security - Is the architectural approach consistent with defense in depth principles? Are internal and external interfaces appropriately secured? Are the appropriate security standards, methods and tools adopted and inserted in the system architecture? Is a balance achieved between security and usability and ease of maintenance?
- Transition to Production - Does the proposal lay out a plan with the appropriate timelines, artifacts and risks to migrate the IDENT data and system functionality to the new HART system? Does the proposal provide appropriate details on how the processing will be switched to the new system including all temporary scaffolding and infrastructure?
- Product Delivery - To what degree of viability does the offeror demonstrate the hardware and infrastructure software procured as part of HART and intended to be installed in DHS facilities will be delivered to one or both of the DHS Enterprise Data Centers (EDCs) for installation by the EDC support contractor? To what degree of viability does the offeror demonstrate that custom developed software (including all auxiliary applications and tools used in development, testing or data conversion) is clearly identified along with delivery methodology and version control? To what degree of viability does the offeror demonstrate that change management will occur via a controlled, mature, systematic and consistent process? To what degree of viability does the offeror demonstrate that in conjunction with the

production implementation of HART, there will be a transfer of knowledge at the end of each period of performance, to include an end of contract transition out approach, from the development contractor to OBIM and to one or more OBIM-designated contractors and/or Government personnel?

- Testing - Has the offeror proposed a technically and programmatically sound approach to the planning and conduct of all testing activities? To what degree is the proposed testing methodology comprehensive, objective, relevant and measurable? To what extent is the performance test strategy sufficient in scope to yield statistically significant results? Does the proposal include a realistic way to test system performance in the absence of a full performance test environment? To what extent has the offeror demonstrated a sound technical approach to analyzing and extrapolating the results of performance testing on a scaled environment? Is the testing approach comprehensive enough to verify readiness and compliance with the HART system requirements? To what degree has the offeror proposed a suite of tools, including test automation tools, that fully supports their test approach? Does the testing process ensure test coverage and include the insertion of corner cases to assess system behavior at boundary conditions? Does the testing approach include a way to realistically test the security attributes of the system? Is the proposed test environment architecture appropriate and does it provide the flexibility for testing with service virtualization or within a cloud environment? To what degree does the offeror demonstrate their ability to support integration testing with multiple stakeholders with varying degrees of participation?
- Design Quality - To what degree does the Offeror demonstrate willingness to design a system specific to DHS needs? Do the components and functions listed show a creative approach to the large scope and scale of DHS biometric operations as opposed to outdated, single-function traditional biometric systems? To what degree does the offeror demonstrate a willingness to leverage the latest IT advancements and best practices to deploy a technical forward-looking solution? To what degree does the offeror demonstrate an understanding of the challenges present within the DHS biometrics mission space? To what degree does the offeror demonstrate an understanding of the legacy systems operational and non-operational environments and service requirements, to include systems, databases, infrastructures, networks and end-user environments?
- Management Approach - The proposal demonstrates a thorough understanding of the requirements contained in the BPO. The proposal describes the management processes and procedures that will be used in managing the work efforts to accomplish the requirements specified in the BPO. The offeror has provided a definitive and comprehensive approach to managing a development project equivalent to Capability Maturity Model Integration (CMMI) for Development Maturity Level 3 or higher to include but not limited to risk management, configuration management, quality management, and requirements management to allow for effective and efficient program/project management. The approach includes adherence and coordination with the requirements of system engineering lifecycle activities, documentation, pre-review and review cycles and gates.
- Schedule - The proposal includes a complete and comprehensive schedule that incorporates activities and milestones necessary for the design, development and implementation of Increment 1, Increment 2, and option periods. The activities include, but are not limited to, major acquisition decision events, systems engineering lifecycle reviews, test events, security, training, etc. The project schedule provides for regular delivery of configuration items, utilizing an iterative approach, to satisfy the requirements contained in the BPO.
- Innovation – The proposal describes three (3) innovations and their value propositions in your proposed technical approach, including how such innovations will increase customer value.

6.1.3 FACTOR 3 – Resource and Analysis

- WBS – Life Cycle Costs - Assessed based upon traceability between the two typologies and consistency of cost data in the two formats. Each structure should be a consistent variation, or view, of the same scope, schedule and resource approach proposed by the vendor.
- Long term O&M analysis - Assessed against the offeror's corresponding technical response to evaluate the reasonableness of the resources proposed to accomplish the actions proposed in the project plan and schedule. (Reference Attachment 7.4)

6.1.4 FACTOR 4 – Staffing

- Staffing - The Government intends to evaluate the extent to which the proposal documents an efficient and well-structured project management organization with clear lines of authority that provides a realistic and achievable staffing plan for satisfying the requirements of the BPO; the proposal demonstrates the incorporation of subcontractors and partners in the staffing plan; and the staffing plan identifies a skill mix with the appropriate level of knowledge and experience for successful execution of the task order requirements.

6.1.5 FACTOR 5 - Past Performance

- Past Performance – The Offeror's past performance submission demonstrates successful management of projects of similar size, scope and complexity as identified in the BPO within the last five years.
- The Offeror demonstrates past experience in designing, developing, testing, integrating, deploying and supporting large-scale information technology transactional systems including those involving integration with legacy systems currently in operation. The past performance indicates applicable experience with the methodologies, tools and technologies proposed for executing the work in the BPO.
- The Offeror demonstrates past experience in incremental iterative development and deployment of configuration items, to include training execution, database updates and restructuring, and configuration management of multiple configurations in various stages of development and deployment.
- Offerors who lack past performance in response to the requirements contained in the RFP will be given a neutral rating for the past performance indicators.

Note: The Government reserves the right to incorporate past performance information from commercial and Government sources and databases in its final rating determination for this factor. These sources may include, but are not limited to, Government audit reports, the Contractor Performance Assessment Reporting System (CPARS), the Past Performance Information Retrieval System (PPIRS), and commercial sources (such as Dun and Bradstreet Reports). In the event other sources conflict with the Offeror's past performance information, the Offeror will be given an opportunity to address the inconsistencies.

6.1.6 FACTOR 6 – Price

Price will be evaluated for reasonableness based on competition and WBS analysis that supports the Offeror's proposed HART PWS.

Due to the potential need of comparing pricing of diverse solutions, pure bottom line pricing comparisons among all proposed solutions provide challenges in determining the reasonableness of pricing solely on the comparison of one total priced offer to another. The Offeror has a number of hosting options for its proposed HART solution in accordance with the BPO. The proposed solution may include the use of the DHS data center (a hosting cost that is separate from the proposed task order award amount), commercial cloud services, or a commercial data center. These diverse choices can result in significant variances of the total evaluated prices of the various proposed solutions. As such, to normalize the comparison of prices from one proposed solution to another, DHS will adjust prices based on vendor hosting choices. To account for the associated cost of DHS data center hosting and Level 1 managed services, the Government will add an amount of up to $16.2 million per year to the prices proposed in the following CLINS: 0001C.1, 0002C.1, 0003C.1, 1001A.1, 2001A.1 and 2001B.1 to reflect the current estimated yearly cost incurred by the Government for these data center services. This represents up to an additional $1.35 million per month to the monthly price quoted on a prorated basis, proportional to the proposed DHS data center footprint. The referenced CLIN prices will be adjusted by the Government upon review of hosting choices made by the Offeror and the estimated hidden hosting costs of the proposed approach.

6.2 EVALUATION METHODOLOGY

6.2.1 Factors (Technical)

The evaluation of each Factor will be done holistically with a rating scale from "*high confidence"* to "*some confidence*" to "*low confidence*." Further, the bulleted indicators or questions under each Factor are not listed in any specific order of importance because an assessment of "confidence" will be made on the totality of each Factor and not based on any individual indicator or question. To receive a rating of "high confidence" the overall submission under a factor must

clearly support the expectation that the Offeror can successfully meet and deliver the BPO requirements. For example, a proposed superior "management approach" under Factor 2 cannot offset an unworkable or flawed technical solution to secure a higher confidence rating. If the totality of the technical submission and the weakness of any indicator does not lead to a successful and functional outcome determination as it relates to the BPO, a low confidence rating is likely. A rating of "*some confidence*" on a technical factor indicates that the Offeror's submission for that factor in total represents a determination by the evaluation team that there is a reasonable expectation that the Offeror has demonstrated its ability to successfully meet the functional and schedule requirements of the BPO.

6.2.2 Factor (Price)

There will be no "confidence" rating for Price. Price will be factored in a best value determination based primarily on competition. However, due to the potential variations in solutions that each Offeror may propose to meet the BPO, a determination of "reasonableness" as it relates to the Offeror's overall proposed solution is also required to be considered for award. The Government reserves the right to utilize the WBS submission or any other proposal information received from the Offeror to assist the Business Team in making a determination of reasonableness. The total evaluated price for purposes of award will be determined by:

1. The total calculation of all CLINS, including options, as identified in the Price Schedule, and
2. The total value of 6 months of Post Deployment 2 to accommodate the estimated value of support services under FAR clause 52.217-8, Option to Extend Services, in the event it is exercised.
3. Adjustments to Offers to normalize the impact of proposal options on the issue of government vs. non-Government hosting. See referenced CLINS under Factor 6, Price, above.

6.3 BASIS OF AWARD

6.3.1. Fair Opportunity

This RFP is conducted under the fair opportunity guidelines of FAR 16.505, which outlines the ordering procedures for orders issued under Multiple Award Indefinite Delivery Indefinite Quantity contracts. Award will be based on a determination of best value to the government, price and non-price factors considered. "Best value" means the expected outcome of an acquisition that, in the government's estimation, provides the greatest overall benefit in response to the requirement. Best value evaluation is, in and of itself, a subjective assessment by the government of the proposed solution that provides the optimal results to the government.

This method does not use any aspects of FAR subpart 15.3. The use of this fair opportunity process does not obligate the government to determine a competitive range, conduct discussions with any contractors, solicit proposals or revisions thereto, or use any other source selection techniques associated with FAR subpart 15.3.

6.3.2. Comparative Analysis

Following receipt of responses (including oral presentations), the government may perform a comparative analysis (comparing contractor responses to one another) to select the contractor that is best suited to fulfill the requirements, based on the contractors' responses to the factors outlined in this RFP and their relative importance.

6.3.3. Award on Initial Responses

The government anticipates selecting the best-suited contractor from initial responses, without engaging in exchanges with contractors. Contractors are strongly encouraged to submit their best technical solutions and price in response to this RFP.

6.3.4. Exchanges with Best-Suited Contractor

Once the government determines the contractor that is the best-suited (i.e., the apparent successful contractor), the government reserves the right to communicate with only that contractor to address any remaining issues, if necessary, and finalize a task order with that contractor. These issues may include technical and price. If the parties cannot successfully address any remaining issues, as determined pertinent at the sole discretion of the government, the government reserves the right to communicate with the next best-suited contractor based on the original analysis and address any remaining issues. Once the government has begun communications with the next best-suited contractor, no further communications with the previous contractor will be entertained until

after the task order has been awarded. This process shall continue until an agreement is successfully reached and a task order is awarded.

6.4 OTHER CONDITIONS FOR AWARD

- Only proposals received from EAGLE II, FC1, Unrestricted vendors will be considered for award.

- **Subcontracting Plan:** For large businesses, an acceptable Subcontracting Plan is required. "Acceptability" of a Subcontracting Plan will be made by the Contracting Officer in accordance with the subcontracting goals and objectives stated in the Offeror's EAGLE II IDIQ contract. A large business which fails to submit an acceptable subcontracting plan with its proposal may be eliminated from further consideration for award. (See 3052.219-70, Small Business Subcontracting Plan Reporting)

- **Software Licensing:** The Government will review the offeror's provided software license agreements and review the terms and conditions to ensure that no terms and conditions are contrary to federal law. If the license agreements contain terms or conditions that are contrary to federal law, the offeror may not receive an award.

- **Acquisition Risk Assessment:** The Government will review the Offeror's response to the Acquisition Risk Questions (See Attachment 7.8) to determine if the Offeror has proposed the use of services, or the incorporation of supplies, that present a national security acquisition risk. If it is determined by the Government that the offeror presents a solution, through the proposed services or supplies, with an unacceptable risk to national security, the Government retains the right to reject the Offeror's proposal.

Note: In addition to Government personnel, the Government intends to utilize contractor personnel from Tecolote Research, Inc. as well as The MITRE Corporation, a Federally Funded Research and Development Center, (FFRDC) as technical advisors in support of the HART system source selection. Technical advisors will assist in a non-voting capacity and shall be prohibited from proposal rating, ranking, or recommending the selection of a source. All non-Government support personnel are required to sign a Non-Disclosure Agreement (NDA) with the Government. All Offerors planning on submitting a proposal to this solicitation are required to secure a completed "company-to-company" NDA agreement with Mitre and Tecolote. Copies of such agreements should be forwarded with the Offeror's written proposal in the Business Volume.

PART 7. LIST OF ATTACHMENTS

7.1 Reading Room Information

- 7.1.1 Reading Room Instructions
- 7.1.2 Reading Room Documents List
- 7.1.3 Reading Room Request Form
- 7.1.4 Notice of Intent to Bid
- 7.1.5 Non-Disclosure Agreement

7.2 Award-Fee Plan

7.3 WBS Information

- 7.3.1 WBS Spreadsheet
- 7.3.2 IDENT O&M Cost Details (Historical Information)

7.4 HART Cost Estimation Questionnaire

7.5 Most Common Commercial Terms Requiring Negotiation

7.6 Sample Performance Work Statement

7.7 Sample Quality Assurance Surveillance Plan

7.8 Company Information Review/Acquisition Risk