Description of document:	Department of Homeland Security (DHS) Privacy Threshold Analyses (PTA) re Homeland Advanced Recognition Technology (HART), 2014
Requested date:	04-July-2018
Release date:	18-April-2019
Posted date:	18-April-2019
Source of document:	FOIA Request Chief FOIA Officer The Privacy Office U.S. Department of Homeland Security 245 Murray Lane SW STOP-0655 Washington, D.C. 20528-0655

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Privacy Office, Mail Stop 0655

April 18, 2019

SENT BY ELECTRONIC MAIL

Re: **2018-HQFO-01201**

This is the final response to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated July 4, 2018, and received by this office on July 5, 2018. You are seeking records regarding: (1) The required PIA conducted for HART; (2) Any Privacy Threshold Analysis or similar initial privacy assessment that assessed the need for a PIA for HART.

A search of the Department of Homeland Security, Privacy Office for records responsive to your request produced 23 pages. After review of those documents, I have determined that 19 pages will be released in their entirety and 4 pages are partially releasable pursuant to Title 5 U.S.C. § 552, (b)(6). FOIA Exemptions 6. Be advised there is currently no PIA at this time, upon completion it will be publicly available.

Enclosed are 23 pages with certain information withheld as described below:

FOIA Exemption 6 exempts from disclosure personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a balancing of the public's right to disclosure against the individual's right to privacy. The privacy interests of the individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

You have a right to appeal the above withholding determination. Should you wish to do so, you must send your appeal and a copy of this letter, within 90 days of the date of this letter, to: Privacy Office, Attn: FOIA Appeals, U.S. Department of Homeland Security, 245 Murray Lane, SW, Mail Stop 0655, Washington, D.C. 20528-0655, following the procedures outlined in the DHS FOIA regulations at 6 C.F.R. Part 5 § 5.8. Your envelope and letter should be marked

"FOIA Appeal." Copies of the FOIA and DHS FOIA regulations are available at www.dhs.gov/foia.

Additionally, you have a right to right to seek dispute resolution services from the Office of Government Information Services (OGIS) which mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. If you are requesting access to your own records (which is considered a Privacy Act request), you should know that OGIS does not have the authority to handle requests made under the Privacy Act of 1974. You may contact OGIS as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

If you need any further assistance or would like to discuss any aspect of your request, please contact the analyst below who processed your request and refer to **2018-HQFO-0201**. You may send an e-mail to foia@hq.dhs.gov, call 202-343-1743 or toll free 1-866-431-0486, or you may contact our FOIA Public Liaison in the same manner.

Sincerely,

James V M L Holzer, I

James Holzer
Department of Homeland Security
Deputy Chief FOIA Officer

Enclosure(s): Responsive Records (23 pages)

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	**Homeland Advanced Recognition Technology (HART) Development Testing Environment (DTE)**		
Component:	National Protection and Programs Directorate (NPPD)	**Office or Program:**	Office of Biometric Identity Management (OBIM)
Xacta FISMA Name (if applicable):	Click here to enter text.	**Xacta FISMA Number (if applicable):**	
Type of Project or Program:	**IT System**	**Project or program status:**	**Update**
Date first developed:	Click here to enter a date.	**Pilot launch date:**	Click here to enter a date.
Date of last PTA update	Click here to enter a date.	**Pilot end date:**	Click here to enter a date.
ATO Status (if applicable)	**In progress**	**ATO expiration date (if applicable):**	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	(b)(6)		
Office:	**OBIM's Identity Operations Division**	**Title:**	System Business Owner
Phone:	(b)(6)	**Email:**	(b)(6)

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	(b)(6)		
Phone:	(b)(6)	**Email:**	(b)(6)

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA

Please provide a general description of the project and its purpose in a way a non-technical person could understand. If this is an updated PTA, please describe what changes and/or upgrades that are triggering the update to this PTA. If this is a renewal please state whether or not there were any changes to the project, program, or system since the last version.

The National Protection and Programs Directorate's (NPPD) Office of Biometric Identity (OBIM), through the Automated Biometric Identification System (IDENT), provides biometric and associated biographic information services to Federal, State, tribal, local and foreign governments and international agencies. IDENT is the central DHS-wide system used for the storage and processing of biometric and associated biographic information for national security, law enforcement, immigration and border management, and intelligence purposes, and is also used to conduct background investigations for national security positions and certain positions of public trust.

HART Increment 1 Overview:

In its mission to provide DHS and its mission partners with enduring identity services that advance informed decision making by producing accurate, timely, and high assurance biometric identity information and analysis, OBIM will replace IDENT with an enhanced, scalable, modular, and multimodal identity management system—the Homeland Advanced Recognition Technology (HART) system. OBIM will deploy this replacement system in four incremental phases (*See Appendix A*).

Increment 1 lays the architectural foundation for the HART system. It implements a new data architecture which includes conceptual, logical, and physical data models, a data management plan, and physical storage of identity data where each identity may have multiple associated biometric modality images. The data and system architecture will be designed for scalability to address the projected growth in identity and image data volumes and to accommodate long term data retention requirements. OBIM will also design and acquire the physical infrastructure for the HART system. OBIM will design the production environment for high availability and for implementation in both of the DHS Enterprise Data Centers in an active-active configuration.

Development Testing Environment:

Increment 1 will include testing environments designed to support developmental and operational testing. Testing will begin in Summer 2018 after HART obtains the Restricted Approval to Connect (RATC) to the IDENT database. This PTA covers the Development Testing Environment (DTE) which consists of the two underlying environments described as follows:

- *Performance Testing Environment (PTE)* – The PTE will include live production data. The data will be encrypted at rest and external users will not have access to this part of the DTE. We will ensure this is logically separated and fully segmented from the rest of DTE.

  DHS has a need for a flexible, cost effective PTE to ensure HART will meet or exceed all IT infrastructure and biometric performance requirements. Initially, the PTE will allow for early validation testing of the HART architecture and the benchmarking of selected biometric matching solutions. The PTE will then be leveraged for controlled tests of each HART release.

The PTE provides test harnesses, test emulators, and representative test data for all external system interfaces.

Vital to the software development lifecycle, performance testing plays a critical role in functional and operational acceptance testing. The HART mission includes numerous stakeholders with differing performance requirements, a non-linear transactional workload, a large storage requirement (due to lossless compression required for biometric images), numerous system-to-system endpoints with varying impacts, and a requirement for a large amount of compute infrastructure. These elements of the HART mission create challenges to accurately predicting operational performance that can only be mitigated by a permanent and fully functioning PTE.

The PTE, delivered as part of Increment 1, will be capable of stressing the HART application and biometric services prior to deployment in the production system. The PTE will provide confidence that the HART system and application meet the required performance metrics. Through implementing simulators and emulators, our PTE generates the workload and workflows of the production system accurately mimicking the production system. The architecture of the PTE also mimics the production system to ensure the behaviors across the two systems are indistinguishable. The PTE will be hosted in the AWS GovCloud region along with the non-production and production environments. Built from identical virtual hardware components deployed in the HART production environment, the PTE accurately represents the production system on a scaled level.

- *Non-Production Environment (NPE)* – The NPE will include synthetic and masked production data, similar to what currently use in the IDENT NPE environment.

  The HART NPE will provide a test system to develop, implement, maintain, and enhance the HART Production Environment (PE) application. The NPE will implement a test automation framework integration that includes testing tools, programming interfaces, protocols and procedures enabling the automated management of testing activities. HART NPE will allow customer systems to connect, if required, for testing and customer training purposes. The infrastructure will include each type of biometric matching subsystem with the capability of supporting a gallery containing up to 2 million identities. The NPE testing infrastructure will allow development and testing environments to be provisioned in response to on-demand and self-service requests.

  The NPE will not contain or interface with production data (also known as, “live data”) and is used primarily for the testing and development for HART. HART stakeholders, will however, be able to temporarily interface their systems with testing environments in the NPE to ensure new functionality is compatible with their application or information system.

  In specific circumstances, where synthetic or masked data cannot properly simulate performance scenarios afforded by live data, live data may be used in these environments for testing purposes under guidance by NPPD/OBIM Privacy and Security.

2. Does this system employ any of the following technologies: *If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*	☐ Closed Circuit Television (CCTV) ☐ Social Media ☐ Web portal[1] (e.g., SharePoint) ☐ Contact Lists ☒ None of these

3. From whom does the Project or Program collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This program does not collect any personally identifiable information[2] ☒ Members of the public ☒ DHS employees/contractors (list components): ☒ Contractors working on behalf of DHS ☒ Employees of other federal agencies

4. What specific information about individuals is collected, generated or retained?

Please provide a specific description of information that is collected, generated, or retained (such as names, addresses, emails, etc.) for each category of individuals.

Data from the existing IDENT system will be transferred over to the HART in Increment 1. Biometric data includes but is not limited to fingerprints, iris scans, and facial images. Associated biographic data includes but is not limited to name, date of birth, nationality, and other personal descriptive data. Encounter data provides the context of the interaction with an individual including but not limited to location, Alien Registration Number (A-Number), document numbers, and/or reason information collected. Test data may be real or simulated biometric, associated biographic, or encounter-related data.

Information is retained in accordance with the existing NARA retention schedule.

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

4(a) Does the project, program, or system retrieve information by personal identifier?	☐ No. Please continue to next question. ☒ Yes. If yes, please list all personal identifiers used: Records may be retrieved by any of the personal identifiers that are mentioned in the IDENT System of Records Notice (SORN), including biometrics. The most common identifiers used to retrieve records are the Fingerprint Identification number (FIN) and the Encounter Identification number (EID). Because the testing and training environments replicate production functionality, data may be retrieved by the same personal identifiers retrieved by IDENT. The PTE is an enclosed, logically separated, environment and cannot be readily searched by IDENT/HART customers.
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☐ No. ☒ Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	As a data steward, on behalf of other DHS and Federal entities, IDENT stores and maintains SSNs sent by other components. Since the data in the HART/DTE comes from IDENT, it may contain SSNs. No specific testing is done using the SSNs.
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	The only active contributor of SSNs to HART will be USCIS. USCIS may provide SSNs in conjunction with pending and approved work authorizations, as documented on forms such as I-765's.
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header

Click here to enter text.

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☐ No. ☒ Yes. If yes, please list: The PTE is an enclosed, logically separated, environment and cannot be readily searched by IDENT/HART customers. Data in the NPE comes from IDENT. In rare cases, IDENT stakeholders, however, may temporarily interface their systems with testing environments in the NPE to ensure new functionality is compatible with their application or information system.
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	☐ No. ☒ Yes. If yes, please list: The PTE is an enclosed, logically separated, environment and cannot be readily searched by IDENT/HART customers. Data in the NPE comes from IDENT. In rare cases, IDENT stakeholders, however, may temporarily interface their systems with testing environments in the NPE to ensure new functionality is compatible with their application or information system.
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Existing

information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

	Please describe applicable information sharing governance in place: DHS has a number of MOUs and LOIs to allow for sharing with various external stakeholders. This system will be the authoritative biometric repository for DHS.
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	☒ No. ☐ Yes. If yes, please list: N/A
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?	☐ No. What steps will be taken to develop and maintain the accounting: ☒ Yes. In what format is the accounting maintained: OBIM logs tests, studies, and bulk data requests (including fingerprint studies or technical reviews) in accordance with the Department's Computer Readable Extract Policy. In all other cases, OBIM discloses PII to individuals with a need to know, in responses made pursuant to the Freedom of Information Act, or in responses to a law enforcement agency pursuant to 5 U.S.C. § 552a(c)(3).
9. Is there a FIPS 199 determination?[4]	☐ Unknown. ☐ No. ☒ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☒ Moderate ☐ High ☐ Undefined Integrity:

[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

	☐ Low ☒ Moderate ☐ High ☐ Undefined Availability: ☐ Low ☒ Moderate ☐ High ☐ Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b)(6)
Date submitted to Component Privacy Office:	**March 1, 2018**
Date submitted to DHS Privacy Office:	May 15, 2018
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	
SORN: Since the data stored and shared remains the same, NPPD/OBIM believes that the current IDENT SORN, *DHS/USVISIT-004 - DHS Automated Biometric Identification System (IDENT) June 5, 2007, 72 FR 31080,* will cover the HART DTE environment during this period. External biometric collections will be covered by the External Biometrics (EBR) SORN pending the public comment period in the Federal Register. **PIA**: HART is a privacy sensitive system and a new PIA will be required. OBIM/NPPD Privacy is working to complete a HART PIA prior to the anticipated ATO in January, 2019.	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6)
PCTS Workflow Number:	**1163365**
Date approved by DHS Privacy Office:	May 16, 2018
PTA Expiration Date	May 16, 2019

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.
Category of System:	IT System If "other" is selected, please describe: Click here to enter text.
Determination:	☐ PTA sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☐ Privacy Act Statement required. ☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required. ☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. ☐ A Records Schedule may be required. Contact your component Records Officer.
PIA:	**New PIA is required.** If covered by existing PIA, please list: New HART PIA
SORN:	New SORN is required. If covered by existing SORN, please list: DHS/ALL-041 External Biometric Records (EBR) System of Records, April 24, 2018, 83 FR 17829; Forthcoming TRACS SORN

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

OBIM Privacy is submitting this PTA because OBIM will replace IDENT with an enhanced, scalable, modular, and multimodal identity management system—the Homeland Advanced Recognition Technology (HART) system. OBIM will deploy this replacement system in four incremental phases.

Increment 1 lays the architectural foundation for the HART system. It implements a new data architecture which includes conceptual, logical, and physical data models, a data management plan, and physical storage of identity data where each identity may have multiple associated biometric modality images.

Increment 1 will include testing environments designed to support developmental and operational testing that will begin in Summer 2018. One of the testing environments, the Performance Testing Environment will include live production data. The data will be encrypted at rest and external users will not have access to this part of the DTE.

The other environment, the Non Production Environment will include synthetic and masked production data, similar to what currently use in the IDENT NPE environment. The HART NPE will provide a test system to develop, implement, maintain, and enhance the HART Production Environment (PE) application. The NPE will not contain or interface with production data (also known as, "live data") and is

used primarily for the testing and development for HART. The DHS Privacy Office finds that is a privacy sensitive system requiring both PIA and SORN coverage because HART collects and maintains SPII on members of the public including biometric data, associated biographic data, and encounter data that will be shared outside of DHS and will be retrieved by personal identifiers. Test data used in the Performance Testing Environment may be real or simulated biometric, associated biographic, or encounter-related data. Due to the large amount of information transferred from IDENT to HART as part of this initiative, and because HART requires live data, an incremental approach to data ingest to ensure that all privacy compliance requirements are met is required.

OBIM Privacy is in the process of developing a new HART PIA prior to the expected ATO in January 2019. Due to reliance on PIA coverage for this test, OBIM cannot send any data external to DHS, without publication of the forthcoming HART PIA (this does not preclude OBIM from use within the AWS-GovCloud).

SORN coverage is provided for the DTE by the DHS-wide External Biometric Records SORN, which covers the maintenance of biometric and associated biographic information from non-DHS entities, both foreign and domestic, for law enforcement, national security, immigration screening, border enforcement, intelligence, national defense, and background investigations relating to national security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities.

Additional SORN coverage will be provided by a new SORN that will be a combination of data elements from both the NPPD/OBIM TRACS SORN, which allows the maintenance of DHS-generated transactional information, such as biometric indicator data and the DHS Automated Biometric Identification System (IDENT) SORN which allows for the repository of biometrics captures in DHS or law enforcement encounters.

Interim SORN coverage is provided by the DHS/USVISIT-004 DHS IDENT SORN, which will be dispositioned upon publication of the new SORN.

The DHS Privacy Office requires a new PTA from OBIM Privacy before Phase 2 of testing.

This PTA will expire in one year due to reliance on PIA and SORN coverage.

APPENDIX A:

Increment 1:
- Core Foundation
- Establishment of Performance Test Environment
- Data Architecture & Data Store Migration
- Biometric Services, Business Workflow, and Business Rules

Increment 2:
- Multimodal Fusion
- Full Performance Test Environment
- Data Warehouse/Data Marts

Increment 3:
- Web Portal
- Person-Centric Services
- Additional Biometric Modalities and Services

Increment 4:
- Identity Management Applications (CVT, SIT replacement)
- Analytics and Reporting Capabilities
- Additional Biometric Modalities

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	**Replacement Biometric System (Increment 1)**		
Component:	**National Protection and Programs Directorate (NPPD)**	**Office or Program:**	**Office of Biometric Identity Management (OBIM)**
Xacta FISMA Name (if applicable):	Click here to enter text.	**Xacta FISMA Number (if applicable):**	Click here to enter text.
Type of Project or Program:	**IT System**	**Project or program status:**	**Development**
Date first developed:	Click here to enter a date.	**Pilot launch date:**	Click here to enter a date.
Date of last PTA update	Click here to enter a date.	**Pilot end date:**	Click here to enter a date.
ATO Status (if applicable)	Choose an item.	**ATO expiration date (if applicable):**	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	(b)(6)		
Office:	**Program Management Cell**	**Title:**	**Deputy Program Manager**
Phone:	(b)(6)	**Email:**	(b)(6)

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	(b)(6)		
Phone:	(b)(6)	**Email:**	(b)(6)

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA

Please provide a general description of the project and its purpose in a way a non-technical person could understand. If this is an updated PTA, please describe what changes and/or upgrades that are triggering the update to this PTA. If this is a renewal please state whether or not there were any changes to the project, program, or system since the last version.

The Department of Homeland Security (DHS) will replace the aging target biometric system, the Automated Biometric Identification System (IDENT), with a new biometric system—the Replacement Biometric System (RBS). The Office of Biometric Identity Management (OBIM) will deploy the replacement system in four incremental phases. This PTA covers the first phase of deployment, known as "Increment 1" which is currently scheduled to be deployed in 3rd quarter of FY 17, OBIM's mission is to provide DHS and its mission partners with enduring identity services that advance informed decision making by producing accurate, timely, and high assurance biometric identity information and analysis. Increment 1 lays the architectural foundation for the entire replacement biometric system.

Biometric matching services will be expanded from the traditional fingerprint matching to include the capability to match additional biometric modalities, specifically iris and facial modalities in the near-term, while designing the framework to add additional modalities in the future. Increment 1 establishes the software capability to perform multimodal biometric matching.

Increment 1 implements a new data architecture which includes conceptual, logical, and physical data models, a data management plan, and physical storage of identity data where each identity may have multiple associated biometric modality images. The data architecture and system architecture will be designed for scalability to address the projected growth in identity and image data volumes and to accommodate long term data retention requirements.

OBIM will also include the implementation of an Online Transaction Processing (OLTP) database; replacement of the current transaction manager with business workflow and business rules management; system software components; initial performance test environment; designated Authentication and Authorization Service (AAS) for IT security; multimodal biometric matching middleware; high availability; initial tiered storage and server consolidation/virtualization; and data migration.

During Increment 1, OBIM will also design and acquire the physical infrastructure for the replacement biometric system. OBIM will design the production environment for high availability and for implementation in both of the DHS Enterprise Data Centers in an active-active configuration. Test environments will be designed to support developmental and operational testing protocol. Testing environments will include a Performance Test Environment that will have storage and processing capacities capable of stressing the application with production-level workloads. OBIM will partially implement the Performance Test Environment in Increment 1.

Lastly, OBIM will reproduce all existing data and IDENT functionality in the Replacement Biometric System.

Subsequent increments will include additional enhancements to the system. These increments are described at a high level below; time frames for implementation are tentative and compliance

documentation will be completed as appropriate for each Increment.

Increment 2 (FY18) - will include iris and facial matchers, multimodal fusion, and a data warehouse and datamart for reporting.

Increment 3 – (FY19 - FY20) - will include a web portal, identity directory, person centric management service, and storage capability for other modalities to include Scars, marks and tattoos and DNA (to accommodate for modalities that DHS Law enforcement agencies may collect.

Increment 4 (FY21) - will include advanced analytics, enhanced reporting, identity management applications and more improved watchlist case management system.

2. Does this system employ any of the following technologies: *If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*	☐ Closed Circuit Television (CCTV) ☐ Social Media ☐ Web portal[1] (e.g., SharePoint) ☐ Contact Lists ☒ None of these

3. From whom does the Project or Program collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This program does not collect any personally identifiable information[2] ☒ Members of the public ☒ DHS employees/contractors (list components): ☒ Contractors working on behalf of DHS ☒ Employees of other federal agencies

4. What specific information about individuals is collected, generated or retained?	
Data from the existing IDENT system will be transferred over to the Replacement Biometric System in Increment 1. A disposition PTA will be completed for IDENT at that time. The Replacement Biometric System will retain biometric, associated biographic, and encounter-related data for operations/production, testing, and training environments. Biometric data includes but is not limited to fingerprints, iris scans, and facial images. Associated biographic data includes but is not limited to name, date of birth, nationality, and other personal descriptive data. Encounter data provides the context of the interaction with an individual including but not limited to location, document numbers, and/or reason information collected. Test data may be real or simulated biometric, associated biographic, or encounter-related data.	
4(a) Does the project, program, or system retrieve information by personal identifier?	☐ No. Please continue to next question. ☒ Yes. If yes, please list all personal identifiers used: Records may be retrieved by any of the personal

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

	identifiers that are mentioned in the IDENT System of Records Notice (SORN), including biometrics. The most common identifiers used to retrieve records are the Fingerprint Identification number (FIN) and the Encounter Identification number (EID).
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☐ No. ☒ Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	Click here to enter text. The authority to collect SSNs is derived from the agencies and systems that are operated and maintained by owners other than OBIM.
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	When provided by collectors in biometric transactions, the replacement biometric system will store the SSN as a unique identifier in the system.
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	
Click here to enter text.	

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☐ No. ☒ Yes. If yes, please list: • U.S. Customs and Border Protection (CBP): o Traveler Primary Arrival Client (TPAC) o E3 Portal o Secure Integrated Government Mainframe Access (SIGMA)

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.
[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

	o Global Enrollment System (GES) o Global Entry (GE) o Automated Targeting System (ATS) o ATS Unified Passenger Module (UPAX) o U.S. Pedestrian Entry o Client applications as managed by CBP Office of Information Technology (OIT) • U.S. Immigration and Customs Enforcement (ICE): o Enforcement Integrated Database (EID) o Immigration and Enforcement Operational Records System (ENFORCE) o EID Arrest Guide for Law Enforcement (EAGLE) • U.S. Citizenship and Immigration Services (USCIS): o Refugees, Asylum, and Parole System (RAPS) o Secure Information Management Service (SIMS) o Background Vetting Service (BVS) o Electronic Fingerprint Image Print Server (EFIPS) o And other immigration applications as submitted by USCIS's Application Support Center(s) through the USCIS Enterprise Service Bus (ESB) • U.S. Coast Guard: o Biometrics at Sea System (BASS) • Transportation Security Administration: o Technology Infrastructure Modernization (TIM) Program • Federal Emergency Management Agency: o Electronic Fingerprint System (EFS) • DHS Management Directorate, Office of the Chief Security Officer (OCSO):

	o Identity Management System (IDMS)
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	☐ No. ☒ Yes. If yes, please list: • Department of State: o Consular Consolidated Database (CCD) • Department of Justice (including State and Local Law Enforcement Agencies): o Federal Bureau of Investigation (FBI) Next Generation Identification (NGI) System o FBI Joint Automated Booking System (JABS) o Terrorist Screening Center Terrorist Screening Database (TSDB) o MyFX Server • Department of Defense: o Automated Biometric Information System (ABIS) o Biometric Identity Intelligence Resource (BI2R) database • Foreign Partners, including but not limited to: o Five Country Conference (FCC) Secure Real-Time Platform (SRTP) o United Kingdom Home Office, UK Visas and Immigration (UKVI) o Virtual Private Networks (VPN) and Secure File Transfer Protocol (SFTP) servers between the United States and Visa Waiver Program/Preventing and Combating Serious Crime (PCSC) Agreement countries
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Existing DHS has a number of MOUs and LOIs to allow for sharing with various external stakeholders. This system will be the authoritative biometric repository

	for DHS.
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	☒ No. ☐ Yes. If yes, please list:
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?	☐ No. What steps will be taken to develop and maintain the accounting: ☒ Yes. In what format is the accounting maintained: OBIM logs tests, studies, and bulk data requests (including fingerprint studies or technical reviews) in accordance with the Department's Computer Readable Extract Policy. In all other cases, OBIM discloses PII to individuals with a need to know, in responses made pursuant to the Freedom of Information Act, or in responses to a law enforcement agency pursuant to 5 U.S.C. § 552a(c)(3).
9. Is there a FIPS 199 determination?[4]	☐ Unknown. ☐ No. ☒ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☐ Moderate ☒ High ☐ Undefined Integrity: ☐ Low ☐ Moderate ☒ High ☐ Undefined Availability: ☐ Low ☐ Moderate ☒ High ☐ Undefined

[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b)(6)
Date submitted to Component Privacy Office:	**March 5, 2015**
Date submitted to DHS Privacy Office:	March 16, 2015
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	
RBS will be operational with data ingest during Increment 1, RBS is a privacy sensitive systems and a new PIA will be required. The new PIA will cover the transfer of data and phase out of the IDENT system. Since the data stored and shared remains the same for both systems, NPPD/OBIM believes that the IDENT SORN will cover both systems during the transfer period. However, the IDENT SORN will require updating once IDENT has been decommissioned.	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6)
PCTS Workflow Number:	**1071655**
Date approved by DHS Privacy Office:	April 3, 2015
PTA Expiration Date	April 3, 2018

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.
Category of System:	IT System If "other" is selected, please describe: Click here to enter text.
Determination:	☐ PTA sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☐ Privacy Act Statement required.

	☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required. ☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. ☐ A Records Schedule may be required. Contact your component Records Officer.
PIA:	**New PIA is required.** If covered by existing PIA, please list: Click here to enter text.
SORN:	SORN coverage TBD If covered by existing SORN, please list: Click here to enter text.

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

PRIV agrees with NPPD/OBIM that a new PIA is necessary before OBIM may launch the Replacement Biometric System. Since Increment 1 is not set be launched for 2 years, and there may be significant changes to the system plans between now and launch, PRIV cannot make a final determination regarding SORN coverage at this time. The RBS will likely receive SORN coverage from the updated IDENT SORN.