PRIVACY IMPACT ASSESSMENT (PIA)

For the

Gatekeeper-on-the-Move-Biometric (GOTM-B) Feasibility Study
Department of the Navy - NAVAIR - 4.5X Special Surveillance Program (SSP)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	**New DoD Information System**	☒	**New Electronic Collection**
☐	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☐	**Yes, DITPR**	Enter DITPR System Identification Number	New system undergoing testing
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☒	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes** ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier A0025-2 SAIS DoD

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

Army SORN authorities:

10 U.S.C. 113, Secretary of Defense;
10 U.S.C. 3013, Secretary of the Army;
10 U.S.C. 5013, Secretary of the Navy;
10 U.S.C. 8013, Secretary of the Air Force;
E.O. 12333, United States Intelligence Activities;
E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information;
National Defense Authorization Act of 2008, Section 1069;
DoDD 8521.01E, Department of Defense Biometrics;
DoDD 8500.1, Information Assurance;
AR 25-2, Information Assurance
DOD Electronic Biometric Transmission Specifications (EBTS), 23 AUG 05, Version 1.1
E.O. 9397 (SSN), as amended.

Other authorities:

Title 18 U.S.C.
USA Patriot Act, Title II, Section 206

Title 50 U.S.C., Chapter 36, Subchapter 1, S1802 and 1810
Privacy Act of 1974

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

This systems is being tested by NAVAIR to verify feasibility of biometirc collection for this project. The purpose of the Gatekeeper-on-the Move-Biometrics (GOTM-B) system is to improve threat detection, while ensuring optimal people flow and efficient non-stop biometric data capture. The non-stop technology reduces the amount of time for data acquisition allowing subjects to continue walking at a normal pace. Captured biometric data is searched against a local white list to identify the subject and their access information.

Personal information collected includes: Biometrics images; biometric templates; supporting documents; identifying biographic information including, but not limited to, name, date of birth, place of birth, height, weight, eye color, hair color, race, globally unique identifier, gender, and similar relevant information such as age.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that GOTM-B, with its extensive collection of PII, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place.

GOTM-B computerized records maintained in a controlled area are accessible only to authorized personnel. Records are maintained in a controlled facility. Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel. Physical and electronic access is restricted to designated individuals having a need therefore in the performance of official duties and who are properly screened and cleared for need-to-know, as well as protecting privacy information in compliance with the Privacy Act of 1974.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. NAVAIR, SPAWAR

☒ **Other DoD Components.**

Specify. CENTCOM, JPM- Guardian, and JIEDDO (Navy and Army)

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

For GOTM-B Technical Demonstration, participants are given informational brief and given the opportunity to volunteer and provide PII for collection for the test demonstration only. Participants will be provided detailed written information about the necessary PII required for the technical demonstration in which they will sign to acknowledge their understanding as well as provide their personal consent for the collection and use of their PII and participation in the technical demonstration. Individuals who choose not to volunteer or provide PII or participate in the technical demonstration will not have their PII collected or be enrolled into the GOTM system.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

A Privacy Act Statement detailing authority and uses of information is presented to the applicant. The form also contains a signature certification and authorization to release any information from an applicant record that DOD needs to determine access authority, which includes biometric and biographic information. All GOTM-B volunteer participants application and registration forms include a Privacy Act Statement and a signature release authorizing use of information.

The participant provides consent when an application/registration is signed to release PII to the GOTM demonstration team that will be used to determine eligibility for access to entry controlled points for the technical demonstration.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒	**Privacy Act Statement**	☐	**Privacy Advisory**
☒	**Other**	☐	**None**

Describe each applicable format.	The applicant will receive a Privacy Act Statement and Consent form during the registration process for signature and consent.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☒ Name	☐ Other Names Used	☐ Social Security Number (SSN)
☐ Truncated SSN	☐ Driver's License	☒ Other ID Number
☐ Citizenship	☐ Legal Status	☒ Gender
☒ Race/Ethnicity	☒ Birth Date	☒ Place of Birth
☐ Personal Cell Telephone Number	☐ Home Telephone Number	☐ Personal Email Address
☐ Mailing/Home Address	☐ Religious Preference	☐ Security Clearance
☐ Mother's Maiden Name	☐ Mother's Middle Name	☐ Spouse Information
☐ Marital Status	☒ Biometrics	☐ Child Information
☐ Financial Information	☐ Medical Information	☐ Disability Information
☐ Law Enforcement Information	☐ Employment Information	☐ Military Records
☐ Emergency Contact	☐ Education Information	☒ Other

If "Other," specify or explain any PII grouping selected.	Other ID: Globally unique identifier Other: height, weight, eye color, hair color and similar relevant information such as age.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

Individuals will voluntarily provide PII during the enrollment/ registration process. Biometric collection will utilize commercially available image scanning devices for fingerprints, facial and iris recognition systems and stored in locally controlled database software and hardware devices.

(3) How will the information be collected? Indicate all that apply.

☒	**Paper Form**	☒	**Face-to-Face Contact**
☐	**Telephone Interview**	☐	**Fax**
☐	**Email**	☐	**Web Site**
☒	**Information Sharing - System to System**		
☒	**Other**		

Collected data from paper form, face to face contact and fingerprint imaging scanning device will be entered in the GOTM enrollment system via keying in information and using the Finger-on-the-Fly (FiOTF) modal for input into the system.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

GOTM-B is a fully automated multi-modal, contact-less biometric system that will collect 3D fingerprint, face, and iris biometric information while subjects are "on the move," for verification, identification, authentication and data matching, thus preventing the adversary and people of interest from exploiting potential entry point vulnerabilities.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Mission-related and Administrative Use:

To enhance identity management of DoD persons and streamline business functions through a biometric database and associated data processing/information service for designated populations.

The following functions are the key processes supported by this system:
To support DoD personnel, physical and logical security, and identity management by identifying or verifying an individual through the use of biometric databases and associated data processing/information services for designated populations for purposes of protecting U.S./Coalition/allied government/national security areas of responsibility and information. To provide personnel identification and verification capabilities during disaster scenarios or other catastrophic events. To enhance or streamline DoD functions that benefit from available biometric information for identification or verification of personnel.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

☐ **Yes** ☒ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. **Who has or will have access to PII in this DoD information system or electronic collection?** Indicate all that apply.

☒ **Users** ☒ **Developers** ☒ **System Administrators** ☒ **Contractors**

☐ **Other**

If "Other," specify here.

d. **How will the PII be secured?**

(1) Physical controls. Indicate all that apply.

☒	**Security Guards**	☒	**Cipher Locks**
☐	**Identification Badges**	☒	**Combination Locks**
☐	**Key Cards**	☐	**Closed Circuit TV (CCTV)**
☒	**Safes**	☐	**Other**

If "Other," specify here.

(2) Technical Controls. Indicate all that apply.

☒	**User Identification**	☐	**Biometrics**
☒	**Password**	☒	**Firewall**
☐	**Intrusion Detection System (IDS)**	☐	**Virtual Private Network (VPN)**
☒	**Encryption**	☐	**DoD Public Key Infrastructure Certificates**
☐	**External Certificate Authority (CA) Certificate**	☒	**Common Access Card (CAC)**
☐	**Other**		

If "Other," specify here.

(3) **Administrative Controls.** Indicate all that apply.

☒ **Periodic Security Audits**

☒ **Regular Monitoring of Users' Security Practices**

☒ **Methods to Ensure Only Authorized Personnel Access to PII**

☒ **Encryption of Backups Containing Sensitive Data**

☒ **Backups Secured Off-site**

☐ **Other**

If "Other," specify here.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

☒ **Yes. Indicate the certification and accreditation status:**

☒	**Authorization to Operate (ATO)**	**Date Granted:**	TBD
☐	**Interim Authorization to Operate (IATO)**	**Date Granted:**	
☐	**Denial of Authorization to Operate (DATO)**	**Date Granted:**	
☒	**Interim Authorization to Test (IATT)**	**Date Granted:**	TBD

☐ **No, this DoD information system does not require certification and accreditation.**

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Collection: Participants will go through the data collection process one time to capture their reference sample (enrollment) and then each time to their normal entry/exit routine to their work facility (identification). The identification collection shall not impede participants' access to appropriate facilities.

Use, retention, processing: The biometric capture and storage device with the demographic information will be safe guarded with password protected and locked in secure location. This device is a stand-alone system and will not be connected to any network. Only authorized personnel with the "need to know" can access a member's PII information.

Disclosure: Fingerprint/facial photo data/recordings will only be used to support this demonstration and shall not

be release to the public or used for any other purposes. Only authorized personnel with the "need to know" can access a member's PII information.

Destruction: All fingerprint/facial photo data/recordings will be destroyed on completion of the demonstration according to DoD standards and regulations.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

N/A

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

The biometric capture and storage device with the demographic information will be safe guarded with password protected and locked in secure location. This device is a stand-alone system and will not be connected to any network. All Fingerprint/facial photo data/recordings will only be used to support this demonstration and shall not be release to the public or used for any other purposes.

The following controls are used to mitigate the risks:
a) Access Controls. Access controls limit access to the application and/or specific functional areas of the application. These controls consist of privileges, general access, password control and discretionary access control. Additionally, each user is associated with one or more database roles. Each role provides some combination of privileges to a subset of the application tables. Users are granted only those privileges that are necessary for their job requirements. The same roles that protect the database tables also determine which buttons and menu items are enabled for the user currently logged on.
b) Confidentiality. This ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.
c) Integrity. This ensures that data has not been altered or destroyed in an unauthorized manner.
d) Audits. This includes review and examination or records, activities, and system parameters, to assess the adequacy of maintaining, managing and controlling events that may degrade the security posture of the application.
e) Training. Security training is provided on a continuous basis to keep users alert to the security requirements. Visual effects are used as constant reminders to ensure users always remain aware of their responsibilities.
f) Physical Security. This consists of placing servers that contain privileged information in a secure and protected location, and to limit access to this location to individuals who have a need to access the servers. An internal policy is set in place to ensure that there are always no less than two users present at a time when privileged information is being retrieved.

Servers are located at NAVAIR, Patuxent River, MD.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature	LAU.ANGELA.J.1246894619 Digitally signed by LAU.ANGELA.J.1246894619 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=LAU.ANGELA.J.1246894619 Date: 2014.02.13 15:09:32 -05'00'
Name:	
Title:	NAVAIR 4.5X SSP deputy
Organization:	
Work Telephone Number:	(301) 342-0374
DSN:	
Email Address:	angela.lau@navy.mil
Date of Review:	02/13/2014
Other Official Signature (to be used at Component discretion)	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	

Other Official Signature (to be used at Component discretion)	SHAW.MARY.P.1229597341 Digitally signed by SHAW.MARY.P.1229597341 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=SHAW.MARY.P.1229597341 Date: 2014.09.09 15:20:05 -04'00'
Name:	for Robin Patterson
Title:	Head, FOIA/Privacy Act Program Office (OPNAV DNS-36)
Organization:	Office of the Chief of Naval Operations (OPNAV DNS-36)
Work Telephone Number:	202-685-6545
DSN:	
Email Address:	robin.patterson@navy.mil
Date of Review:	
Component Senior Information Assurance Officer Signature or Designee	MAYER.RICHARD.R.JR.1029330600 Digitally signed by MAYER.RICHARD.R.JR.1029330600 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=MAYER.RICHARD.R.JR.1029330600 Date: 2014.03.05 14:30:57 -05'00'
Name:	Richard R. Mayer
Title:	Air 4.5. IAM
Organization:	NAVAIR 4.5. (NAWC-AD 7.2.6. embedded)
Work Telephone Number:	301-757-2868
DSN:	
Email Address:	richard.r.mayer@navy.mil
Date of Review:	5 Mar 2014
Component Privacy Officer Signature	EVANS.MARY.ELLEN.1229319775 Digitally signed by EVANS.MARY.ELLEN.1229319775 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=EVANS.MARY.ELLEN.1229319775 Date: 2014.03.05 14:47:09 -05'00'
Name:	Mary Ellen Evans
Title:	NAVAIR Privacy Act Administrator
Organization:	Command Operations & Leadership Support Dept
Work Telephone Number:	301-757-3693
DSN:	
Email Address:	mary.evans@navy.mil
Date of Review:	5 Mar 2014

Component CIO Signature (Reviewing Official)	MUCK.STEVEN.ROBERT.1179488597 Digitally signed by MUCK.STEVEN.ROBERT.1179488597 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=MUCK.STEVEN.ROBERT.1179488597 Date: 2014.09.10 13:15:11 -04'00'
Name:	for Barbara Hoffman
Title:	Principal Deputy CIO
Organization:	Office of the Department of the Navy Chief Information Officer (DON CIO)
Work Telephone Number:	703-695-1842
DSN:	
Email Address:	barbara.hoffman@navy.mil
Date of Review:	10 September 2014

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.