PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Office of Special Investigations Global Network (OGN)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

12/09/20

Office of Special Investigations

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

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

The Office of Special Investigation Global Network (OGN) hosts a collection of mission essential information technology systems and file shares that supports Office of Special Investigations (OSI). Thru the OGN, OSI developed an integrated and unified, comprehensive enterprise program / system that houses Unclassified - Law Enforcement Sensitive (LES) data (unstructured) leveraging existing and future OSI LE enterprise information technology assets and other external data sources providing a full range of law enforcement functions to support business objectives and mission. OGN stores UNCLASSIFED files (such as unstructured data) in any format to include controlled unclassified information (CUI) which may contain PII that may have been collected via another method (i.e. another source).
The IT systems hosted on OGN are registered separately and have its own privacy Impact Assessment and system of records notice.

PII collected: Since PII collection is through different applications but under the AFOSI entity collecting source, it is not possible for OSI to definitively identify what is collected and stored in OGN. Individual application owners are responsible for identifying specific PII collections.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

The information is collected to identify persons involved as subjects, suspects, witnesses or victims of crimes and to assist in the investigative process; to verify and authenticate owners of authorized vehicles and weapons; to properly account for and administer persons in confinement; verification, authentication, and identification of information provided by applicants for creating credentials and verifying eligibility and qualification for employment. This information is also used to confirm the facts as stated in the case.

e. Do individuals have the opportunity to object to the collection of their PII? [ ] Yes [x] No

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

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Given the nature of Law Enforcement responsibilities and undercover operations, suspects and subjects are not always given the opportunity to object. Individuals may refuse to cooperate with investigations as long as their actions do not obstruct justice. Erroneous records may be expunged or corrected by request to Headquarters Office of Special Investigations (OSI).

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] No

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

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

Given the nature of Law Enforcement responsibilities and undercover operations, suspects and subjects are not always given the opportunity to consent to the use of their PII.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☐ Privacy Act Statement ☐ Privacy Advisory ☒ Not Applicable

OGN does not collect PII direction Privacy Act Statements/Advisories provided at source of collection.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	USAF Security Forces, Secretary of the Air Force (SAF) Inspector General (IG), USAF Judge Advocate General's Corps (JAG), Air Force Personnel Center (AFPC), US Space Force
☒ Other DoD Components	Specify.	DOD Law Enforcement Exchange (DDEX), US Army Criminal Investigation Command (CID), Marine Corps CID, Navy Military Police, Naval Criminal Investigative Service (NCIS), Defense Manpower Data Center (DMDC), Defense Human Resources Activity (DHRA), DOD Inspector General, Defense Criminal Investigative Service, Defense Finance and Accounting Service (DFAS)
☒ Other Federal Agencies	Specify.	Federal Bureau of Investigations (FBI) Army and Air Force Exchange Services (AAFES), Office of Management and Budget, Department of Veterans Affairs, other Federal Law Enforcement and Confinement/Correctional Agencies; Bureau of Prisons, Alcohol, Tobacco & Firearms, Office of Personnel Management, Department of Homeland Security, Federal Child Protection Services or Family Support Agencies, Immigration and Naturalization Services, Department of Justice, Internal Revenue Service, General Services Administration, National Archives and Records Administration, the Merit Systems Protection Board, US Congress and the Office of Special Counsel
☒ State and Local Agencies	Specify.	In addition to those disclosures generally permitted under 5 U.S.C. 552 a (b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a (b) (3) as follows: Information concerning criminal or possible criminal activity is disclosed to Federal, State, local and/or foreign law enforcement agencies in accomplishing and enforcing criminal laws; analyzing modus operandi, detecting organized criminal activity, or criminal justice employment; motor vehicle departments, State and local confinement/ correctional facilities; Medical facilities; State and local child protection services and family support agencies. Information may also be disclosed to foreign countries under the provisions of the Status of Forces Agreements or Treaties.

☒	Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	Abacus Technology Corporation Contract #FA8732-15-D-0022 (Task Order # - FA701419FA201) Expiration Date - 30 September 2020 Yes, FAR privacy clauses are included in the Performance Work Statement (PWS) 52.224-1 Privacy Act Notification. As prescribed in 24.104, insert the following clause in solicitations and contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function: Privacy Act Notification (Apr 1984) The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties. (End of clause) 52.224-2 Privacy Act. As prescribed in 24.104, insert the following clause in solicitations and contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function: Privacy Act (Apr 1984) (a) The Contractor agrees to— (1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies— (i) The systems of records; and (ii) The design, development, or operation work that the contractor is to perform; (2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and (3) Include this clause, including this paragraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records. (b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.
☒	Other *(e.g., commercial providers, colleges)*.	Specify.	Limited information may be provided to victims and witnesses of crimes, limited information may be disclosed to foreign countries under the provision of the Status of Forces Agreements, or Treaties.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

- [x] Individuals
- [x] Databases
- [x] Existing DoD Information Systems
- [x] Commercial Systems
- [x] Other Federal Information Systems

Information is obtained through other IT systems hosted in OGN and individuals, from victim and witnesses of crimes, through research involving access to multiple automated data systems, records and third parties, citizens band and commercial radio, local proactive crime watching/prevention organizations, and individual applicants. Other source of PII are Defense Enrollment Eligibility Reporting System (DEERS)/Realtime Automated Personal Identification System (RAPIDS), Criminal Justice Information System (CJIS) and Base Level Communication Infrastructure (BLCI).

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [x] E-mail
- [x] Official Form (*Enter Form Number(s) in the box below)*
- [x] Face-to-Face Contact
- [x] Paper
- [x] Fax
- [x] Telephone Interview
- [x] Information Sharing - System to System
- [x] Website/E-Form
- [ ] Other *(If Other, enter the information in the box below)*

PII collected from AFOSI employees, victims and witnesses of crimes came from DEERS, RAPIDS and CJIS
OPM Optional Form 306, Declaration for Federal Employment

k. 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 must be consistent.

- [ ] Yes
- [x] No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

OGN's does not collect PII directly. OGN is hosts information from feeder that are covered by existing SORNs. The following SORNs cover all of AFOSI system of records.

The following SORNs cover the IT systems hosted on the OGN:
Command Learning Management System, F071 AFOSI E
Counterintelligence Operations and Collection Records, F071 AF OSI A
Investigative Information Management System, F071 AF OSI D
Air Force Badge and Credentials, F071 AF OSI G
Investigative Applicant Processing Records, F071 AF OSI F

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. N1-AFU-87-23

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

T 71-01 R 01.00 Investigations into Offenses of Mutiny or Sedition, Misbehavior Before the Enemy, Subordinate Compelling Surrender, Retire as permanent; T 71-01 R 02.00 Investigations into Offenses of Espionage, Sabotage, Treason, Sedition, Violations at AFOSI Field Extensions, Destroy 90 days after receipt of permanent file at HQ AFOSI/XILD or when no longer needed, whichever is sooner; T 71-01 R 03.00 Investigations into Alleged Violations of Laws, Regs and Directives (Excluding Investigations in Rules 1, 2, 7, 8 and 12), Disposition Pending; T 71-01 R 04.00 Investigations into Alleged Violations of Laws, Regs and Directives (Excluding Investigations in Rules 1, 2, 7, 8 and 12), Disposition Pending; T 71-01 R 05.00 Investigations into Alleged Violations of Laws, Regs and Directives (Excluding

NOTE: Sections 1 above is 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 if they contain information that would reveal sensitive information or raise security concerns.