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 Classified Global Network (OGCN)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

12/17/20

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 Classified Global Network (OCGN) hosts a collection of mission essential information technology systems and file shares that supports Office of Special Investigations (OSI). Thru the OCGN, OSI developed an integrated and unified, comprehensive enterprise program / system that houses Classified - 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. OCGN stores CLASSIFED 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 OCGN 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 OSI entity collecting source, it is not possible for OSI to definitively identify what is collected and stored in OCGN. See section 2a for comprehensive list.

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 counterintelligence investigative process.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] 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).

Individuals give consent to use, collection, and storage of their information in identifiable form through their signing of the application for employment/agent application process.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [x] Yes [ ] 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.

All other unstructured data containing PII that are stored in OGCN were collected from subjects, suspects, witnesses or victims of crimes and who were given the opportunity to consent during the interview process.

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

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)

[X] 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 OCGN 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)/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
[ ] 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 OSI employees, victims and witnesses of crimes.

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.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier F071 AF OSI A, F071 AF OSI D

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.

The retrieval method from file shares in OCGN vary. OCGN stores unstructured files used for file/information sharing (file shares). OCGN stores official records in records drive. The following SORNs cover all of OSI records stored in CI2MS which includes some records stored in OCGN.

The following SORNs cover the IT systems hosted on the OCGN:
Counterintelligence Operations and Collection Records, F071 AF OSI A
AFOSI Investigative Records, F071 AF OSI D

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. NC1-AFU-77-55; N1-AFU-90-03; NC1-AFU-76-23; N1-AFU-87-21; N1-

(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 Investigations in Rules 1, 2, 7, 8 and 12), Disposition Pending; T 71-01 R 06.00 Reciprocal Investigations at HQ AFOSI/XILD, Destroy after 1 year; T 71-01 R 07.00 Reciprocal Investigations at AFOSI Field Extension, Destroy after 3 months; T 71-01 R 08.00 Zero Files (All Categories Contained in 71-Series Tables), Disposition Pending; T 71-01 R 09.00 Zero Files (All Categories Contained in 71-Series Tables), Destroy 2 years after receipt at HQ AFOSI/XILD or when no longer needed, whichever is later; T 71-01 R 10.00 Counter-Inteligence Investigations (CI) Special Inquiry Cases, Disposition Pending; T 71-01 R 11.00 Counter-Intelligence Investigations (CI) Special Inquiry Cases, Disposition Pending; T 71-01 R 12.00 Counter-Intelligence Investigations (CI) Special Inquiry Cases, Destroy after 1 year or when no longer determined pertient by an annual review; T 71-01 R 013.00 AFOSI Reports of Investigation, Destroy when no longer needed; T 71-01 R 14.00 Investigations Into Alleged Violations of Laws, Regs and Directives (Excluding Those Covered in Rules 1, 2, 10, 11 and 12), Disposition Pending; T 71-01 R 15.00 Investigations Into Alleged Violations of Laws, Regs and Directives (Excluding Those Covered in Rules 1, 2, 10, 11 and 12), Disposition Pending; T 71-07 R 01.00 Evidence Tracking System at AFOSI Detachments, Destroy 2 years after the close-out of each diskette; T 71-07 R 02.00 AFOSI Indexing Information in the Defense Clearance and Investigations Index, Disposition Pending; T 71-07 R 03.00 Liaison and Jurisdictional Agreements at HQ AFOSI/XILD, Retire as permanent; T 71-07 R 04.00 Liaison and Jurisdictional Agreements at AFOSI Field Extensions, Destroy when no longer needed; T 71-07 R 05.00 School and College Ability Tests (SCATS), Destroy when superseded or obsolete; T 71-07 R 06.00 Authority to Issue Badges and Credentials, Destroy after 1 year or when no longer needed, whichever is sooner; T 71-07 R 0800 AFOSI Investigative Resumes for USAF Commanders at HQ AFOSI/SCP, Destroy after 5 years; T 71-07 R 09.00 AFOSI Investigative Resumes for USAF Commanders at Other Offices, Destroy when no longer needed; T 71-07 R 10.00 Threatened Airman Program (TAP) at HQ AFOSI/DOG, Destroy after 10 years; T 71-07 R 11.00 Threatened Airman Program (TAP) at AFOSI Field Extensions, Destroy after 1 year, or when no longer needed, whichever is sooner; T 71-07 R 12.00 AFOSI Applicant Investigative Processing Disapproved Applications at HQ AFOSI/SILD, Destroy 10 years after disapproval; T 71-07 R 13.00 AFOSI Applicant Investigative Processing Approved Applications at HQ AFOSI/XILD, Destroy 10 years after individual's termination, decertification, discharge, or reassignment; T 71-07 R 14.00 AFOSI Applicant Investigative Processing at AFOSI Field Extensions, Disposition Pending; T 71-07 R 15.00 Wire Tapping and Eavesdropping Records Accumulated by Investigative Personnel, Destroy under same destruction criteria assigned to the substantive case supported; T 71-07 R 16.00 Identi-Kit Composite Constructed in Unknown Subject Cases, Destroy after 5 years; T 71-07 R 17.00 Fraud/Criminal Briefing Program at HQ AFOSI, Destroy after 3 years; T 71-07 R 18.00 Fraud/Criminal Briefing Program at HQ AFOSI and AFOSI Field Extensions, Disposition Pending; T 71-07 R 19.00 Specialized Crime Reports and Studies - Record Copies at HQ AFOSI, Destroy after 6 years; T 71-07 R 20.00 Specialized Crime Reports and Studies at AFOSI Field Extensions, Destroy after 2 years; T 71-07 R 21.00 Specialized Crime Reports and Studies at Units, Destroy after 1 year; T 71-07 R 22.00 Contraband Drugs and Paraphernalia as Training Aids at AFOSI Field Extensions, Destroy 1 year after last entry;T 71-07 R 23.00 Criminal Alert Notices (CANs) at HQ AFOSI/XILD, Destroy after 15 years; T71-07 R 24.00 Criminal Alert Notices (CANs) at HQ AFOSI/ DOQA and AFOSI Field Extensions, Disposition Pending;

Note 1: Among the NARA dispositions cited in this field, the one with the longest retention time will be used on the system's records data. .

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

18 U.S.C. 499, Military naval or official passes established by 10 USC Section 2672 Protection of buildings, grounds, property and persons and DODI 5505.16 Investigations by DoD Components; 506, Seals of departments or agencies; 701, Official badges, identification cards, other insignia, Air Force Office of Special Investigations Instruction 90-203, AFOSI Credentials and Identification cards.
10 U.S.C. 9013, Secretary of the Air Force; AFI 36-2201 V1, Training Development, Deliver and Evaluation; Air Force Mission Directive 39, Air Force Office of Special Investigations (AFOSI); Air Force Policy Directive 71-1, Criminal Investigations and Counterintelligence; and E.O. 9397 (SSN) as amended. 28 U.S.C. 534 note, Uniform Federal Crime Reporting Act; 42 U.S.C. 10601 et seq., Victims' Rights and Restitution Act of 1990; 18 U.S.C. 922 note, Brady Handgun Violence Prevention Act; 10 U.S.C. Chapter 47, Uniform Code of Military Justice, and 8013, Secretary of the Air Force; DoD Instruction (DoDI) 5505.11, Air Force Mission Directive (AFMD) 39, DoD Directive 7730.47, Defense Incident Based Reporting System (DIBRS); AFOSI AFMD 39 authorizes AFOSI/CC to initiate investigations according to Public Law (PL) 99-145 § 1223, Authority for Independent Criminal Investigations by Navy and Air Force Investigative Units; and Air

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.