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:

Investigations, Schedule, Track and Review System (iSTAR)

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

05/23/25

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees
- [x] from both members of the general public and Federal employees
- [ ] 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 Investigations Schedule, Track, and Review (ISTAR) system is a contractor-owned/contractor operated (CO/CO) suite of applications and components that the vendor uses to form its internal contractor owned case management system and fieldwork access endpoints to support the DCSA background investigation mission. The purpose of the iSTAR system is to assign investigation tasks to specific investigators conducting investigations on behalf of DCSA, to maximize/monitor the vendor's productivity. The tasks assigned by the system help the vendor's investigators conduct comprehensive interviews with subjects, employers, associates, references, and other knowledgeable individuals; and review appropriate records to obtain facts to resolve all material issues in a case or to establish the background, reputation, character, suitability, or qualifications of the subject under investigation. The iSTAR core application, is used as a project management and monitoring tool, with eventual addition of virtual file room to centralize all case management activities and transient document/record management.
The PIPS laptops are used to traverse case information, which contains PII, and to access DCSA information systems (FDR and FWS). PII is contained within the DCSA applications, FWS and FDR, and the data within is outside of the iSTAR boundary and covered by separate PIA(s).

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 PII is collected as part of a background investigation for a federal security clearance. All information is required in order to obtain the desired clearance level through the official process, the PIPS laptops are used to traverse case information, which contains PII.

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.

Subjects cannot object directly within iSTAR. Individuals are notified about the collection of their PII at the point of collection, at the beginning of an in person interview, and on various consent forms. They are informed that providing information is voluntary but that if they do not consent to the collection of the required information, it may affect the completion of their background investigation.

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.

Subjects cannot consent directly within iSTAR. Individuals are notified about the collection of their PII at the point of collection, at the beginning of an in person interview, and on various consent forms. They are informed that providing information is voluntary but that if they do not consent to the collection of the required information, it may affect the completion of their background investigation.

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

Investigators shall verbally provide the following Privacy Act Statement (PAS) verbatim.
"The Defense Counterintelligence and Security Agency (DCSA) is conducting a background investigation of you at the request of a U.S. Government agency. The Privacy Act of 1974 (5 U.S.C. §552a) requires that you be advised of the following four points:
1. DCSA's collection of the requested information is authorized by Executive Order 13467, as amended by Executive Order 13869.
2. This inquiry is being conducted to obtain information which will enable authorized U.S. Government officials to evaluate your initial or continued: eligibility for access to classified information or to hold a sensitive position, suitability for enlistment or appointment into military service, suitability or fitness for Federal employment, fitness for assignment to work under contract for or on behalf of the U.S. Government, or authorization to be issued a credential for physical or logical access to U.S. Government systems or facilities.
3. The information obtained will be provided to officials at the U.S. Government agency requesting the investigation, will be maintained by DCSA, and will be released to you at your request unless otherwise exempt. In addition, this information may be released to other U.S. Government agencies without your consent and without prior notice to you, provided such disclosure qualifies as a "routine use." A complete list of these routine uses can be found in the system of records notice for the Department of Defense Personnel Vetting Records System, "DUSDI 02-DoD" at: https://www.federalregister.gov/documents/2018/10/17/2018-22508/privacy-act-of-1974-system-of-records.
4. Disclosure of personal information to DCSA is voluntary. However, if you do not provide the requested information, DCSA may not be able to conduct a complete investigation, and the U.S. Government may not be able to make a determination or adjudication regarding your qualifications, suitability, eligibility, or fitness."

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

☒ Within the DoD Component	Specify.	DCSA
☐ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	
☐ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	
☐ State and Local Agencies	Specify.	
☒ 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.	CACI. All contractor personnel performing on the contract will be responsible for safeguarding all Government equipment, information, and materials in accordance with the National Industrial Security Program Operating Manual (NISPOM) 32 CFR § 117, DCSA Interim Policy Memorandum 24-003, Protection of Personally Identifiable Information (PII) and Breach Reporting, BI Operational Policy Memorandum 2- 005: Controlled Unclassified Information (CUI) Marking Guidance for Documents Containing Personally Identifiable Information (PII) and DoD Instruction 5200.48 Controlled Unclassified Information (CUI). Contractor Personnel performing activities associated with maintaining a system of records on behalf of a DoD component shall complete PII training in accordance with DoDI 5400.11, DoD 5400.11-R, and OMB Circular A-130. The contract includes FAR privacy clauses 52-224-1 Privacy Act Notifications, and 52.224-3 Privacy Training
☐ Other *(e.g., commercial providers, colleges)*.	Specify.	

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

☒ Individuals ☒ Databases
☒ Existing DoD Information Systems ☐ Commercial Systems
☒ Other Federal Information Systems

During the course of the background investigation process, commercial data is not used. However, publicly available data may be used as state, local and public court records are gathered, as required by the scope of a given background investigation.

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

☐ E-mail ☐ Official Form (*Enter Form Number(s) in the box below)*
☒ In-Person Contact ☒ Paper

[X] Fax
[X] Telephone Interview
[ ] Information Sharing - System to System
[ ] Website/E-Form
[ ] Other *(If Other, enter the information in the box below)*

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 DUSDI-02, Personnel Vetting

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.

iSTAR is not the final repository for DUSDI-02 records, however, the information/data/images that traverse through iSTAR during the processing of project/case management are collected under this SORN, and its authorities. While in-process, this is the only location for that information until transmitted.

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. DAA-0446-2019-0004-0002

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

(3) Retention Instructions.

Delete 30 days after closing date of the related investigation.
All documents associated with the investigation, to include the investigator's case notes, must be retained for 30 days from the close date, or date of cancellation in the instance of a canceled case. The 30 day retention period allows for audit purposes conducted for required quality control. Destruction of the ROI and all other materials associated (both electronic and hard copy) must occur on day 31 and be documented by a certification of destruction that details the cases destroyed/deleted with case number and the officiating individual (CACI employee) responsible for the destruction/deletion. Certification of the destruction is provided back to the customer agency with the Monthly Progress Report.

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.

Executive Orders 13869, 10450 (repealed by E.O. 13764), 10865, 12333 (amended by E.O. 13470), and 12968; sections 3301, 3302, and 9101 of title 5, United States Code (U.S.C.); sections 2165 and 2201 of title 42, U.S.C.; chapter 23 of title 50, U.S.C.; and parts 2, 5, 731, 732, and 736 of title 5, Code of Federal Regulations (CFR)

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

iSTAR is a contractor owned/contractor operated system used to provide background investigation services under contract to DCSA.
Info Collect Forms:
SF-85: Questionnaire for Non-sensitive Positions, 3206-0261, December 2027
SF-85P: Questionnaire for Public Trust Positions, 3206-0258, April 2027
SF-85P-S: Supplemental Questionnaire for Selected Positions, 3206-0258, April 2027
SF-86: Questionnaire for National Security Positions, 3206-0005, November 2026
SF-87: Fingerprint Chart, 0705-0002, April 2027
FD-258: Standard Fingerprint Form (FBI), 1110-0046 (FBI Managed)