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:

Central Adjudication Security Personnel Repository (CASPR) PSI Billing

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

07/31/20

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.

PSI Billing Module of CASPR stores information enabling DoD components to pay for Personnel Security Investigations, and to allow tracking, reconciliation, and reporting on payments for security investigations. CASPR PSI Billing module stores the invoices with SSNs provided by CASPR Billing Managers. The invoice contains spreadsheets with records of charges for security investigations.
The types of personal information stored in the system are items needed to identify the subject of the investigation. These include Name, EDIPI, SSN, Case Type, Invoice Number, Case Number, Duty Location, and Security Office Identifier.

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)*

CASPR PSI Billing only uses the PII to verify identification of the individual to determine which DoD component should pay for the individual's security investigation and to ensure that the billed amounts are valid. (Mission-related)

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.

When individuals (who enter the federal workforce) complete the Electronic Questionnaires for Investigations Processing, they enter their personal information in Defense Information System for Security (DISS), which give individuals the opportunity to consent to the use of their PII (required for 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.

When individuals (who enter the federal workforce) complete the Electronic Questionnaires for Investigations Processing, they enter their personal information in Defense Information System for Security (DISS), which give individuals the opportunity to consent to the use of their PII (required for background investigation). If individuals desire employment with the Federal government, they must consent to the required 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
- [x] 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)*

[X]	Within the DoD Component	Specify.	Billing Managers
[X]	Other DoD Components	Specify.	All Assigned DoD Components
[ ]	Other Federal Agencies	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.	
[ ]	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)*

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

Prior to placing the SSNs in Electronic Questionnaires for Investigations Processing (EQIP), individual's (who enter the federal workforce) PII is entered in Defense Information System for Security (DISS) (process of establishing ownership of an individual). Then the EQIP is generated to initiate the background investigation of the individual. OPM administrators then schedules the investigation at which time an invoice is generated from National Background Investigations Bureau (NBIB) which is provided to CASPR Billing Managers. CASPR Billing Managers in turn upload the invoice into the CASPR - PSI Billing system. DCSA OPM PSI Billing Team are the billing managers for all OPM legacy PSI submissions/cases. DCSA OPM PSI Billing Team work with Office of the Chief of Finance Office (OCFO) within DCSA and OPM Financial Management Team

Note: CASPR PSI Billing is NOT connected to EQIP, DISS, and NBIB or any other system. OPM administrators provide CASPR PSI Billing Managers with an invoice each month. CASPR Billing Managers upload the invoice into the CASPR PSI Billing module Automated Imported/or MANUALLY. The invoices, which contain SSNs and other PII, are zipped text files that generate spreadsheets with records of charges for security investigations upon entry into CASPR. DISS has an approved SSN Justification memo.

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

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

OPM administrators provide CASPR PSI Billing Managers with an invoice each month. CASPR Billing Managers upload the invoice into the CASPR PSI Billing module Automated Imported/or MANUALLY. The invoices, which contain SSNs and other PII, are zipped text files that generate spreadsheets with records of charges for security investigations upon entry into CASPR.

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.

Information is retrieved by Month then Component then Invoice #. SORN is not required for PSI Billing. The collection for the adjudication of individuals is covered by DoD Wide SORN DMDC-24-DoD

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-GRS-2013-0003-00

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

(3) Retention Instructions.

GRS 1.1 Item 1 Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting. Disposition Authority: DAA-GRS-2013-0003-0001. Information will be purged from system manually.

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.

10 U.S.C. 9013, Secretary of the Air Force; 5 U.S.C. 301, Departmental Regulations; 5 U.S.C. 7531(Definitions), 7532 (Suspension and removal), and 7533 (Effects on other statues); E.O. 10450, Security Requirements for Government Employment; DoDI 5200.02, Department of Defense Personnel Security Program; and E.O. 9397 (SSN).

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.

[X] 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.

OMB # 0704-0573 is the approved OMB # for Personnel Security Investigation, expires 07/31/2021. CASPR PSI Billing Module does not collect information from the public, it stores information collected by DISS and OPM which is approved by OMB.

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)***?** *(Check all that apply)*

☐ Biometrics	☐ Birth Date	☐ Child Information
☐ Citizenship	☐ Disability Information	☒ DoD ID Number
☐ Driver's License	☐ Education Information	☐ Emergency Contact
☒ Employment Information	☐ Financial Information	☐ Gender/Gender Identification
☐ Home/Cell Phone	☐ Law Enforcement Information	☐ Legal Status
☐ Mailing/Home Address	☐ Marital Status	☐ Medical Information
☐ Military Records	☐ Mother's Middle/Maiden Name	☒ Name(s)
☐ Official Duty Address	☐ Official Duty Telephone Phone	☐ Other ID Number
☐ Passport Information	☐ Personal E-mail Address	☐ Photo
☐ Place of Birth	☐ Position/Title	☐ Protected Health Information (PHI)[1]
☐ Race/Ethnicity	☐ Rank/Grade	☐ Religious Preference
☐ Records	☐ Security Information	☒ Social Security Number (SSN) *(Full or in any form)*
☐ Work E-mail Address	☒ If Other, enter the information in the box below	

Case Type (Type of security clearance applied for), Invoice Number, Case Number, Security Office Identifier. CASPR PSI Billing is not the initial method of collection. The DISS is the initial point of collection and has a a valid SSN justification memo.

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☒ Yes ☐ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

CASPR PSI Billing does not collect SSNs. The DISS approved SSN justification memo for the adjudication covers the PSI Billing for the purpose of using SSN as the primary identifier. Per DISS Justification memo, "as required in DoDI 1000.30, the acceptable use for the Social Security Number (SSN) has been identified as 03, Security Clearance Investigation or Verification. The SSN is the single identifier that links all aspects of a security clearance investigation together. This use case is also linked to other Federal agencies that continue to use the SSN as a primary identifier."The Defense Privacy, Civil Liberties and Transparency Division (DPCLTD) has accepted the SSN justification memo Continued Use of SSN in Defense Information System for Security (DISS), DITPR ID# 1640 for continued use of the SSN for the purpose of (3) Security Clearance Investigation or Verification to accelerate the clearance process, reduce security clearance vulnerabilities, decrease back-end processing timelines, and support simultaneous information sharing within various DoD entities, as well as among a number of authorized federal agencies.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

As required in DoDI 1000.30, the acceptable use for the Social Security Number (SSN) has been identified as 03, Security Clearance Investigation or Verification. The SSN is the single identifier that links all aspects of a security clearance investigation together. This use case is also linked to other Federal agencies that continue to use the SSN as a primary identifier.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

N/A

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☐ Yes ☒ No

The SSN is the single identifier that links all aspects of a security clearance investigation together. This use case is also linked to other Federal agencies that continue to use the SSN as a primary identifier.

b. What is the PII confidentiality impact level[2]? ☐ Low ☐ Moderate ☒ High

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.