# 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:**

Defense Cash Accountability System

**2. DOD COMPONENT NAME:**

Defense Finance and Accounting Service

**3. PIA APPROVAL DATE:**

08/13/21

## 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 Defense Cash Accountability System (DCAS) supports the Department of Defense (DoD) financial reporting process by performing cross-disbursing functions in reconciling financial transactions among the DoD reporting entities, as well as contributing to the reconciliation functions related to DoD reporting entities' Funds Balance with Treasury (FBwT). DCAS processes Personally Identifiable Information (PII) in order for partner systems to be able to perform their missions.

DCAS contains the following types of personal information: Electronic Data Interchange Personal Identifier (EDIPI)/DoD Identification (ID) number, name(s), Social Security Number (SSN), and work e-mail address.

**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)*

DCAS collects PII in order for partner systems and databases to be able to perform their missions. DCAS collects PII from Automated Disbursing System (ADS). ADS has interconnecting systems that require the use of the SSN in the disbursement process. DCAS collects PII directly from Defense Corporate Database (DCD) via cross-disbursement transactions and needs the name and SSN to tie the transaction back to an individual traveler. Defense Travel System (DTS) is the source of the DCD PII. DCAS collects PII from the Defense Disbursing Analysis Reporting System (DDARS). DDARS requires the use of the SSN for the matching of disbursements and collections, and the reconciling and identifying of unmatched or problem disbursements. DCAS collects PII from the Operational Data Store (ODS). ODS requires the use of the SSN to track financial transactions from beginning to end. DCAS collects PII from the Defense Civilian Pay System (DCPS). The Cleveland Payroll Offices need this PII to identify the employees with collections.

The EDIPI/DoD ID number, name(s), SSN, and work e-mail address are stored only for the identification of the users.

The intended use is mission-related: the DCAS application must store and provide PII to other interconnecting systems to support their cross-disbursing needs.

**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.

The DCAS is a pass-through type of data processing service. Other government financial systems provide PII data to DCAS. The other financial systems provide Users (Individuals) with the contents of the Privacy Act Statement (Section 6311 of Title 5, United States Code (U.S.C.)) and the contents of Public Law 104-134 (April 26, 1996) at the time of account creation. As a condition of employment or contract, the DoD pays individuals and proprietorships by direct deposit.

**f. 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.

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

DCAS obtains information from supporting financial management systems utilized by Active Duty, Reserve, Guard, separated or retired military members, cadets, dependents, annuitants, civilian employees, and individuals operating proprietorships. The systems advise individuals of PII usage and individuals provide consent at the time of registration.

**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. | Defense Finance and Accounting Service (DFAS) organizations that demonstrate a need-to-know |
| ☒ Other DoD Components | Specify. | United States (US) Army, US Air Force, US Marine Corps, US Navy, Defense Commissary Agency (DCA), Defense Information Systems Agency (DISA), Defense Logistics Agency (DLA) |
| ☐ 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)*

☐ Individuals ☐ Databases

☒ Existing DoD Information Systems ☐ Commercial Systems

☐ Other Federal Information Systems

SYSTEMS:
- ADS, System Owner: DFAS, DoD IT Portfolio Repository (DITPR) ID: 36, System of Records Notice (SORN) ID: T7906
- DCD, System Owner: DFAS, DITPR ID: 17250, SORN ID: T7320
- DCPS, System Owner: DFAS, DITPR ID: 93, SORN ID: T7335
- DDARS, System Owner: DFAS, DITPR ID: 838, SORN ID: T7300
- DTS, System Owner: DLA, DITPR ID: 125, SORN ID: DHRA 08 DoD
- Financial Management System Next Generation (FMSNG), System Owner: Naval Systems Management Activity (NSMA)
- ODS, System Owner: DFAS, DITPR ID: 13, SORN ID: T7900
- Standard Accounting, Budget and Reporting System (SABRS), System Owner: DFAS, DITPR ID: 21, SORN ID: The systems does not retrieve information by name or SSN.

**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)*

☐ Face-to-Face Contact ☐ Paper

☐ Fax ☐ 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.

☐ Yes ☒ 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.

DCAS does not retrieve information by PII and as such does not have a SORN requirement. DCAS does not query by PII or manipulate any of the PII information pushed to the DCAS system. Other government financial systems provide PII data to DCAS. The other financial systems provide Users (Individuals) with the contents of the Privacy Act Statement (Section 6311 of Title 5, U.S.C.) and the contents of Public Law 104-134 (April 26, 1996) at the time of account creation.

**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?** DFAS 5015.2-M Volume

(1) NARA Job Number or General Records Schedule Authority.

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

(3) Retention Instructions.

Cutoff is at the end of the fiscal year, and destroy 10 years after cutoff.

**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.

Public Law 104-134, Debt Collection Improvement Act of 1996; DoD Financial Management Regulation 7000.14-R, Volumes 7B, 7C, 8, Military Pay Policy and Procedures Retired Pay, Military Pay Policy and Procedures Active Duty and Reserve Pay, Civilian Pay Policy and Procedures; and Executive Order (E.O.) 9397 (SSN), as amended.

**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.

The DCAS does not have a Paperwork Reduction Act (PRA) requirement as it receives all data through other government systems. DoD 8910.01 clears the data at point of entry.

## 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 | |

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.

DCAS forwarded the SSN Justification Memo signed by Director, Information Technology. DPCLTD approved the memo on October 3, 2019.

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

The justification for the use of the SSN is DoDI 1000.30, Enclosure 2, paragraph 2.c. (4) "Interactions with Financial Institutions" and Enclosure 2, Paragraph 2.c. (7) "Federal Taxpayer Identification Number." Financial institutions may require that individuals provide the SSN as part of the process to open accounts. It may therefore be required to provide the SSN for systems, processes, or forms that interface with or act on behalf of individuals or organizations in transactions with financial institutions. The application of Federal and State income tax programs rely on the use of the SSN. As such, systems that have any function that pertains to the collection, payment, or record keeping of this use case may contain the SSN. Additionally, individuals who operate corporate entities under their own name may use their SSN as the tax number for that business function.

The authority for this DoD information system to collect, use, maintain, and/or disseminate PII is found in the following: Public Law 104-134, Debt Collection Improvement Act of 1996; DoD Financial Management Regulation 7000.14-R, Volumes 7B, 7C, 8, Military Pay Policy and Procedures Retired Pay, Military Pay Policy and Procedures Active Duty and Reserve Pay, Civilian Pay Policy and Procedures; and E.O. 9397 (SSN), as amended. The DITPR ID for this system is 17248. A SORN is not required for ADS, DCD, DCPS, DDARS, DTS, and ODS support, because these systems already have SORNs. DCAS also completed a DoD Privacy Impact Assessment.

Justification for the use of the SSN does not constitute blanket permission to use such data. The DCAS application supports the DoD financial reporting process by performing cross-disbursing functions in reconciling financial transactions among the DoD reporting entities, as well as contributing to the reconciliation functions related to DoD reporting entities' FBwT. The SSN must continue to be collected and stored in order for partner systems to be able to perform their missions.

(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".

The DCAS has taken the following steps to safeguard the SSNs: (1) limiting access to SSNs through user roles, (2) Common Access Card enabling the application, (3) limiting access to .mil, (4) monitoring and removing access in a timely manner, (5) using software and hardware to encrypt data in transit between DCAS and other interconnecting systems, (6) maintaining the application at a Defense Information Systems Agency location, and (7) mandating all users complete annual privacy act training.

(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

DFAS continues to evaluate applications and application's outputs, forms, and processes for opportunities to eliminate and reduce the use of the SSN. DCAS pursues alternative safeguards such as those noted in the paragraphs above when elimination and/or reduction are not feasible.

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

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

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

(1) Physical Controls. *(Check all that apply)*

- ☒ Cipher Locks
- ☒ Combination Locks
- ☒ Key Cards
- ☒ Security Guards
- ☒ Closed Circuit TV (CCTV)
- ☒ Identification Badges
- ☐ Safes
- ☒ If Other, enter the information in the box below

Data is stored in government office buildings protected by guards, controlled screening, visitor registers are used, electronic access, and/or locks. Physical access to data is limited to properly screened and cleared individuals on a need-to-know basis in the performance of their official duties. Physical access to hardware and software are limited to persons responsible for servicing the system.

(2) Administrative Controls. *(Check all that apply)*

- ☒ Backups Secured Off-site
- ☒ Encryption of Backups
- ☒ Methods to Ensure Only Authorized Personnel Access to PII
- ☒ Periodic Security Audits
- ☒ Regular Monitoring of Users' Security Practices
- ☒ If Other, enter the information in the box below

DCAS limits access to .mil, monitors and removes access in a timely manner, mandates all users complete annual privacy training, and holds incident response and continuity of operations exercises annually.

(3) Technical Controls. *(Check all that apply)*

- ☐ Biometrics
- ☒ Command Access Card (CAC)
- ☒ DoD Public Key Infrastructure Certificates
- ☒ Encryption of Data at Rest
- ☒ Encryption of Data in Transit
- ☐ External Certificate Authority Certificates
- ☒ Firewall
- ☒ Intrusion Detection System (IDS)
- ☒ Least Privilege Access
- ☒ Role-Based Access Controls
- ☒ Used Only for Privileged (Elevated Roles)
- ☒ User Identification and Password
- ☒ Virtual Private Network (VPN)
- ☐ If Other, enter the information in the box below

**d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?**

DCAS implements defense in depth with a balanced focus on people, technology, and operations to mitigate privacy risks. People: All authorized system users have successfully completed a background investigation and qualify for Information Technology Level II (IT Level II) or higher. Technology: Application software, firewalls, intrusion detection systems, and routers are Common Criteria validated. DCAS protects PII information at rest and in transit with Federal Information Processing Standards (FIPS) 140-2 validated encryption. Operations: System changes undergo a security impact analysis (SIA) to ensure they will not adversely impact the system's cybersecurity posture. DCAS performs STIG scans, installs security patches and virus updates, and maintains up-to-date access control lists.

## SECTION 3: RELATED COMPLIANCE INFORMATION

**a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool[3]?**

| | | | |
|---|---|---|---|
| [X] | Yes, DITPR | DITPR System Identification Number | 17248 |
| [ ] | Yes, SIPRNET | SIPRNET Identification Number | |
| [X] | Yes, RMF tool | RMF tool Identification Number | 95 |
| [ ] | No | | |

If "No," explain.

**b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology".**

Indicate the assessment and authorization status:

| | | | |
|---|---|---|---|
| [X] | Authorization to Operate (ATO) | Date Granted: | 1/13/2021 |
| [ ] | ATO with Conditions | Date Granted: | |
| [ ] | Denial of Authorization to Operate (DATO) | Date Granted: | |
| [ ] | Interim Authorization to Test (IATT) | Date Granted: | |

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

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

[X] Yes [ ] No

If "Yes," Enter UII 007-97-01-01-01-0133-00 If unsure, consult the component IT Budget Point of Contact to obtain the UII

[3]Guidance on Risk Management Framework (RMF) tools (i.e., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at https://rmfks.osd.mil.