# 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:**

Departmental Cash Management System (DCMS)

**2. DOD COMPONENT NAME:**

Defense Finance and Accounting Service

**3. PIA APPROVAL DATE:**

11/23/20

## 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.**

PRINCIPAL PURPOSE(S): DCMS manages and reconciles cash disbursements, reimbursements, collections, and receipts for Air Force department-wide. It reconciles interfund processing for network users and provides support for improved cash management business processes by consolidating and generating annual reports of expenditures and receipts. Minimal personally identifiable information (PII) is collected via interface partner file transmissions to perform the aforementioned business processes. The Social Security Number (SSN), which may be full or truncated, is embedded in a standard document identifier from the line of accounting for official Government travel.

**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)*

Data Matching: DCMS is designed to automate the For/By Others process which uses the SSN, Truncated SSN.

**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.

DISCLOSURE: DCMS does not collect PII directly from the individual.

**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.

DCMS does not collect PII directly from the individual.

**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

DCMS does not collect PII directly from the individual.

**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. | PII will be shared with DFAS organizations that demonstrate a need-to-know (e.g., accounting or finance operations), and have the required clearance to use that information. |
| [x] | Other DoD Components | Specify. | United States Air Force (USAF), Army, Navy, Marine Corps, active, reserve, guard members, and National Geospatial-Intelligence Agency civilian employees. |
| [ ] | 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
- [x] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [ ] Databases
- [ ] Commercial Systems

General Accounting and Finance System - Base Level (GAFS-BL) which is a system in the General Accounting and Finance System - Re-engineered (GAFS-R) umbrella.

**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
- [x] Information Sharing - System to System
- [ ] 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

**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 T7305

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.

**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. DFAS 5015.2-M, Volume

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

(3) Retention Instructions.

Records are retained according to DFAS records retention schedule (Vol 1 - 4500; Vol 2 - 7205, 7221, 7300, 7333, 7335, 7340, 7344).

**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.

5 United States Code (U.S.C.) 301, Departmental Regulations; Department of Defense Financial Management Regulation (DoDFMR) 7000.14-R Vol. 4; 31 U.S.C. Sections 3511, 3512, and 3513; and Executive Order (EO) 9397 Social Security Number (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.

There is no Paper Reduction Act (PRA) requirement for DCMS system. Data is collected only through information sharing – system to system.

## 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.

Draft SSN Justification Memo is awaiting signature from the Chief Information Officer (CIO). Once signed, the memo will be sent to the DFAS Privacy Office for submission to DoD Privacy.

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

Computer Matching - DCMS Mid-Tier data is linked to GAFS-BL records containing the SSN or truncated SSN within the Standard Document 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".

All SSN data is encrypted in storage and in transit. Until a suitable solution can be met for all affected systems, the SSN or truncated SSN must continue to be used in the DCMS Mid-Tier application.

(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

Source system (GAFS-BL, a system in the GAFS-R umbrella) has no plan to eliminate SSN.

**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)*

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

DCMS inherits all physical controls protecting the Defense Information System Agency (DISA) Data Centers Ogden and Mechanicsburg hosting enclaves. The DISA Data Centers' physical infrastructure support consists of environmental controls (including fire suppression systems, temperature control and humidity control), access control (including gates, fences, Common Access Cards, and physical barriers), and facility personnel management (including building maintenance and physical and personnel security). In addition, DCMS inherits all physical controls protecting DFAS facilities and the DFAS Enterprise Local Area Network (ELAN) where developers, users, and application system administrators are located.

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

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

Access to DCMS is limited to persons authorized to service or to use the system in performance of their official duties and who are properly screened and cleared for need-to-know. All applicable administrative controls required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, for the system's security categorization of Moderate Confidentiality, Moderate Integrity, and Moderate Availability, and with a High Privacy Confidentiality Impact Level, have been implemented or documented on the DCMS Plan of Action and Milestones (POA&M) for future implementation. DISA sites may not be encrypted for operational reasons, but they are subject to layered protective measures determined to be adequate for sensitive unclassified information.

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

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

All applicable technical controls required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, for the system's security categorization of Moderate Confidentiality, Moderate Integrity, and Moderate Availability, and with a High Privacy Confidentiality Impact Level, have been implemented or documented on the DCMS Plan of Action and Milestones (POA&M) for future implementation.

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

All Civilian, Military and Contractor personnel accessing DCMS are required to take annual Cybersecurity Awareness Challenge training and Privacy Act and Personally Identifiable Information training which addresses risks and proper safeguarding and use of PII. For Official Use Only (FOUO) statements are included on reports that contain PII data. Hard copy reports are locked until shredded. Electronic records are destroyed by degaussing the media. User manuals, briefings, training material, and other documentation are reviewed to ensure they do not contain PII.

## 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 | 030 |
| [ ] | Yes, SIPRNET | SIPRNET Identification Number | |
| [X] | Yes, RMF tool | RMF tool Identification Number | 5 |
| [ ] | 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: | 8/20/2020 |
| [ ] | 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 007-97-01-01-02-0643-00 If unsure, consult the component IT Budget Point of Contact to obtain the UII

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

## SECTION 4: REVIEW AND APPROVAL SIGNATURES

*Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Mandatory coordinators are: Component CIO, Senior Component Official for Privacy, Component Senior Information Security Officer, and Component Records Officer.*

| | | | |
|---|---|---|---|
| **a. Program Manager or Designee Name** | Guy Moran | (1) Title | System Manager |
| (2) Organization | DFAS-ZTCBE, DCMS SM | (3) Work Telephone | 614.701.2210 |
| (4) DSN | 791-2210 | (5) E-mail address | Guy.D.Moran.Civ@mail.mil |
| (6) Date of Review | 11/06/19 | (7) Signature | MORAN.GUY.D.1151930804 Digitally signed by MORAN.GUY.D.1151930804 Date: 2019.11.06 10:26:53 -05'00' |
| **b. Other Official *(to be used at Component discretion)*** | Ronald Murlin | (1) Title | System Director |
| (2) Organization | DFAS-ZTC, Director, IT Accounting Services | (3) Work Telephone | 216.204.7069 |
| (4) DSN | 580-7069 | (5) E-mail address | ronald.e.murlin.civ@mail.mil |
| (6) Date of Review | 11/08/19 | (7) Signature | MURLIN.RONALD.E.1230833490 Digitally signed by MURLIN.RONALD.E.1230833490 Date: 2019.11.08 11:49:19 -05'00' |
| **c. Other Official** *(to be used at Component discretion)* | | (1) Title | |
| (2) Organization | | (3) Work Telephone | |
| (4) DSN | | (5) E-mail address | |
| (6) Date of Review | | (7) Signature | |
| **d. Component Privacy Officer (CPO)** | Gregory L. Outlaw | (1) Title | Privacy Program Manager |
| (2) Organization | DFAS-ZC, Corporate Communications | (3) Work Telephone | 317.212.4591 |
| (4) DSN | 699.4591 | (5) E-mail address | gregory.l.outlaw.civ@mail.mil |
| (6) Date of Review | 02/05/20 | (7) Signature | OUTLAW.GREGORY.L.1085047317 Digitally signed by OUTLAW.GREGORY.L.1085047317 Date: 2020.02.05 14:58:03 -05'00' |

| | | | |
|---|---|---|---|
| **e. Component Records Officer** | Ralph Mullins | (1) Title | Agency Records Manager |
| (2) Organization | DFAS-IN, ZED | (3) Work Telephone | 317.212.7775 |
| (4) DSN | 699.7775 | (5) E-mail address | ralph.e.mullins.civ@mail.mil |
| (6) Date of Review | 02/06/20 | (7) Signature | MULLINS.RALPH.EDWARD.JR.1059546534 Digitally signed by MULLINS.RALPH.EDWARD.JR.1059546534 Date: 2020.02.06 10:42:34 -05'00' |
| **f. Component Senior Information Security Officer or Designee Name** | Jack Schiller | (1) Title | Deputy Director, IT Shared Services |
| (2) Organization | DFAS-ZTA | (3) Work Telephone | 317.212.1808 |
| (4) DSN | 699.0018 | (5) E-mail address | jack.j.schiller.civ@mail.mil |
| (6) Date of Review: | 11/05/20 | (7) Signature | SCHILLER.JACK.JOSEPH.1457280200 Digitally signed by SCHILLER.JACK.JOSEPH.1457280200 Date: 2020.11.05 21:54:02 -05'00' |
| **g. Senior Component Official for Privacy (SCOP) or Designee Name** | Angela Schultz | (1) Title | Director, Corporate Communications |
| (2) Organization | DFAS-ZC | (3) Work Telephone | 317.212.6195 |
| (4) DSN | 699.6195 | (5) E-mail address | angela.r.schultz6.civ@mail.mil |
| (6) Date of Review | 02/20/20 | (7) Signature | SCHULTZ.ANGELA.RENAE.1230338309 Digitally signed by SCHULTZ.ANGELA.RENAE.1230338309 Date: 2020.02.20 23:17:59 -05'00' |
| **h. Component CIO Reviewing Official Name** | G. Paul Gass | (1) Title | Director, Information Technology |
| (2) Organization | DFAS-ZT | (3) Work Telephone | 317.212.4800 |
| (4) DSN | 699.4800 | (5) E-mail address | gregory.p.gass2.civ@mail.mil |
| (6) Date of Review | 11/23/20 | (7) Signature | GASS.GREGORY.PAUL.II.1109700440 2020.11.23 12:30:12 -05'00' |

**Publishing:** Only Section 1 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: osd.mc-alex.dod-cio.mbx.pia@mail.mill.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Section 1.