

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:

Automated Disbursing System (ADS)

2. DOD COMPONENT NAME:

Defense Finance and Accounting Service

3. PIA APPROVAL DATE:

08/16/21

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: foreign nationals are included in general public.)

- | | |
|--|--|
| <input type="checkbox"/> From members of the general public | <input type="checkbox"/> From Federal employees and/or Federal contractors |
| <input checked="" type="checkbox"/> From both members of the general public and Federal employees and/or Federal contractors | <input type="checkbox"/> Not Collected (if checked proceed to Section 4) |

b. The PII is in a: (Check one)

- | | |
|--|---|
| <input type="checkbox"/> New DoD Information System | <input type="checkbox"/> New Electronic Collection |
| <input checked="" type="checkbox"/> Existing DoD Information System | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> 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 ADS system automates disbursing and collection related functions for various entitlement and accounting systems. ADS accepts payment and collection data through two primary ways:

- 1) Entitlement pay systems generate payment data which is automatically transmitted to ADS via system interfaces; and
- 2) Disbursing Operations users, as well as users at various operating/entitlement organizations, may manually input miscellaneous payments and collections into ADS. ADS processes payment data received and depending on payment type, collects and aggregates payment transactions into:
 - 1) Bulk Electronic Funds Transfer (EFT) payment files for submission to the Federal Reserve Bank (FRB) Automated Clearing House (ACH) network for payment, or
 - 2) Check files transmitted to other entities for printing/payment.

Personally Identifiable Information (PII) includes education information, financial information, mailing/home address, marital status, name(s), rank/grade, Social Security Number (SSN), and Tax Identification Number (TIN). The ability to view PII within the system is limited to users based on need-to-know and least privilege access rules.

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)

Identification – The ADS system automates the processing of disbursements, collections, and reporting payments for a variety of entitlement and accounting systems. Mission-related use – ADS provides this information to the United States (U.S.) Department of the Treasury and FRB for reporting the financial status of the Department of Defense (DoD) funds and providing information on check issues and electronic fund transfers. This system is a disbursing system of record and consolidates disbursing information for the DoD.

e. Do individuals have the opportunity to object to the collection of their PII? 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.

ADS does not collect PII directly from the individual. PII is part of the payment and collection data ADS receives from the entitlement and accounting systems. The entitlement and accounting systems received the information directly from the individual.

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.

ADS does not collect PII directly from the individual. PII is part of the payment and collection data ADS receives from the entitlement and

accounting systems. The entitlement and accounting systems received the information 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 Not Applicable

ADS does not collect PII directly from the individual. PII is part of the payment and collection data ADS receives from the entitlement and accounting systems. The entitlement and accounting systems receives the information 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)

Within the DoD Component

Specify.

ADS shares PII with internal Defense Finance and Accounting Service (DFAS) organizations that demonstrate a need to know (e.g., disbursing operations).

Other DoD Components

Specify.

Army
Navy
Air Force
Marine Corps
Defense Agencies

Other Federal Agencies

Specify.

U.S. Department of the Treasury
FRB
Internal Revenue Service (IRS)
Health and Human Services (HHS)
Department of Energy (DOE)
Environmental Protection Agency (EPA)
Veterans Affairs (VA)
Executive Office of the President (EOP)
Broadcasting Board of Governors (BBG)
Military Sealift Command (MSC)

State and Local Agencies

Specify.

Court Order State Garnishment
State and Local Tax Agencies

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.

Various U.S. Banks & Colleges
– Grants may contain TIN

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

ADS receives PII from:
Defense Civilian Payroll System (DCPS)
Defense Joint Military Payroll System (DJMS) - Active Command (AC)
DJMS - Reserve Command (RC)
Defense Retired and Annuitant Pay System (DRAS)
One Pay
Navy Integrated Automated Travel System (IATS)
Navy Enterprise Resource Planning (ERP)
General Fund Enterprise Business System (GFEBS)

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://dpcl.d.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.

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

(3) Retention Instructions.

Cutoff at end of fiscal year upon verification of deposits or resolution of any outstanding adjustments. 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 statute 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.

Department of Defense Financial Management Regulation (DoDFMR) 7000.14-R, Vol. 5, Chapter 20; 31 United States Code (U.S.C.) Sections 3511, 3512, and 3513; 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.

ADS receives all data through entitlement systems and as such does not have a Paper Reduction Act (PRA) requirement. Instruction

provided in DoD 8910.01, the entitlement systems, clears data at the 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)

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

TIN

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.

The ADS SSN Justification Memo received signature of DFAS Chief Information Officer (CIO) signature dated March 22, 2021.

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

(8) Computer Matching. Systems, processes, or forms that interact with other Government agencies may require the continued use of the SSN as a primary identifier until such time as the applications to which they are linked move to some other identifier as a primary means for transferring, matching, or checking information. These applications shall be rigorously scrutinized to determine the availability of some other means for conducting these transactions. (11) Legacy System Interface. Many systems, processes, or forms that do not meet the criteria in sub-paragraphs 2.c.(1) through 2.c.(10) of this enclosure for the continued use of the SSN may not be able to transition to another identifier in a timely manner due to an interface with a legacy system still using the SSN, or due to the excessive cost associated with the change. In these cases, the continued use of the SSN may be acceptable for a specified period of time, provided that formalized, written plans are in place for the migration away from the SSN in the future. Plans to alter these use cases must take into account interactions with other applications as well as all methods for entry, processing, or transfer of information from said application. It is critical that transfer away from the SSN does not cause unacceptably long interruptions to continued operations.

(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".

Truncating SSNs and removing full SSNs from hard copy reports.

(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

ADS utilizes SSN information to conduct its daily business transactions. Mitigating efforts include masking of SSN information. ADS operates in a secure computing environment to prevent compromise of data.

b. What is the PII confidentiality impact level²?

Low Moderate High

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

²Guidance 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)*

- | | |
|---|--|
| <input checked="" type="checkbox"/> Cipher Locks | <input checked="" type="checkbox"/> Closed Circuit TV (CCTV) |
| <input checked="" type="checkbox"/> Combination Locks | <input checked="" type="checkbox"/> Identification Badges |
| <input checked="" type="checkbox"/> Key Cards | <input checked="" type="checkbox"/> Safes |
| <input checked="" type="checkbox"/> Security Guards | <input checked="" type="checkbox"/> If Other, enter the information in the box below |

ADS inherits controls relevant to physical controls protecting the Defense Information Systems Agency (DISA) hosting enclaves as well as inheriting physical controls protecting the DFAS where developers, users, and system administrators are located.

(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

Since ADS is located within the DISA secured enclave, ADS operates under layered protective measures determined to be adequate for sensitive unclassified information. Additionally, ADS inherits controls relevant to administrative controls protecting DISA hosting enclaves as well as inheriting administrative controls protecting the DFAS where developers, users, and system administrators are located.

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

- | | | |
|---|---|--|
| <input type="checkbox"/> Biometrics | <input checked="" type="checkbox"/> Common Access Card (CAC) | <input checked="" type="checkbox"/> DoD Public Key Infrastructure Certificates |
| <input checked="" type="checkbox"/> Encryption of Data at Rest | <input checked="" type="checkbox"/> Encryption of Data in Transit | <input type="checkbox"/> External Certificate Authority Certificates |
| <input checked="" type="checkbox"/> Firewall | <input checked="" type="checkbox"/> Intrusion Detection System (IDS) | <input checked="" type="checkbox"/> Least Privilege Access |
| <input checked="" type="checkbox"/> Role-Based Access Controls | <input type="checkbox"/> Used Only for Privileged (Elevated Roles) | <input checked="" type="checkbox"/> User Identification and Password |
| <input checked="" type="checkbox"/> Virtual Private Network (VPN) | <input type="checkbox"/> If Other, enter the information in the box below | |

ADS inherits controls relevant to technical controls protecting DISA hosting enclaves as well as inheriting technical controls protecting DFAS where developers, users, and system administrators are located.

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

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) tool³?

<input checked="" type="checkbox"/> Yes, DITPR	DITPR System Identification Number	<input type="text" value="36"/>
<input type="checkbox"/> Yes, SIPRNET	SIPRNET Identification Number	<input type="text"/>
<input checked="" type="checkbox"/> Yes, RMF tool	RMF tool Identification Number	<input type="text" value="86"/>
<input type="checkbox"/> 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:

<input checked="" type="checkbox"/> Authorization to Operate (ATO)	Date Granted:	<input type="text" value="12/11/2018"/>
<input type="checkbox"/> ATO with Conditions	Date Granted:	<input type="text"/>
<input type="checkbox"/> Denial of Authorization to Operate (DATO)	Date Granted:	<input type="text"/>
<input type="checkbox"/> Interim Authorization to Test (IATT)	Date Granted:	<input type="text"/>

(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?

Yes No

If "Yes," Enter UII If unsure, consult the component IT Budget Point of Contact to obtain the UII

³Guidance 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>.