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:

Financial Accounting Management Information System (FAMIS) -WCF

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

10/02/19

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
- [x] From Federal employees and/or Federal contractors
- [ ] 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.

FAMIS-WCF is a financial accounting system that executes financial transactions, performs financial inquires and creates financial reporting. The systems collects and maintains time and attendance and travel obligation information via an interface file from the Defense Civilian Pay System (DCPS) and the Defense travel System (DTS). The authority to collect, use and maintain the applicable information is noted from the DoD Financial Management Regulation (FMR) Volume 8, Chapter 2, Paragraph 020205
The following authority permits FAMIS-WCF to collect data:
- DISA CIO Memorandum, Subject: Authorization to Operate for the Federal Financial Accounting Management Information System (FAMIS), Tracking Number 1289711, dated 24 Aug 2009.
PII collected includes: Vendor and customer Point of Contact (POC) information, Employee Names, and Government Social Security Numbers for financial management purposes.

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)*

FAMIS-WCF receives a bi-weekly data interface of gross pay and master employee data from DCPS. Data records are uniquely identified by Social Security Number for the purpose of cost accounting, billing customers and recording financial transactions.

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.

FAMIS-WCF is not the authoritative data source of PII. Individuals do not have the opportunity to object to the collection of PII within FAMIS-WCF. The system collects and maintains time and attendance and travel obligation information via interface file and DCPS and DTS where the initial collection and authorization of PII is performed.

The PIA completed for DCPS states: "Individuals are provided the opportunity to object to the collection of their personal information, such as SSN, that is collected using various personnel forms when the individual becomes a federal government employee."

The PIA completed for DTS states: "Privacy notice presented to user prior to login states "DISCLOSURE: Voluntary, however, failure to provide all of the requested information may preclude the processing of both the travel request and claim for reimbursement."

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.

FAMIS-WCF is not the authoritative data source of PII. Individuals do not have the opportunity to object to the collection of PII within FAMIS-WCF. The system collects and maintains time and attendance and travel obligation information via interface file and DCPS and DTS where the initial collection and authorization of PII is performed.

The PIA completed for DCPS states: "When personal information is collected by the Human Resources Office or another office, the forms used to collect the data contain a Privacy Act Statement."

The PIA completed for DTS states: "Privacy notice presented to user prior to login states "DISCLOSURE: Voluntary, however, failure to provide all of the requested information may preclude the processing of both the travel request and claim for reimbursement."

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.)*

- [x] Privacy Act Statement
- [ ] Privacy Advisory
- [ ] Not Applicable

FAMIS-WCF is not the authoritative data source of PII. Individuals do not have the opportunity to object to the collection of PII within FAMIS-WCF. The system collects and maintains time and attendance and travel obligation information via interface file from DCPS and DTS where the initial collection and authorization of PII is performed.

The PIA completed for DCPS states: "When personal information is collected by the Human Resources Office or another office, the forms used to collect the data contain a Privacy Act Statement."

The PIA completed for DTS states: "Privacy notice presented to user prior to login states "DISCLOSURE: Voluntary, however, failure to provide all of the requested information may preclude the processing of both the travel request and claim for reimbursement."

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.	DISA Financial Management Personnel
[x] Other DoD Components	Specify.	DFAS Financial Management Personnel
[ ] 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

FAMIS-WCF is not the authoritative source of PII. The systems collects and maintains time and attendance and travel obligation information via an interface file from DCPS and DTS where the initial collection and authorization of PII is performed.

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

FAMIS-WCF is not the authoritative source of PII. The systems collects and maintains time and attendance and travel obligation information via an interface file from DCPS and DTS where the initial collection and authorization of PII is performed.

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 K890.30

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.

N/A

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. General Records Schedule 1.1

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

(3) Retention Instructions.

Item 011: This system's outputs are accounting related transactions and reports. Disposition Instruction is temporary: Destroy when business use ceases. Note: Other applicable guidance related to accounting files should be adhered to enable access by GAO, Office of the Inspector General, or other authority audit.

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.

The authority to collect, use and maintain the applicable information is noted from the DoD Financial Management Regulation (FMR) Volume 8, Chapter 2, Paragraph 020205

The following authority permits FAMIS-WCF to collect data:

- DISA CIO Memorandum, Subject: Authorization to Operate for the Federal Financial Accounting Management Information System (FAMIS), Tracking Number 1289711, dated 24 Aug 2009.

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.

OMB approval is not required in accordance with Section 8.b.11 of Enclosure 3 of DoD Manual 8910.01 - Volume 2

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	

Vendor and customer Point of Contact (POC) information.

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.

Vincent Stephen Lance - 2018-06-21

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

Use of the SSN within the FAMIS-WCF system fall under Acceptable Use 2.c.(4) of the DOD Instruction 1000-30 SSN Reduction Act: Acceptable Use 2.c.(4) is applicable to Interactions with Financial Institutions. The SSN is contained in the Gross Pay Files and Master Employee Records obtained through transactions with DoD financial institutions and are used for processing the labor data within the FAMIS-WCF system.

(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".

Information is restricted to DISA and Defense Finance and Accounting Service (DFAS) financial management personnel and only available on a need to know basis as prescribed by the roles and responsibilities assigned for financial management purposes. Printing of the information is not required. At database level, data at rest or in transit is encrypted according to Federal Information Processing Standards (FIPS) 140-2.

(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

FAMIS-WCF is not the authoritative data source of the PII.

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

PII information is maintained electronically at the DISA Datacenter Oklahoma, secured through the physical controls noted above and at user locations which include security badge access.

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

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

The DISA Field Security Office (FSO) conducts information assurance reviews in accordance with the DoD Risk Management Framework (RMF). The Datacenters conduct self-assessments of assets in accordance with FISMA guidance. In addition, records or logs of security checks and inspections are maintained, Veritas Netbackup used for the DISA operation environments is encrypted and backups are secured at an off-site location according to defined DISA policy.

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

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

FAMIS-CS Modernization adheres to the policies and guidance provided by DISA and DoD policy regarding passwords, logins and account management. User and administrator accounts are CAC restricted. Oracle service accounts follow established policy for uniqueness, password length, complexity, maximum age, password history and masking at entry points. Service account passwords are encrypted with Rivest, Shamir & Adleman (RSA) Advanced Encryption Standard (AES) 128/256-bit encryption in Cipher Block Chaining (CBC) mode and Secure Hashing Algorithm (SHA-1) according to encryption methods approved under FIPS-140-2.

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

None

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	16495
[ ]	Yes, SIPRNET	SIPRNET Identification Number	
[X]	Yes, RMF tool	RMF tool Identification Number	541
[ ]	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:	3/21/2018
[ ]	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 00010089 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	Robert Barrow	(1) Title	Program Manager
(2) Organization	DISA Development & Business Center	(3) Work Telephone	Office: 301-225-6646 DSN: 375-6646
(4) DSN	DSN: 375-6646	(5) E-mail address	robert.w.barrow.civ@mail.mil
(6) Date of Review	09/05/19	(7) Signature	BARROW.ROBERT.WEBSTER.1044156837 Digitally signed by BARROW.ROBERT.WEBSTER.1044156837 Date: 2019.09.05 12:21:48 -04'00'
b. Other Official *(to be used at Component discretion)*	Gary Hartzog	(1) Title	Information Systems Security Manager
(2) Organization	DISA	(3) Work Telephone	850 452-7831
(4) DSN	459-7831	(5) E-mail address	gary.r.hartzog.ctr@mail.mil
(6) Date of Review	09/05/19	(7) Signature	HARTZOG.GARY.RAY.1067345416 Digitally signed by HARTZOG.GARY.RAY.1067345416 Date: 2019.09.05 11:12:40 -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)	Jeanette M. Weathers-Jenkins	(1) Title	DISA Privacy Officer
(2) Organization	RME/RE2	(3) Work Telephone	301-225-8158
(4) DSN		(5) E-mail address	jeanette.m.weathersjenkins.civ@mail.mil
(6) Date of Review		(7) Signature	WEATHERSJENKINS.JEANETTE.M.1181238670 Digitally signed by WEATHERSJENKINS.JEANETTE.M.1181238670 Date: 2019.09.13 11:24:50 -04'00'

e. Component Records Officer	Ms. Shannon S. Lawrence	(1) Title	Records and Information Management Officer
(2) Organization	CIO/REC2	(3) Work Telephone	301-225-4003
(4) DSN	312-375-4003	(5) E-mail address	shannon.s.lawrence2.civ@mail.mil
(6) Date of Review	09/18/19	(7) Signature	LAWRENCE.SHANNON.SELENE.1286005698 Digitally signed by LAWRENCE.SHANNON.SELENE.1286005698 Date: 2019.09.18 13:43:22 -04'00'
f. Component Senior Information Security Officer or Designee Name	Mrs. Alma J. Miller	(1) Title	Senior Information Security Officer
(2) Organization	RME/RE2	(3) Work Telephone	301-225-8244
(4) DSN	312-375-8244	(5) E-mail address	alma.j.miller2@mail.mil
(6) Date of Review:	09/18/19	(7) Signature	MILLER.ALMA.J.1113816224 Digitally signed by MILLER.ALMA.J.1113816224 Date: 2019.09.18 14:46:59 -04'00'
g. Senior Component Official for Privacy (SCOP) or Designee Name	Mrs. Myra McIntosh-Williams	(1) Title	Deputy Risk Management Executive and Senior Component Official for Privacy
(2) Organization	RME	(3) Work Telephone	301-225-8625
(4) DSN	312-375-8625	(5) E-mail address	myra.d.mcintoshwilliams.civ@mail.mil
(6) Date of Review		(7) Signature	
h. Component CIO Reviewing Official Name	Mr. Roger S. Greenwell / Ms. Jennifer L. Augustine	(1) Title	Chief Information Officer Deputy Chief Information Officer
(2) Organization	CIO / Deputy CIO	(3) Work Telephone	301-225-3214 / 301-225-6700
(4) DSN	312-375-3214 312-375-6700	(5) E-mail address	ROGER.S.GREENWELL.CIV@MAIL.MIL JENNIFER.L.AUGUSTINE4.CIV@MAIL.MIL
(6) Date of Review	10/02/19	(7) Signature	Digitally signed by AUGUSTINE.JENNIFER.L.1229169668 Date: 2019.10.02 08:52:50 -04'00'

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.