SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.
☒ (2) Yes, from Federal personnel* and/or Federal contractors.
☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.
SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- [x] Yes, DITPR
  Enter DITPR System Identification Number: 7905
- [x] Yes, SIPRNET
  Enter SIPRNET Identification Number:
- [ ] No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- [ ] Yes
- [x] No

If “Yes,” enter UPI:

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

- [ ] Yes
- [x] No

If “Yes,” enter Privacy Act SORN Identifier: N/A for current usage. Should usage be expanded in the future

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/
or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.
e. Does this DoD information system or electronic collection have an 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

Enter OMB Control Number

Enter Expiration Date

☒ No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

   (b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

BAM does not collect new information or information directly from individuals. BAM is a Mission Support business tool used to perform analysis on data collected and housed by native systems. All information collected by BAM is transferred via secure file transfer from other existing systems. Many of these systems, such as Integrated Accounts Payable System (IAPS), have their own Privacy Impact Assessments, and have been authorized by the following:


Identifiable information is collected as part of existing financial transaction records for business activity monitoring purposes. Existing data will be analyzed by the BAM tool to identify, monitor, reduce or eliminate transactional errors, misuse, and potential fraud resulting in financial discrepancies, losses, and workflow inefficiencies. This analysis is in accordance with the requirements set forth in the Improper Payments Information Act of 2002 (Public Law No: 107-300).
g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

DFAS implemented BAM to evaluate financial transactions to determine whether or not proper payments were made. This analysis is in accordance with the requirements set forth in the Improper Payments Information Act of 2002 (Public Law No: 107-300).

BAM does not collect data directly from individuals. All data utilized by BAM is originally collected by existing systems it receives information from. Information may include: Social Security if a vendor uses it instead of a tax identification number, Bank Routing Number, and Tax ID. Specific data requirements will be determined as each system is integrated with BAM.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The BAM application owners will identify specific access privileges and authority. The adopted security measures will allow access to only those individuals who have a need-to-know and are authorized to access the system. Each user will be restricted to specific actions by the software application and specific web screens by BAM, therefore minimizing the access to the system. Developers, in the context of BAM, only modify configurable items to improve data analytics and do not have access to nor develop BAM source code. Developers do not have access to production systems and will only have access to the portion of the system on which they are working. System administrators will strictly control and grant permission for access to specific modules as authorized by the business application owners. System, Security, and Application Administrators do not have write access in the production application.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

- **Within the DoD Component.**
  - Specify. Shared with only DFAS Accounts Payable-related Operations and contracting staff maintaining BAM servers.

- **Other DoD Components.**

- **Other Federal Agencies.**
  - Specify.

- **State and Local Agencies.**
  - Specify.

- **Contractor** (Enter name and describe the language in the contract that safeguards PII.)
  - Specify. BAM is a business tool owned by a contractor which provides Managed Services and all hardware and software are managed by the external contractor with privileged user
Not applicable since BAM will never collect information directly from individuals. Privacy Act Statements and notices for each specific system from which BAM will receive its information are provided to individuals before using that system and use is typically voluntary. These statements are typically provided on the form used to collect the data or on the Web-based application used to collect the information.

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

☐ Yes  ☒ No

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

j. 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.
k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement  ☐ Privacy Advisory

☐ Other  ☒ None

Describe each applicable format.

NOTE:

Sections 1 and 2 above are to be posted to the Component’s Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.