PRIVACY IMPACT ASSESSMENT (PIA)

For the

Integrated Center Information System (ICIS)

Aviation and Missile Research, Development, and Engineering Center

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**
- ☐ **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?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 16165 (DA301040)
- ☐ **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**
- ☒ **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**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier: A0690-200 DAPE, Dept of Army Civilian Personnel Systems

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.

5 U.S.C 301, Departmental Regulations; 10 U.S.C. 3013, Secretary of the Army; Army Regulation 690-200, General Personnel Provisions, and E.O. 9397 (SSN).

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.

ICIS is used to help manage AMRDEC's business assets. It is a relational database application developed to capture and track manpower data, budget and funding information, contract award information, and scopes of work in support of Program Executive Offices (PEOs) and/or Project Management Offices (PMOs). The system assists AMRDEC analysts in response to data calls by providing one consolidated source of information.

ICIS provides budgeting requirements, TDA, manpower, and execution management capabilities to authorized users within AMRDEC. The system provides the functions, capabilities, and data that a resource manager or human resource manager requires to develop a Program Executive Memorandum (dollars, manpower, assets, formulate budget (dollars, manpower, assets), authorize and distribute funds, execute budget (dollars, manpower, assets), manage authorized and required spaces, manage end strength, and manage personnel and organization functions. ICIS is divided into four main modules: Personnel & Administrative, Budget and Funding, Contract Tracking, and Scopes of Work.

The Personnel & Administrative Module has PII that is needed for administrative purposes for determination and maintenance of an individual's employment status, qualifications, and other personnel-related eligibilities and issues including employee pay and TDA information. This data is either collected directly from the employee during in-processing or merged from other government/Army databases and centralized to create one central source of information for HR functions. It contains detailed personnel data on each employee; travel, awards, training data, educational information; TDA data; lab demo performance appraisals; and visitor requests.

The type of PII collected is personal, employment, educational, and financial information.

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

The security risk associated with maintaining PII in an electronic environment has been identified and mitigated through administrative, technical, and physical safeguards as well as with policy and procedures for handling, using, maintaining PII and training for authorized users of PII data. Due to the stringent safeguards and access requirements, the system and data are secure and it is unlikely that the data would be compromised or provided to any unauthorized individuals or agencies.

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. Aviation and Missile Research, Development, and Engineering Center authorized users. This is an AMRDEC internal use only system and as such data is shared with authorized users who have a need to know the data in order to perform personnel services within the organization. Information is available to authorized users with a need to know in order to perform official government duties. Internal DOD agencies that would obtain access to PII in

this system, on request in support of an authorized investigation or audit, may include DOD IG, DCIS, Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, and ASA FM&C. In addition, the DOD blanket routine used apply to this system.

☒ **Other DoD Components.**

Specify. In order to correct or update an employee's personnel information, ICIS may potentially share PII with any DOD agency Staff Principals.

☒ **Other Federal Agencies.**

Specify. In order to correct or update an employee's personnel information, ICIS may potentially share PII with any Federal agency.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. CSC Contract No. W31P4Q-05-A-0028 is the contractor providing support and maintenance for ICIS. The system developers have access to the database. Contractor personnel provide database administration, application development, system administration, data management, user support, and is the webmaster for the ICIS application. The contractor will implement and maintain appropriate IA management, operational, and technical controls and processes to ensure compliance with DOD and DA requirements.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

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.

Some employee personal data must be collected directly and immediately from individuals when they in-process into AMRDEC. For collection of this data, employees are provided a Privacy Act Statement on AMRDEC Form 690-R-E which tells them why the data is needed, how the data will be used, and any possible consequences of not providing the data, thus employees do have the opportunity to object to collection of their PII. However after in-processing, other personally identifiable information data is populated into ICIS from DOD/Army interfaces with systems outside of AMRDEC, such as SOMARDS (financial), DCPDS (personnel), TIPS (training), PCMS (government credit card), ATAAPS (timecard/labor information), DTS (travel system). Individuals implicitly consent to capture and use of that information at the time of employment in the Department of the Army.

(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.

For PII data collected from employees during AMRDEC in-processing, employees are told how their PII will be used in the Privacy Act Statement on AMRDEC Form 690-R-E. For PII downloaded into ICIS from other Army information systems, individuals implicitly consent to capture and use of that information at the time of employment in the Department of the Army, at which time they are provided a Privacy Act Statement/ Advisory when the data was collected for each of those Army information systems and that Privacy Act Statement/Advisory would define the specific uses of the PII collected.

(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.

Some Privacy Data is obtained via downloads from other DOD/Army information systems and Privacy Act Statements or Privacy Advisories are provided to individuals when they provide personal data to those systems. For personal data collected directly from individuals when in-processing into AMRDEC, a Privacy Act Statement is provided on AMRDEC Form 690-R-E. If the personal data is collected verbally from an individual, then the individual is read a Privacy Act Advisory which tells them why the data is needed, how it will be used, and whether providing the information requested is voluntary or mandatory as well as possible consequences if the data is not provided. Privacy Data is only used when absolutely necessary to interface with other DOD/Army information systems. Policies and procedures are in place for safe handling and maintaining privacy data. Access to this data is restricted via the ICIS application and requires each ICIS user having access to privacy data to have limits on their access to the privacy data.

The following statement is on the AMRDEC Form 690-R-E:

PRIVACY ACT STATEMENT
The information you provide to the AMRDEC Integrated Center Information System (ICIS) is covered by the Privacy Act of 1974 (Public Law 92-549). This notice informs you of the purposes and routine uses of this information. For specific questions regarding your personal information, please contact