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:

Department of Defense (DOD) Public Key Infrastructure (PKI)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

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
- ☐ 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
- ☒ 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.

The DOD PKI system creates and manages digital certificates for the use of Public Key Encryption. These certificates are used for email encryption as well as identification and authorization activities throughout the DOD. The key functionality of the PKI is the asymmetrical nature of the encryption meaning in order for the system to work the public key is made available. The certificates contain Name, Business email address and the DOD ID number of the individual.

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)*

The DOD PKI system creates and manages digital certificates for the use of Public Key Encryption. These certificates are used for email encryption as well as identification and authorization activities throughout the DOD. The key functionality of the PKI is the asymmetrical nature of the encryption meaning in order for the system to work the public key is made available. The certificates contain Name, Business email address and the DOD ID number of the individual.

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.

All persons issued a Common Access Card (CAC) will have certificates created on the PKI system the certificate will be tied to their identity via their name,business email address and DOD ID number.

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.

The PKI program use of PKI are limited to legitimate business use within the DOD for identity and authentication purposes.

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

Not Applicable

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.	All systems using PKI within DISA
☒ Other DoD Components	Specify.	All systems using PKI within DOD
☒ Other Federal Agencies	Specify.	All Federal Agencies that use DOD PKI certificates , Additionally Federal law enforcement can subpoena a certificate to decrypt encrypted email exchanges in for the purpose of criminal investigation or prosecution.
☒ State and Local Agencies	Specify.	Any agency who receives an email signed with a DOD certificate, Additionally law enforcement can subpoena a certificate to decrypt encrypted email exchanges in for the purpose of criminal investigation or prosecution.
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.	Anyone who receives an email signed with a DOD certificate would have access to the public certificate. As we are considering all potential information exchange outside of just DOD PKI there is no limit for who could receive a public certificate.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

- ☐ Individuals
- ☒ Existing DoD Information Systems
- ☐ Other Federal Information Systems
- ☐ Databases
- ☐ Commercial Systems

DOD PKI

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
- ☒ 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

Defense Manpower Data Center - DMDC
Trusted Associate Sponsorship System -TASS

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 K890.14 DoD

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. N1-GRS07-3, item 13a1

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

(3) Retention Instructions.

Department of Defense Public Key Infrastructure Second Layer Certification Authority Certification Practice Statement, dtd June 2017

5.5.2 Retention Period for Archive
Archive records are kept for a period of at least ten years, six months.

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.

DoD Instruction DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling.
DoD Instruction (DoDI) 8520.2 in accordance with the authority
in DoD Directive (DoDD) 5144.1 to establish and implement policy, assign
responsibilities, and prescribe procedures for developing and implementing a DoD-wide PKI and
enhancing the security of DoD information systems by enabling these systems to use PKI for
authentication, digital signatures, and encryption.

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 Control Number: 0704-0415; Expiration Date: None