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:

Electronic Security System (C-CURE 9000)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

White House Communications Agency

3. PIA APPROVAL DATE:

09/06/18

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
- [ ] Existing DoD Information System
- [x] 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 purpose of the Badge and Access Control System is to authenticate authorized access into and within certain areas of WHCA facilities. The information collected and used by the Access Control System is badge/pass issuance records, photograph of person, identification card issue and expiration dates, Social Security Number, First, Middle and Last name, Clearance level, and Common Access Card (CAC)/ Personal Identity Verification-Interoperability (PIV-I) Full FASC-N CHUID number.

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)*

Authentication of personnel gaining access to the WHCA facilities.

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

Individuals sign DD Form 2842s; which informs of their right to refusal of providing the requested information, it is strictly voluntary; however, their denial may result in the denial of PKI keys, because the access control system operates on PKI private keys, thus disallowing access to the facility; without access to the facility, the member may not be able to perform his/her duties.

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.

The members cannot object to providing the aforementioned PII because this data is used to authentic access into the facility. It is collected from their Common Access Card (CAC), which is used to scan in/out of the controlled facility.

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

AUTHORITY: 5 U.S.C. 301, Departmental Regulation; 44 U.S.C. 3101.
PRINCIPAL PURPOSE(S): To collect personal identifiers during the certification registration process, to ensure positive identification of the subscriber who signs this form.
ROUTINE USES: Information is used in the DoD PKI certification registration process.
DISCLOSURE: Voluntary; however failure to provide the information may result in denial of issuance of a token containing PKI private

keys. The member has been authorized to receive one or more private and public key pairs and associated certificates. A private key enables digital signature of documents and messages. People and electronic systems inside and outside the DoD will use public keys associated with private keys to verify digital signatures, or to verify identities when attempting to authenticate to systems, or to encrypt data. The certificates and private keys are issued on a token (e.g., CAC) another hardware token. The certificates and private keys on your token are property of the US government and may be used only for official purposes.
Liability: The member will have no claim against the DoD arising from the use of subscriber's certificates, the key recovery process or a Certification Authority (CA's) determination to terminate or revoke a cert. DoD is not liable for any loses, including direct or indirect, incidental, consequential, special or punitive damages, arising out of or relating to any certificate issued by a DoD CA.
Governing Law: DoD Public Key Certs are governed by the laws of the United States of America.

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.	Office of the Inspector General; Office of the General Counsel
[ ]	Other DoD Components	Specify.	
[ ]	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)*

- [x] Individuals
- [ ] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [ ] Databases
- [ ] Commercial Systems

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [ ] E-mail
- [x] 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

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.

[x] Yes [ ] No

If "Yes," enter SORN System Identifier WHCA.09

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. GRS 5.6, Item 120

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

(3) Retention Instructions.

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.

10 U.S.C. 193 and 142; Department of Defense Directive 5105.19, Defense Information Systems Agency; Dept of Defense Directive 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board; HSPD-12

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.

18 Jun 2018