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:

Basic Employee And Security Tracker (BEAST)

2. DOD COMPONENT NAME:

White House Communications Agency

3. PIA APPROVAL DATE:

08/30/2018

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.

To manage personnel and security records for the purpose of validation, analysis, and appraisal throughout the life-cycle. This system is used to track security, sensitive items such as access/accountable badges and employment data of military personnel, DoD Government employees, and DoD contractors who support the White House Communications Agency (WHCA) and/or the White House Military Office (WHMO)

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)*

Mission Related Use (e.g., administrative use, background investigations, authentication, identification and verification).

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.

The members can object at anytime to the collection of their PII; however failure to consent could lead to non-consideration for Presidential Support Duty. Employment/Duty at WHMO/WHCA is 100% voluntary.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [x] 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.

During the security interview, at the time of application or anytime thereafter, the member can non-consent to the use of their PII; however failure to consent could lead to non-consideration or dismissal from Presidential Support Duty. Employment/Duty at WHMO/WHCA is 100% voluntary.

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
- [x] Privacy Advisory
- [ ] Not Applicable

PRIVACY ACT STATEMENT: The Authority for collecting the requested information resides in Executive Orders 10450 (Security requirements for Government employment), 11652 (Classification and declassification of national security information and material) & 9397 (Federal Agency Use of Social Security Numbers). The information is used in making security determinations, granting access to classified/ PSD protected information and for making personnel management decisions. Routine uses include determining the scope and coverage of a personnel security investigation, checking investigative leads assuring completeness of the investigation, and providing evaluators and/or adjudicators with basic personal history information relevant to security/suitability and are referenced in the SORN. Information may be

disclosed to and maintained by Government agencies and administrative personnel involved in processing security actions that evolve during the course of these determinations. When populated with data, this questionnaire becomes PII and must be encrypted prior to transmittal. The personal data collection will be transferred into an approved system of record, under an Authority to Operate, granted on 10 Jul 09, under federal register chronicle 78 FR 70543, 26 Nov 13, 79 FR 34299, 16 Jun 14 and maintained for up to 75 years. The SORN allowing this collection can be found at: http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Article-View/Article/570748/kwhc08/

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.	Human Resource Office, Security and the System Administrators (IAW non-disclosure agreements)
[X]	Other DoD Components	Specify.	White House Military Office (WHMO)
[X]	Other Federal Agencies	Specify.	United States Secret Service (USSS)
[ ]	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	[ ]	Databases
[X]	Existing DoD Information Systems	[ ]	Commercial Systems
[ ]	Other Federal Information Systems		

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

[X]	E-mail	[X]	Official Form (*Enter Form Number(s) in the box below)*
[X]	Face-to-Face Contact	[ ]	Paper
[ ]	Fax	[ ]	Telephone Interview
[ ]	Information Sharing - System to System	[X]	Website/E-Form
[ ]	Other *(If Other, enter the information in the box below)*		

WHCA Form 89 (WHCA Security Questionnaire), DISA recruiting website: http://www.disa.mil/careers/whca, DD Form 1172-2 (Application for Identification Card/DEERS), J2 COR-OGA Form. Members can also opt to email the data, following encryption and data in motion requirements.

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 KWHC-08

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. GRS: N1-330-08-010 (Pending)

(2) If pending, provide the date the SF-115 was submitted to NARA. 5/19/2017

(3) Retention Instructions.

Basic Employee and Security Tracker (BEAST). Proposed disposition for the BEAST database is Temporary - maintain for 75 years, then destroy.

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.

5 U.S.C. 1303 Investigations; 5 U.S.C 3301, Civil service; 44 U.S.C. 3101, Administrative Procedure Act; DoDI 5025.01, DoD Directives Program; and E.O. 9397 (SSN), as amended

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 - 0704-0507