DEPARTMENT OF DEFENSE
Defense Information Systems Agency
Narrative Statement on Altered Systems of Records
Under the Privacy Act of 1974

1. System identifier/name: KWHC 08, entitled BEAST formerly known as Defense Ready.

2. Responsible official: Kevin A. Gifford, System Manager, White House Communications Agency (WHCA), Executive Network Command (ENC), Information Systems Division, (ISD) Enterprise Architect Branch (EAB), 2743 Defense Blvd SW, Bldg. 399, Anacostia Annex, Washington DC 20373-5117, Telephone: 202-757-5758.

3. Nature of proposed changes for the system: The Defense Information Systems Agency (DISA) is proposing to alter the system of records by updating the system name, from Defense Ready to Basic Employee and Security Tracker (BEAST). Authorities, routine uses, safeguards, notification procedure, and record access procedures will remain the same under the previously approved version.

4. Authority for the maintenance of the system: DoDI 5210.55, Department of Defense Presidential Support Program; DoD Directive 1000.17, Detail of DoD Personnel Assigned to Duty Outside the Department of Defense; DoDI 5210.8, Selection of DoD Personnel and Contractor Employees for Assignment to PSAs; DoD 5200.2-R, DoD Personnel Security Program, January 1987 and E.O. 9397 (SSN), as amended.

5. Provide the agency's evaluation on the probable or potential effects on the privacy of individuals: In developing this system of records notice, DISA has carefully reviewed the safeguards established for the system to ensure they are compliant with DoD requirements and are appropriate to the sensitivity of the information stored within this system. BEAST records are maintained in areas only physically accessible to system administrators, while virtual access is limited to Human Capitol/Resource Professionals and Security Officers who use the records to perform their duties. Analyst are provided access on a case-by-case basis, for agency analysis. All records are maintained in a facility, which is guarded 24-hours a day, 365 days a year, residing on a DoD installation, protected by police officers, contract guard personnel and active duty Marines. The system is housed inside of a vaulted Sensitive Compartmented Information Facility (SCIF), protected by a blast door and an intrusion detection systems, accessible only to authorized personnel with a need-to-know who are properly screened, cleared, and trained. System access requires a government Common Access Card (CAC) and associated Personal Identification Number (PIN) in addition to user identifications and passwords. Any paper generated files are disposed of via a GSA approved industrial cross-cut shredder IAW WHMO's 100% shred policy.

6. Routine use compatibility: The routine uses are consistent with the purpose for which the information is collected, necessary and proper. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

(a) Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

(b) Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

(c) Data Breach Remediation Purposes Routine Use: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when

i. The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised;

ii. The Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and

iii. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

7. OMB public information collection requirements:

OMB collection required: Yes
OMB Control Number: 0704-0507
Date submitted to OMB: 12/14/2016
Expiration Date: 02/28/2020

Provide titles of any information collection requests (e.g. forms and number, surveys, interviews scripts, etc.) contained in the system of records.

- WHCA/WHMO Security Screening Questionnaire (SSQ) - WHCA Form 89 and on-line application via the http://disa.mil/careers/whca DEPS protected website.

If collecting on members of the public and no OMB approval is required, state the applicable exception(s): N/A.

Information required by DPCLTD (not submitted to OMB).

8. Name of IT system and DITPR Number (state NONE if paper records only): DefenseReady – 0704-0507 (will be remained to BEAST)

9. Is this system, in whole or in part, being maintained, collected, used, or disseminated by a contractor? Yes. Federal Acquisition Regulation (FAR) clause subpart 24.1 is included in the contract.

Billing Code:
DEPARTMENT OF DEFENSE

[Docket ID:] Privacy Act of 1974; System of Records
AGENCY: Defense Information Systems Agency, DoD
ACTION: Notice to alter a System of Records

SUMMARY: Pursuant to the Privacy Act of 1974, 5 U.S.C. 552a, and Office of Management and Budget (OMB) Circular No. A–130, notice is hereby given that the Defense Information Systems Agency (DISA) proposes to alter a system of records, KWHC 08, entitled "DefenseReady," last published at June 16, 2014, 79 FR 34299.

The system of records exists to make accessibility and hiring decisions; it will be used [to] manage personnel and security records for the purpose of security clearance and suitability validation, analysis, and appraisals/evaluations throughout the lifecycle. This system is used specifically to track travel, security, sensitive items such as access/accountable badges, ownership and employment data of White House Military Office (WHMO) employees for the White House community. It is also used to manage DoD military, civilian and contractor personnel.

This alteration reflects considerable changes that in sum warrant an alteration to the systems of records notice. The following Department of Defense (DoD) blanket routine uses have been applied to this system: Law Enforcement, Disclosure of Information to the National Archives and Records Administration, and Data Breach Remediation Purposes. This alteration also reflects administrative changes to the system name, safeguards, notification procedure, and record access procedures sections of the systems of records notice.

DATES: Comments were accepted on or before 12/28/2017. This proposed action will be effective on the date following the end of the comment period unless comments are received which result in a contrary determination.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

- Federal Rulemaking Portal: http://www.regulations.gov Follow the instructions for submitting comments.
- Mail: Department of Defense, Office of the Deputy Chief Management Officer, Directorate of Oversight and Compliance, 4800 Mark Center Drive, Mailbox #24, Alexandria, VA 22350-1700.

Instructions: All submissions received must include the agency name and docket number for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet

at http://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Kevin A. Gifford, System Manager, White House Communications Agency (WHCA). Telephone: 202-757-6000.

SUPPLEMENTARY INFORMATION: The Office of the Secretary of Defense notices for systems of records subject to the Privacy Act of 1974, as amended, have been published in the Federal Register and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy, Civil Liberties, and Transparency Division website at http://defense.gov/privacy

The proposed systems reports, as required by of the Privacy Act, as amended, were submitted on INSERT DATE, to the House Committee on Oversight and Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to Section 6 to OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," revised December 23, 2016 (December 23, 2016, 81 FR 94424).

The proposed system report, as required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, was submitted on **INSERT DATE**, to the House Committee on Oversight and Government Reform, the Senate Committee on Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4 of Appendix I to OMB Circular No. A-130, "Federal Agency Responsibilities for Maintaining Records About Individuals," revised November 28, 2000 (December 12, 2000 65 FR 77677).

FOR FURTHER INFORMATION CONTACT: The White House Communications Agency Privacy Officer: Christopher G. Baker at 202-757-6612.

SUPPLEMENTARY INFORMATION: The Defense Information Systems Agency's notices for systems of records subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published in the Federal Register and are available from the address in **FOR FURTHER INFORMATION CONTACT** or from the Defense Privacy, Civil Liberties and Transparency Office website at http://dpcld.defense.gov/.

Dated:

Aaron Siegel,
Alternate OSD Federal Register Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: Basic Employee and Security Tracking (BEAST) Delete Previous Entry: DefenseReady (June 16, 2014, 79 FR 34299

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: 2743 Defense Blvd SW, Bldg. 399, Anacostia Annex, Washington DC 20373-5117

SYSTEM MANAGER(S): Kevin A. Gifford, White House Communications Agency (WHCA), Washington Area Communications Command, Information Systems Division, Enterprise Architect Branch, 2743 Defense Blvd SW, Bldg. 399, Anacostia Annex, Washington DC 20373-5117, Telephone: 202-757-5756.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 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.

PURPOSE(S) OF THE SYSTEM: To manage personnel and security records for the purpose of validation, analysis, and appraisal throughout the lifecycle. This system is used to track travel, security, sensitive items such as access/accountable badges, supervisor status and employment data of military personnel, Federal Government employees and DoD contractors who support WHMO.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Current and former Military personnel, Federal Government employees and DoD contractors supporting the White House Military Office (WHMO).

CATEGORIES OF RECORDS IN THE SYSTEM: Full name, office room, building, home address, home of record, civilian education level, gender, race, marital status, previous work experience, date of birth, Social Security Number (SSN), DoD ID Number, communications devices (e.g., blackberries, secure travel phones), vehicles (makes, models and licenses plates) evaluations/job performance, deployment status, sensitive items (e.g., access and accountable badges), awards, decorations and medals.

Other data: Results from Security Background Investigative reviews and final determination letter.

RECORD SOURCE CATEGORIES: Individuals and employees under the purview of the White House Military Office.

RECORD ACCESS/NOTIFICATION PROCEDURES:
Individuals seeking to determine whether information about themselves is contained in this system of records should address written inquiries to White House Communications Agency Security Division (WHCA/J2) Attn. Freedom of Information Act Rep, 2743 Defense Blvd SW, Anacostia Annex, DC 20373-5117.

(a) Signed written requests should include full name, serial/service number as appropriate (if any), date of birth, branch of military service, if applicable, as well as the requester's current address, e-mail address, telephone number, and the name and number of this system of records notice.
(b) In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:
    i. If executed outside the United States: 'I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).'
    ii. If executed within the United States, its territories, possessions, or commonwealths: 'I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).'
    iii. The requester may also visit one of the system managers listed on the WHCA intranet. As proof of identity, the requester must present a current Defense Information Systems Agency (DISA) identification badge or a driver's license."

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Retrieved by Full name, office room, building, home address, home of record, civilian education level, gender, race, marital status, previous work experience, date of birth, Social Security Number (SSN), DoD ID Number, vehicles (makes, models and licenses plates), office, home or mobile phone number and/or sensitive item number (e.g., access and accountable badges).

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: These records are retained and disposed of consistent with the National Archives and Records Administration approved Records Disposition Schedules. Cut off annually after approval or denial, at the end of the calendar year. Destroy/delete 75 years after cutoff (pending approval).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Records are maintained in areas accessible only to system administrators, Human Capital/Resource Managers and Security Personnel who use the records to perform their duties. All records are maintained using aforementioned methods in paragraph #5 of this document.

CONTESTING RECORD PROCEDURES: The WHMO rules for accessing records, for contesting contents and appealing initial agency determinations are published in the WHMO Security Procedures Manual (SPM), 14 Sep 16.

EXEMPTIONS CLAIMED FOR THE SYSTEM: None.

HISTORY: None.

STORAGE: Electronic Storage Media.