Billing Code: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID DoD-2014-OS-0115]

Privacy Act of 1974; System of Records

AGENCY: Department of Defense.

ACTION: Notice to add a new Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, as amended, the Office of the Secretary of Defense proposes to establish a new system of records for Continuous Evaluation (CE).[1] These records will be used to conduct CE, as defined in Executive Order 13467, to: (1) identify DoD-affiliated personnel who have engaged in conduct of security concern; (2) identify and initiate needed follow-on inquiries and/or investigative activity and enable security officials and adjudicators to determine and take appropriate actions; and (3) perform research, development, and analyses related to DoD's CE program. These analyses are conducted to: (a) evaluate and improve DoD and Federal personnel security, insider

[1] E.O. 13467 defines continuous evaluation as "reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information."

threat,[2] and other background vetting and continuous evaluation procedures, programs, and policies; (b) assist in providing training, instruction, and advice on personnel security and insider threats, and assess continuing reliability of subjects; (c) encourage cooperative research within and among DoD Components, the Intelligence Community, and the Executive branch on initiatives having DoD or Federal Government-wide implications in order to ensure that appropriate information is shared efficiently when authorized to do so and to avoid duplication of efforts; (d) address items of special interest to personnel security officials within DoD Components, the Intelligence Community, and the Executive branch (e.g., evaluating responses to excessive indebtedness, auditing information to ensure individuals with mental health issues are being protected appropriately, monitoring numbers and types of security incidents); (e) conduct personnel security pilot test projects related to DoD's CE program for purposes of research and development.

[2] The November 21, 2012 Presidential Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs" identified insider threat programs as including the following: monitoring user activity on U.S. government networks; continued evaluation of personnel security information; and employee awareness training on risks posed by malicious insiders and recognition of malicious behaviors.

DATES: Comments will be accepted on or before [**INSERT 30 DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. This proposed action will be effective 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: Federal Docket Management System Office, 4800 Mark Center Drive, East Tower, 2nd Floor, Suite 02G09, Alexandria, VA 22350-3100.

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: Ms. Cindy Allard, Chief, OSD/JS Privacy Office, Freedom of Information Directorate, Washington Headquarters Service, 1155 Defense Pentagon, Washington, D.C. 20301-1155, or by phone at (571) 372-0461.

The Office of the Secretary of Defense 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 at the Defense Privacy and Civil Liberties Office website at http://dpclo.defense.gov/.

The proposed system report, as required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, was submitted on June 30, 2014, 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 4c of Appendix I to OMB Circular No. A-130, "Federal Agency Responsibilities for Maintaining Records About Individuals," dated February 8, 1996 (February 20, 1996, 61 FR 6427).

SUPPLEMENTARY INFORMATION:

Further background: The DoD is implementing a program to help ensure that DoD-affiliated personnel who have been approved for eligibility for access to classified information or assignment to national security positions remain reliable, loyal, and trustworthy as well as non-threatening to the safety and well-being of the people they work with. The Department will implement CE based on signed consent of participants in compliance with the Privacy Act. System capabilities will be coordinated and aligned with the Office of the Director of National Intelligence as the Security Executive Agent pursuant

to Executive Order 13467 and other Government agencies to ensure the development of a fully integrated, non-duplicative, and cost-effective CE solution that is implemented in accordance with Departmental and Federal law and policy.

Following the 2013 Washington Navy Yard shooting, the President directed the Office of Management and Budget (OMB) to conduct, within 120 days, a review of suitability and security clearance procedures for Federal employees and contractors. In response, OMB established an interagency review team to assess risks and vulnerabilities inherent in current security, suitability, and credentialing processes and identified solutions to safeguard our personnel and protect our nation's most sensitive information. The resulting report to the President committed the DoD to expanding its current CE pilots in FY14 and expanding overall CE capability beginning in FY15. Concurrent with the OMB review, the Secretary of Defense directed internal and independent reviews to identify and recommend actions that address gaps or deficiencies in DoD programs, policies, and procedures regarding security at DoD installations and the issuance and renewal of security clearances for DoD and contractor personnel. On March 18, 2014, the Secretary of Defense approved the internal review's four resulting recommendations, including: Task 1 - Implement Continuous Evaluation and Task 2 – Establish the DoD Insider Threat

Management and Analysis Center.

To implement CE, the Department is developing an efficient and cost-effective technical solution that supplements existing Federal Investigative Standards and Departmental security processes (such as periodic reinvestigations and self-reporting) to more quickly and reliably identify and prioritize new information that gives cause to question whether individuals who are affiliated with the DoD should retain eligibility for access to classified information or be allowed unescorted access to controlled facilities. A technical CE solution will play a crucial role in improving personnel security and identifying potential insider threats.

The CE capability will use automated records checks of authoritative commercial and Government data sources (e.g., criminal, financial, or credit records) consistent with source records' permissible uses and will flag issues of security concern when behaviors are detected that could potentially disqualify an individual for eligibility for access to classified information or assignment to national security positions. Disqualifiers within the realm of security clearance eligibility are described in the Federal Adjudicative Guidelines. The CE capability will utilize business rules that are aligned with these guidelines and the revised Federal Investigative Standards and will only be applied to personnel

who have consented to CE.

At all points during the development and implementation of the Department's CE solution, any issues related to privacy, civil liberties, and accuracy will be addressed and appropriate safeguards, consistent with national security, will be put into place.

Dated: July 25, 2014.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

DMDC 17 DoD

System name:

Continuous Evaluation Records for Personnel Security.

System location:

Defense Manpower Data Center, DoD Center Monterey Bay, 400 Gigling Road, Seaside, CA 93955-6771.

Categories of individuals covered by the system:

DoD-affiliated individuals who have signed and submitted the March 2010 or later version of the SF-86, "Questionnaire for National Security Positions" (SF-86) and have thereby agreed

to be subject to Continuous Evaluation (CE).[3] This includes: DoD civilian employees, military members (Active Duty, National Guard, and Reserve military service members of the Army, Navy, Marine Corps, and Air Force) or DoD-cleared contractor employees with an active eligibility for access to classified information, or those who otherwise occupy national security positions.

Categories of records in the system:

Applicable records containing the following information about the individual subject to continuous evaluation may be maintained:

a. Evidence of the individual's signed consent to continuous evaluation.

b. Responses from official questionnaires (e.g., SF 86 Questionnaire for National Security Positions) that include: name, former names, and aliases; date and place of birth; social security number; height; weight; hair and eye color; gender; mother's maiden name; current and former home

[3] E.O. 13467 defines continuous evaluation as "reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information."

addresses, phone numbers, and e-mail addresses; employment history; military record information; selective service registration record; residential history; education and degrees earned; names of associates and references with their contact information; citizenship; passport information; criminal history; civil court actions; prior security clearance and investigative information; results of prior continuous evaluation checks; mental health history; records related to drug and/or alcohol use; financial record information; information from the Internal Revenue Service pertaining to income tax returns; credit reports; the name, date and place of birth, social security number, and citizenship information for spouse or cohabitant; the name and marriage information for current and former spouse(s); the citizenship, name, date and place of birth, and address for relatives; information on foreign contacts and activities; association records; information on loyalty to the United States; and other agency reports furnished to DoD in connection with background investigation, continuous evaluation, or insider threat detection processes, and other information developed from above.

c. Reports of security violations and security-related incidents and data collected and actions taken to resolve them.

d. Pre-employment screening reports, such as counter-intelligence screening or military accessions vetting.

e. Dates and types of past investigations; dates and types of access granted based on qualifying investigations; indications of whether prior investigations were adjudicated based on exceptions, deviations, or waivers; denials, revocations, debarments, administrative actions, and other adverse actions based on adjudication of investigations.

f. Records of personnel background investigations conducted by other Federal agency investigation service providers.

g. Agency Use Block (AUB) question responses including type of investigation requested, case number, extra coverage/advance results, sensitivity level, access/eligibility, nature and date of action, geographic location, position code and title, Submitting Office Number (SON), location of official personnel folder, Security Office Identifier (SOI), use of the Intra-governmental Payment and Collection (IPAC) system, Treasury Account Symbol (TAS),

obligating document number, Business Event Type Code (BETC), investigative requirement, requesting officials' name, title, email address, phone number, and applicant affiliation.

h. Educational data on schools and dates of attendance; conduct information that includes disciplinary actions, transcripts, commendations, degrees, certificates, and subject's explanations regarding education conduct.

i. Employment information on current and previous employment that includes: name of employer, dates employed, address, name, and phone number of supervisor. Conduct information that includes promotions, dates and reasons for disciplinary actions to include termination; performance evaluation; and subject's explanations regarding employment conduct; employment references names, current address, phone number and e-mail address; salary and wage information.

j. Selective Service record, military history, and conduct information.

k. Foreign contact and activities information that include names of individuals known, dates, country(ies) of citizenship, country(ies) of residence, type and nature or

contact, financial interests, assets, benefits from foreign governments, countries and dates of arrival and departure for U.S. border crossings.

l. Results of subject and reference interviews conducted during the course of Continuous Evaluation, Counterintelligence Screening, or security incident resolution.

m. Information contained in local, state, and Federal criminal justice agency records and local, state, and Federal civil and criminal court records.

n. Information that pertains to excessive use of alcohol or use of illegal drugs. (This does not include or authorize CE checks of individuals' health or medical records).

o. Information about and evidence of unauthorized use of information technology systems.

p. For purposes of detecting unexplained affluence: U.S. and foreign finance and real estate information that consists of names of financial institutions, number of accounts held, monthly and year-end account balances for bank and investment

accounts, address, year of purchase and price, capital investment costs, lease or rental information, year of lease or rental, monthly payments, deeds, lender/loan information and foreclosure history.

q. For purposes of detecting unexplained affluence: Information on leased vehicles, boats, airplanes and other U.S. and foreign assets that include type, make model/year, plate or identification number, year leased, monthly rental payment; year of purchase and price, and year-end fair market value.

r. For purposes of detecting unexplained affluence: Information pertaining to large currency transactions or other suspicious financial transactions.

s. For purposes of detecting unexplained affluence: U.S. and foreign mortgages, loans, and liabilities information that consist of type of loan, names and addresses of creditors, original balance, monthly and year-end balance, monthly payments, payment history, and name and address of institution where safe deposit box is located.

t. Publically available electronic information about or generated by the subject of continuous evaluation (e.g., public records, civil court records, social media content, news articles, and web blog information). This only includes information that is accessible to any member of the public while browsing the web.

u. Results of automated record checks required to test new or alternative investigative data sources for purposes of improving efficiency or cost-effectiveness of CE.

v. Information about affiliation with known criminal and/or terrorist organizations.

Authority for maintenance of the system:

5 U.S.C. 9101, Access to Criminal History Information for National Security and Other Purposes; 10 U.S.C. 137, Under Secretary of Defense for Intelligence; 10 U.S.C. 504, Persons Not Qualified; 10 U.S.C. 505, Regular components: qualifications, term, grade; E.O. 10450, Security Requirements for Government Employment; E.O. 10865, Safeguarding Classified Information Within Industry; E.O. 12333, United States Intelligence Activities; E.O. 13526, Classified National Security Information; E.O. 12968, as amended, Access

to Classified Information; E.O.13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information; E.O. 13470, Further Amendments to Executive Order 12333; 32 CFR part 154, Department of Defense Personnel Security Program Regulation; 32 CFR part 155, Defense Industrial Personnel Security Clearance; 32 CFR part 156, Department of Defense Personnel Security Program (DoDPSP); DoD Directive 1145.03E, United States Military Entrance Processing Command (USMEPCOM); DoD Instruction (DoDI) 1304.26, Qualification Standards for Enlistment, Appointment and Induction; DoDI 5200.02, DoD Personnel Security Program (PSP); DoDI 5220.06, Defense Industrial Personnel Clearance Review Program; DODI 5220.22, National Industrial Security Program (NISP); DoD 5200.2-R, Department of Defense Personnel Security Program Regulation; HSPD 12: Policy for a Common Identification Standard for Federal Employees and Contractors; FIPS 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors; Director of Central Intelligence Directive 8/1: Intelligence Community Policy on Intelligence Information Sharing; and E.O. 9397 (SSN), as amended.

Purpose(s):

Records in the system will be used to conduct CE to: (1) identify DoD-affiliated personnel with eligibility for access to classified information who have engaged in conduct of security concern; (2) identify and initiate needed follow-on inquiries and/or investigative activity and enable security officials and adjudicators to determine and take appropriate actions; and (3) perform research, development, and analyses related to DoD's CE program. These analyses are conducted to: (a) evaluate and improve DoD and federal personnel security, insider threat, and other background vetting and continuous evaluation procedures, programs, and policies; (b) assist in providing training, instruction, and advice on personnel security and insider threats, and assess continuing reliability of subjects; (c) encourage cooperative research within and among DoD Components, the Intelligence Community, and the Executive branch on initiatives having DoD or Federal Government-wide implications in order to ensure that appropriate information is shared efficiently when authorized to do so and to avoid duplication of efforts; (d) address items of special interest to personnel security officials within DoD Components, the Intelligence Community, and the Executive branch (e.g., evaluating responses to excessive indebtedness, auditing information to ensure individuals with mental health issues are being protected appropriately,

monitoring numbers and types of security incidents); and (e) conduct personnel security pilot test projects related to DoD's CE program for purposes of research and development.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained in the system may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows, where release is not otherwise restricted by law or executive order:

- To Federal, State, local, tribal government agencies, if necessary, to obtain information from them for the purposes of CE, which will assist DoD in identifying security risks and areas in the personnel security field that may warrant more training, instruction, research, or intense scrutiny.

- To Federal Bureau of Investigation and U.S. Office of Personnel Management counterintelligence personnel to assist them with their investigations and inquiries.

- To the Office of Personnel Management, the Office of the Director of National Intelligence, and other Federal Government agencies responsible for conducting background investigations and continuing evaluation in order to provide them with information relevant to their inquiries and investigations.

- To law enforcement agencies, if a system of records maintained by a DoD Component to carry out its functions contains information indicative of a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether Federal, state, local, tribal, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

- To the Director of National Intelligence, as Security Executive Agent, or his assignee, to perform any

functions authorized by law or executive order in support of personnel security programs. Examples include the Intelligence Reform and Terrorism Prevention Act and E.O. 13467.

- To the Office of Personnel Management, to perform any functions authorized by law or executive order in support of personnel security programs. Examples include the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458) and E.O. 10450.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices apply to this system. The complete list of DoD blanket routine uses can be found Online at:

http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx .

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Electronic storage media and paper records maintained in file folders.

Retrievability:

Records may be retrieved by name and Social Security Number (SSN), and/or, where applicable, DoD identification number.

Safeguards:

Records are stored under lock and key, in secure containers, or on electronic media that contain intrusion safeguards. Access to these investigative, incident report and response, and adjudicative records is role-based and is limited to those individuals requiring access in the performance of their official duties. All individuals who are granted access must have a need-to-know, been investigated and granted security clearance eligibility level at a level equal to or higher than subjects of records to which they have access, and been advised as to the sensitivity of the records and their responsibilities to safeguard the information contained in them from unauthorized disclosure. All individuals granted access to this system of records will receive Information Assurance and Privacy Act training.

Audit logs will be maintained to document access to data. All data transfers and information retrievals using remote communication facilities are encrypted. Records are maintained in a secure database in a controlled area accessible only to authorized personnel. Entry to these areas is restricted by the use of locks, guards, and administrative procedures.

Retention and disposal:

Disposition pending (until the National Achieves Records Administration (NARA) disposition schedule is approved, treat as permanent).

System manager(s) and address:

Deputy Director for Identity, Defense Manpower Data Center, 4800 Mark Center Drive, Alexandria, VA 22350-6000 and Deputy Director, Defense Manpower Data Center, 400 Gigling Road, Seaside, CA 93955-6771.

Notification procedure:

Individuals seeking to determine whether this system contains information about them should address written inquiries to the Privacy Office, Defense Manpower Data Center, DoD Center Monterey Bay, 400 Gigling Road, Seaside, CA 93955-6771.

Written requests must contain the following information:

a. Full name, former name, and any other names used.

b. Date and place of birth.

c. Social Security Number.

d. The address to which the record information should be sent.

e. Telephone number.

f. You must sign your request.

Record access procedures:

Individuals wishing to request access to their records should address written inquiries to the Privacy Office, Defense Manpower Data Center, DoD Center Monterey Bay, 400 Gigling Road, Seaside, CA 93955-6771.

Written requests must contain the following information:

a. Full name, former name, and any other names used.

b. Date and place of birth.

c. Social Security Number.

d. The address to which the record information should be sent.

e. You must sign your request.

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:

If executed outside of 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).'

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).'

Attorneys or other persons acting on behalf of an individual must provide written authorization from that individual for the representative to act on their behalf.

The written authorization must also include an original notarized statement or an unsworn declaration in accordance with 28 U.S.C. 1746, in the following format: I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).

Contesting record procedures:

The OSD rules for accessing records, for contesting contents and appealing initial agency determinations are published in OSD Administrative Instruction 81; 32 CFR part 311; or may be obtained from the system manager.

Record source categories:

Information in this system may be provided by the individual based on responses on their signed SF-86 and investigative interviews; Department of Defense civilian, contractor, and military personnel, criminal, and security record systems; Military Component recruiting information systems; Federal Government systems of records (as authorized by their routine use clauses in system of records notices) that provide security-relevant information; publicly available electronic information sources; commercial data providers (e.g., credit reporting companies and online news sources); local, state, and tribal civil and criminal record systems; systems for monitoring misuse of government-owned information technology systems; past and present employers; personal references; education institutions.

Exemptions claimed for the system:

Exempt records received from other systems of records in the course of Continuous Evaluation record checks may, in turn, become part of the case records in this system. When records are exempt from disclosure in systems of records for record sources accessed by this system, the Defense Manpower Data Center hereby claims the same exemptions for any copies of such records received by and stored in this system.

[FR Doc. 2014-17944 Filed 07/29/2014 at 8:45 am; Publication Date: 07/30/2014]