

PURPOSE(S):

The information in the system is being collected to enable the CFPB to carry out its responsibilities under the FOIA and the PA, including enabling staff to receive, track, and respond to requests. This requires maintaining documentation gathered during the consideration and disposition process, administering annual reporting requirements, managing FOIA-related fees and calculations, and delivering responsive records.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

These records may be disclosed, consistent with the CFPB's Disclosure of Records and Information Rules, promulgated at 12 CFR 1070 *et seq.*, to:

(1) Appropriate agencies, entities, and persons when: (a) The CFPB suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the CFPB 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 CFPB or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the CFPB's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

(2) Another federal or state agency to (a) permit a decision as to access, amendment or correction of records to be made in consultation with or by that agency, or (b) verify the identity of an individual or the accuracy of information submitted by an individual who has requested access to or amendment or correction of records;

(3) The Office of the President in response to an inquiry from that office made at the request of the subject of a record or a third party on that person's behalf;

(4) Congressional offices in response to an inquiry made at the request of the individual to whom the record pertains;

(5) Contractors, agents, or other authorized individuals performing work on a contract, service, cooperative agreement, job, or other activity on behalf of the CFPB or Federal Government and who have a need to access the information in the performance of their duties or activities;

(6) The DOJ for its use in providing legal advice to the CFPB or in representing the CFPB in a proceeding before a court, adjudicative body, or other administrative body, where the use of such information by the DOJ is deemed by the CFPB to be relevant and necessary to the advice or proceeding, and such proceeding names as a party in interest:

(a) The CFPB;

(b) Any employee of the CFPB in his or her official capacity;

(c) Any employee of the CFPB in his or her individual capacity where DOJ has agreed to represent the employee; or

(d) The United States, where the CFPB determines that litigation is likely to affect the CFPB or any of its components;

(7) A court, magistrate, or administrative tribunal in the course of an administrative proceeding or judicial proceeding, including disclosures to opposing counsel or witnesses (including expert witnesses) in the course of discovery or other pre-hearing exchanges of information, litigation, or settlement negotiations, where relevant or potentially relevant to a proceeding, or in connection with criminal law proceedings;

(8) Appropriate agencies, entities, and persons, including but not limited to potential expert witnesses or witnesses in the course of investigations, to the extent necessary to secure information relevant to the investigation; and

(9) Appropriate federal, state, local, foreign, tribal, or self-regulatory organizations or agencies responsible for investigating, prosecuting, enforcing, implementing, issuing, or carrying out a statute, rule, regulation, order, policy, or license if the information may be relevant to a potential violation of civil or criminal law, rule, regulation, order, policy or license.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM: STORAGE:

Paper and electronic records.

RETRIEVABILITY:

Records are retrievable by a variety of fields including, but not limited to, the requester's name, the subject matter of request, requestor's organization, FOIA tracking number, and staff member assigned to process the request. Records may also be searched by the address, phone number, fax number, email address of the requesting party, and subject matter of the request, or by some combination thereof.

SAFEGUARDS:

Access to electronic records is restricted to authorized personnel who have been issued non-transferrable access codes and passwords. Other records are maintained in locked file cabinets or rooms with access limited to those personnel whose official duties require access.

RETENTION AND DISPOSAL:

Computer and paper records will be maintained in accordance with published National Archives and Records Administration Disposition Schedule, Transmittal No. 22, General Records Schedule 14, Information Service Records.

SYSTEM MANAGER(S) AND ADDRESS:

Consumer Financial Protection Bureau, Chief FOIA Officer, 1700 G Street NW., Washington, DC 20552.

NOTIFICATION PROCEDURE:

Individuals seeking notification and access to any record contained in this system of records, or seeking to contest its content, may inquire in writing in accordance with instructions appearing in the CFPB's Disclosure of Records and Information Rules, promulgated at 12 CFR 1070 *et seq.* Address such requests to: Chief Privacy Officer, Bureau of Consumer Financial Protection, 1700 G Street NW., Washington, DC 20552.

RECORD ACCESS PROCEDURES:

See "Notification Procedures" above.

CONTESTING RECORD PROCEDURES:

See "Notification Procedures" above.

RECORD SOURCE CATEGORIES:

Information in this system covers individuals about whom records are maintained; agency staff assigned to help process, consider, and respond to the request, including any appeals; entities filing requests or appeals on behalf of the requestor; other governmental authorities; and entities that are the subjects of the request or appeals.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. 2013-18848 Filed 8-2-13; 8:45 am]

BILLING CODE 4810-AM-P

DEPARTMENT OF DEFENSE**Office of the Secretary**

[Docket ID DoD-2012-OS-0060]

Submission for OMB Review; Comment Request

ACTION: Notice.

The Department of Defense has submitted to OMB for clearance, the following proposal for collection of information under the provisions of the Paperwork Reduction Act (44 U.S.C. Chapter 35).

DATES: Consideration will be given to all comments received by September 4, 2013.

Title; Associated Form; and OMB Number: How Differences in Pedagogical Methods Impact ChalleNge Program Outcomes; OMB Control Number: 0704–TBD.

Type of Request: New.

Number of Respondents: 150.

Responses per Respondent: 1.

Annual Responses: 150.

Average Burden per Response: 20 minutes.

Annual Burden Hours: 50 hours.

Needs and Uses: The information collection requirement is necessary to obtain data on the pedagogical methods of National Guard Youth ChalleNge program teachers. The data will be used by DoD to evaluate how differences in classroom teaching methods impact program outcomes. The data will also be used to identify those policies and techniques that are most effective so they may be shared program-wide.

Affected Public: Individuals or households.

Frequency: One time.

Respondent's Obligation: Voluntary.

OMB Desk Officer: Ms. Jasmeet Seehra.

Written comments and recommendations on the proposed information collection should be sent to Jasmeet Seehra at the Office of Management and Budget, Desk Officer for DoD, Room 10236, New Executive Office Building, Washington, DC 20503.

• *Federal eRulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name, docket number and title 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.

DOD Clearance Officer: Ms. Patricia Toppings.

Written requests for copies of the information collection proposal should be sent to Ms. Toppings, WHS/ESD, 4800 Mark Center Drive, 2nd floor, East Tower, Suite 02G09, Alexandria, VA 22350–3100.

Dated: July 30, 2013.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2013–18732 Filed 8–2–13; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD–2013–OS–0063]

Privacy Act of 1974; System of Records

AGENCY: Defense Intelligence Agency, DoD.

ACTION: Notice to alter a System of Records.

SUMMARY: The Defense Intelligence Agency is proposing to alter a system of records in its existing inventory of records systems subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended.

DATES: This proposed action will be effective on September 5, 2013 unless comments are received which result in a contrary determination. Comments will be accepted on or before September 4, 2013.

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. Theresa Lowery at Defense Intelligence Agency, DAN 1–C, 600 MacDill Blvd., Washington, DC 20340–0001 or by phone at (202) 231–1193.

SUPPLEMENTARY INFORMATION: The Defense Intelligence Agency system of records notices 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 **FOR FURTHER INFORMATION CONTACT**.

The proposed system report, as required by 5 U.S.C. 552a of the Privacy

Act of 1974, as amended, was submitted on March 21, 2013, 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).

Dated: July 31, 2013.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

LDIA 0011

SYSTEM NAME:

Student Information Files (May 11, 2010, 75 FR 26201)

CHANGES

* * * * *

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Delete entry and replace with “Current and former civilian and military members as students of the National Intelligence University.”

* * * * *

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Delete entry and replace with “DoD Instruction 3305.01, National Intelligence University, 10 U.S.C. 2161, Joint Military Intelligence College: Academic degrees; American Association of Collegiate Registrars and Admissions Officer, and E.O. 9397 (SSN), as amended.”

PURPOSE(S):

Delete entry and replace with “This information is collected to provide data for managing the student population at the National Intelligence University and for historical documentation.”

* * * * *

SAFEGUARDS:

Delete entry and replace with “Records are stored in office buildings protected by guards, controlled screenings, use of visitor registers, electronic access, and/or locks. Access to records is limited to individuals who are properly screened and cleared on a need-to-know basis in the performance of their duties. Passwords and User IDs are used to control access to the system data, and procedures are in place to deter and detect browsing and unauthorized access. Physical and electronic access are limited to persons responsible for servicing and authorized to use the system.”

* * * * *