information collection on respondents, including through the use of automated collection techniques or other forms of information technology.

DATES: Consideration will be given to all comments received by February 19, 2013.

ADDRESSES: You may submit comments, identified by docket number DOD–2012–OS–0168 and title: DoD CIO IASP Information Collection, by any of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Mail:* Federal Docket Management System Office, 4800 Mark Center Drive, East Tower, Suite 02G09, Alexandria, VA 22350–3100.

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.

FOR FURTHER INFORMATION CONTACT: To request more information on this proposed information collection or to obtain a copy of the proposal and associated collection instruments, please write to Office of the Chief Information Officer, 4800 Mark Center Drive, East Tower, Suite 11E08, Alexandria, VA 22350–1900.

Title and OMB Number: Information Assurance Scholarship Program; OMB Control Number 0704–0486.

Needs and Uses: The National Security Agency (NSA) is the Executive Administrator of the DoD Information Assurance Scholarship Program (IASP), serving on behalf of DoD Chief Information Officer. Those who wish to participate in the DoD IASP Recruitment program must complete and submit an application package through their college or university to NSA. Centers of Academic Excellence in Information Assurance and Research (CAEs) interested in applying for capacity-building grants must complete and submit a written proposal, and all colleges and universities subsequently receiving grants must provide documentation on how the grant funding was utilized and the resulting accomplishments. Without this written documentation, the DoD has no means of judging the quality of applicants to the program or collecting information regarding program performance. In addition, the DoD IASP participants and their faculty advisors (Principal Investigators) are asked to complete annual program assessment surveys. These surveys are collectively reviewed to assess the program's effectiveness from the perspective of the students and Principal Investigators. The survey information is used to improve the program in subsequent years.

Affected Public: ''Individuals or households,'' specifically college students at institutions designated as CAEs who are interested in, and qualify to apply for a scholarship; CAEs interested in submitting proposals for capacity-building grants, and faculty advisors (Principal Investigators).

Application Process

Annual Burden Hours: 1,926 hours.
Number of Respondents: 337.
Responses per Respondent: 1.
Average Burden per Response: 5.715 hours.

Assessments

Annual Burden Hours: 37 hours.
Number of Respondents: 147.
Responses per Respondent: 1.
Average Burden per Response: 15 minutes.
Frequency: Annually.

SUPPLEMENTARY INFORMATION:

Summary of Information Collection

Respondents to the scholarship information collection are applicants who provide academic records and professional experience summaries to the NSA for the IASP scholar selection process. Respondents to the grants information collection are Principal Investigators at designated Centers of Academic Excellence (CAE) participating in the IASP who provide proposals for capacity building initiatives supporting the expansion of Information Assurance programs at the CAE and across the nation. The DoD IASP is designed to: Increase the number of new college graduate entrants to DoD who possess key cyber-security skill sets; serve as a tool to develop and retain well-educated military and civilian personnel who support the Department's cyberspace mission including cutting edge research and development; and serve as a mechanism to build the nation's cyber infrastructure through grants to colleges and universities designated as CAEs by the National Security Agency and the Department of Homeland Security. In addition, respondents to the annual program assessment survey provide feedback on the program, including suggestions for improvements and changes that can be incorporated to make the grants IASP information collection process stronger and more efficient.

Dated: December 18, 2012.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2012–30743 Filed 12–20–12; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DOD–2012–HA–0165]

Proposed Collection; Comment Request

AGENCY: Office of the Assistant Secretary of Defense for Health Affairs, DoD.

ACTION: Notice.

In compliance with Section 3506(c)(2)(A) of the *Paperwork Reduction Act of 1995,* the Office of the Assistant Secretary of Defense for Health Affairs announces the extension of an existing public information collection and seeks public comment on the provisions thereof. Comments are invited on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden of the proposed information collection; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the information collection on respondents, including through the use of automated collection techniques or other forms of information technology.

DATES: Consideration will be given to all comments received by February 19, 2013.

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

- *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Mail:* Federal Docket Management System Office, 4800 Mark Center Drive, East Tower, Suite 02G09, Alexandria, VA 22350–3100.

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.

FOR FURTHER INFORMATION CONTACT: To request more information on this proposed information collection or to obtain a copy of the proposal and associated collection instruments, please write to the Office of the Assistant Secretary of Defense for Health Affairs (OASD), TRICARE Operations Division, ATTN: Lt Col Kathleen Gates, 7700 Arlington Blvd., Suite 5101, Falls Church, VA 22042, or call TRICARE Operations Division, at 703–681–0039.

Title; Associated Form; and OMB Number: Department of Defense Active Duty/Reserve Forces Dental Examination; DD Form 2813; OMB Number 0720–0222.

Needs and Uses: The information collection requirement is necessary to obtain and record the dental health status of members of the Armed Forces. This form is the means for civilian dentists to record the results of their findings and provide the information to the member's military organization. The military organizations are required by Department of Defense policy to track the dental status of its members.

Affected Public: Business or other for profit; Not-for-profit institutions.

Annual Burden Hours: 35,560.

Number of Respondents: 711,204.

Responses per Respondent: 1.

Average Burden per Response: 3 minutes.

Frequency: Annually.

SUPPLEMENTARY INFORMATION:

Summary of Information Collection

Respondents are medical professionals who provide dental services. Members of the Armed Forces of the United States are the recipients of the dental examination. The Armed Forces Reserve component members must maintain their dental health at a predetermined level so problems do not occur when they are deployed to a military operation. Reserve component members usually receive their dental care from civilian dentists; therefore it would be civilian dentists who would complete the form. Following a routine dental examination, the dentist would review the categories listed on the form and circle the number corresponding to the condition that best describes the dental health of the patient. If dental problems can be identified, they are indicated on the form. Once the form is complete and the dentist signs it, the members take the form back to the organization to which they belong. The information on the form is logged into a database. The form is kept in the health record until no longer needed and then it is destroyed.

Dated: December 18, 2012.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2012–30742 Filed 12–20–12; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD–2012–OS–0162]

Privacy Act of 1974; System of Records

AGENCY: Defense Contract Audit Agency, DoD.

ACTION: Notice to amend a System of Records.

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

DATES: This proposed action will be effective on January 22, 2013 unless comments are received which result in a contrary determination. Comments will be accepted on or before January 22, 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: Mr. Keith Mastromichalis, DCAA FOIA/Privacy Act Management Analyst, 8725 John J. Kingman Road, Suite 2135, Fort Belvoir, VA 22060–6219, Telephone number: (703) 767–1022.

SUPPLEMENTARY INFORMATION: The Defense Contract Audit Agency systems 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 in **FOR FURTHER INFORMATION CONTACT**.

The proposed changes to the record system being amended are set forth below. The proposed amendment is not within the purview of subsection (r) of the Privacy Act of 1974 (5 U.S.C. 552a), as amended, which requires the submission of a new or altered system report.

Dated: December 18, 2012.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

RDCAA 215.1

SYSTEM NAME:

Voluntary Leave Transfer Program (January 31, 1997, 62 FR 4731).

CHANGES:

* * * * *

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Delete and replace with ''DCAA government employees who have volunteered to participate in the leave transfer program as either a donor or a recipient.''

* * * * *

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Delete and replace with ''5 U.S.C. 6331 et seq., Leave; 10 U.S.C. 136, Assistant Secretaries of Defense; 5 CFR part 630, Absence and Leave; DoD Directive 5105.36, Defense Contract Audit Agency; E.O. 9397 (SSN), as amended.''

* * * * *

SAFEGUARDS:

Delete and replace with ''Electronic records are maintained in password-protected network and accessible only to DCAA personnel, management, and administrative support personnel on a need-to-know basis to perform their duties. Access to the network where records are maintained requires a valid Common Access Card (CAC). Paper records are secured in locked cabinets, offices, or buildings during non-duty hours. The same security standards currently applied to individually-issued CAC card are applicable to paper compilations.''

* * * * *

CONTESTING RECORD PROCEDURES:

Delete and replace with ''DCAA's rules for accessing records, for contesting contents and appealing initial agency determinations are published in DCAA Instruction 5410.10;