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). Proposal information listed in the September 9, 2011 Federal Register notice (76 FR 55883–55886) will supplement the application and assist OEA in determining compliance with legal and programmatic requirements. Grant awards will be made to successful applicants until the available funds are exhausted.

Affected Public: State, local, or tribal government.
Frequency: On occasion.
Respondent’s Obligation: Required to obtain or retain benefits.
OMB Desk Officer: Ms. Jasmeet Seehra.
Written comments and recommendations on the proposed information collection should be sent to Ms. Seehra at the Office of Management and Budget, Desk Officer for DoD, Room 10236, New Executive Office Building, Washington, DC 20503.
You may also submit comments, identified by docket number and title, by the following method:
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: Ms. Theresa Lowery, 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 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.

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

LDIA 05–0003

SYSTEM NAME:
Joint Intelligence Virtual University (JIVU II), (April 12, 2012, 77 FR 21974)
SYSTEM NAME: Delete entry and replace with “Advanced Global Intelligence Learning Environment (AGILE).”

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Delete entry and replace with “Federal employees, contractors and active duty service members who access AGILE in order to facilitate a training requirement.”


SUPPLEMENTARY INFORMATION: 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. The proposed system report, as required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, was submitted on May 14, 2012, 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).


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

DCIO 01


DoD Cyber Crime Center, 911 Elkridge Landing Road, Suite 200, Linthicum, MD 21090–2991.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Supporting DoD contractor (hereafter referred to as “DIB company”) personnel (points of contact and individuals submitting incident reports) providing DIB company information.

CATEGORIES OF RECORDS IN THE SYSTEM: DIB company point of contact information includes name, company name and mailing address, work division/group, work email, and work telephone number. DIB incident summary information includes name, company name, work division/group, group email, work telephone and fax numbers.


PURPOSE(S): To facilitate the sharing of DIB CS/IA cyber threat information and best practices to DIB companies to enhance and supplement DIB participant capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems. When incident reports are received, DoD Cyber Crime Center (DC3) personnel analyze the information reported for cyber threats and vulnerabilities in order to develop response measures as well as improve U.S. Government and DIB understanding of advanced cyber threat activity. DoD may work with a DIB company on a more detailed, digital forensics analysis or damage assessment, which may include sharing of additional electronic media/files or information regarding the incident or the affected systems, networks, or information.

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, these records contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: DIB company point of contact information may be provided to other participating DIB companies to facilitate the sharing of information and expertise related to the DIB CS/IA program, cyber threat information and best practices, and mitigation strategies.

Only the DoD “Blanket Routine Uses” 1 and 14 set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices apply to this system.

DoD Blanket Routine Use 01 (Law Enforcement).