Billing Code: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DOD-2012-OS-0057]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary of Defense, DoD.

ACTION: Notice to add a new system of records.

SUMMARY: The Office of the Secretary of Defense proposes to add a new system of records in its 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 **[INSERT DATE 30 DAYS FROM DATE PUBLISHED IN THE FEDERAL REGISTER]** 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: Cindy Allard, Chief, OSD/JS Privacy Office, Freedom of Information Directorate, Washington Headquarters Services, 1155 Defense Pentagon, Washington, D.C. 20301-1155, or by phone at (571) 372-0461.

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).

Dated: May 14, 2012.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

DCIO 01

System name:

Defense Industrial Base (DIB) Cyber Security/Information Assurance Records.

System location:

Director, Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Program, 1235 South Clark Street, Suite 1500, Arlington, VA 22202.

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, work email, work telephone and fax numbers.

Authority for maintenance of the system:
10 U.S.C. 2224, Defense Information Assurance Program; 44 U.S.C. 3544, Federal Agency Responsibilities; HSPD 7, Critical Infrastructure, Identification, Prioritization, and Protection; DoD Directive (DoDD) 3020.40, DoD Policy and Responsibilities for Critical Infrastructure; DoDD 5505.13E, DoD Executive Agent for the DoD Cyber Crime Center (DC3); DoD Instruction (DoDI) 3020.45, Defense Critical Infrastructure Program (DCIP) Management; and DoDI 5205.13, Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities.

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).

DoD Blanket Routine Use 14 (Counterintelligence).

Any release of information contained in this system of records outside the DoD will be compatible with the purpose(s) for which the information is collected and maintained.

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

Storage:
Electronic storage media.

Retrievability:
DIB Company POC information is retrieved primarily by company name and work division/group and secondarily by individual POC name.

DIB incident reports are primarily retrieved by incident number but may also be retrieved by company name. They are not retrieved by the individual name.

Safeguards:

Records are accessed by DIB CS/IA program office and DC3 personnel with security clearances who are properly screened, trained, under a signed confidentiality agreement, and determined to have "need to know." Access to records requires DoD Common Access Card (CAC) and PIN. Physical access controls include security guards, identification badges, key cards, cipher locks, and combination locks.

Retention and disposal:
Disposition pending (treat records as permanent until the National Archives and Records Administration has approved the retention and disposition schedule).

System manager(s) and address:
Director, DIB Cyber Security/Information Assurance Office, 1235 South Clark Street, Suite 1500, Arlington, VA 22202.

Notification procedure:
Individuals seeking to determine whether this system of records contains information on themselves should address written inquiries to Director, DIB Cyber Security/Information Assurance Office, 1235 South Clark Street, Suite 1500, Arlington, VA 22202.

The individual should provide their name, company name and work division/group, and correspondence must be signed.

Record access procedures:
Individuals seeking access to information about themselves contained in this system of records should address a written request to the Office of the Secretary of Defense/Joint Staff Freedom of Information Act Requester Service Center, 1155 Defense Pentagon, Washington DC 20301-1155.

The request should include the individual's name, company name and work division/group, the name and number of this system of records notice and correspondence must be signed.

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:
From the individual, participating DIB companies, and the Joint Personnel Adjudication System (JPAS).

Exemptions claimed for the system:

None.

[FR Doc. 2012-12028 Filed 05/17/2012 at 8:45 am; Publication Date: 05/18/2012]