DEPARTMENT OF DEFENSE
Office of the Secretary of Defense
Narrative Statement on a New System of Records
Under the Privacy Act of 1974

1. System identifier and name: DCIO 01, entitled "Defense Industrial Base (DIB) Cybersecurity Records."

2. Responsible official: Ms. Vicki Michetti, Deputy Director, Defense Industrial Base Cybersecurity and Information Assurance (DIB CS/IA), 1550 Crystal Drive, Suite 1000A, Arlington, VA 22202, telephone (703) 604-3167.

3. Purpose of establishing the system: The Office of the Secretary of Defense proposes to establish a new system of records to facilitate the mandatory incident reporting and the expansion of sharing of DIB CS cyber threat information and cybersecurity best practices to enhance and supplement DIB companies' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems. When incident reports are received, DC3 personnel analyze the information reported for cyber threats and vulnerabilities in order to develop response measures, as well as improve USG 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.

4. Authority for the maintenance of the system: 10 U.S.C. 2224, Defense Information Assurance Program; 44 U.S.C. 3544, Federal Agency Responsibilities; PPD-21, Critical Infrastructure Security and Resilience; 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.

5. Provide the agency's evaluation of the probable or potential effects on the privacy of individuals: In constructing this SORN, the Director of the DIB Cybersecurity Program Office carefully reviewed the safeguards established for the system to ensure they are compliant with the DoD's requirements and are appropriate to the sensitivity of the information stored within this system. The specific routine use has been reviewed to ensure the minimum amount of personally identifiable information is provided, and the most likely to be used DoD blanket routine uses have been identified in the SORN.

6. Is the system, in whole or in part, being maintained by a contractor? Yes.

7. Steps taken to minimize risk of unauthorized access: Records are accessed by DIB CS 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.

8. Routine use compatibility: 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 program, cyber threat information and best practices, and mitigation strategies.

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. 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. Of those blanket routine uses, we anticipate the following two would most likely be used:

DoD Blanket Routine Use 01 (Law Enforcement Routine Use). If a system of records maintained by a DoD Component to carry out its functions indicates 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, 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.

DoD Blanket Routine Use 14 (Counterintelligence Purpose Routine Use). A record from a system of records maintained by a DoD Component may be disclosed as a routine use outside the DoD or the U.S. Government for the purpose of counterintelligence activities authorized by U.S. Law or Executive Order or for the purpose of enforcing laws which protect the national security of the United States.

9. OMB information collection requirements:
OMB collection required: Yes
OMB Control Number:
Title of collection if other than #10:
Date Approved or Submitted:
Expiration Date:

10. Name of IT system (state NONE if paper records only):
Defense Industrial Base (DIB) Cybersecurity Activities.
DCIO 01

System name:
Defense Industrial Base (DIB) Cybersecurity Records.

System location:
Deputy Director, Defense Industrial Base (DIB) Cybersecurity (CS) Program, 1550 Crystal Drive, Suite 1000A, Arlington, VA 22202, telephone (703) 604-3167.

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; PPD-21, Critical Infrastructure Security and Resilience; 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) Cybersecurity/Information Assurance (CS/IA) Activities.

Purpose(s):
To facilitate the sharing of Defense Industrial Base (DIB) Cybersecurity (CS) 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, DC3 personnel analyze the information reported for cyber threats and vulnerabilities for the development of effective response measures and improved 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 program, cyber threat information and best practices, and mitigation strategies.

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. 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. Of the blanket routine uses, we anticipate the following two would most likely be used:

DoD Blanket Routine Use 01 (Law Enforcement Routine Use). If a system of records maintained by a DoD Component to carry out its functions indicates 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, 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.

DoD Blanket Routine Use 14 (Counterintelligence Purpose Routine Use). A record from a system of records maintained by a DoD Component may be disclosed as a routine use outside the DoD or the U.S. Government for the purpose of counterintelligence activities authorized by U.S. Law or Executive Order or for the purpose of enforcing laws which protect the national security of the United States.

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.

Safeguards:
Records are accessed by DIB CS 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 Cybersecurity Office,
1550 Crystal Drive, Suite 1000A, 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 Cybersecurity Office, 1550 Crystal Drive, Suite 1000A, 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.