SYSTEM NAME AND NUMBER: Defense Industrial Base (DIB) Cybersecurity (CS) Activities Records, DCIO 01. (May 17, 2019; 84 FR 22477)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Defense Industrial Base (DIB) Cybersecurity Program, 6000 Defense Pentagon, ATTN: DIB CS Program, Washington, DC 20301–6000.

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

SYSTEM MANAGER(S): Director, DIB Cybersecurity, 6000 Defense Pentagon, ATTN: DIB CS Program, Washington, DC 20301–6000, 703–604–3167, OSD.DIBCSIA@ MAIL.MIL.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 391, Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors; 10 U.S.C. 393, Reporting on penetrations of networks and information systems of certain contractors; 10 U.S.C. 2224, Defense Information Assurance Program; 50 U.S.C. 3330, Reports to the intelligence community on penetrations of networks and information systems of certain contractors; 32 CFR 236, Department of Defense (DoD)'s Defense Industrial Base (DIB) Cybersecurity (CS) Activities; and DoDI 5205.13, Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities.

PURPOSE(S) OF THE SYSTEM: To facilitate communications and the sharing of cyber threat information among DIB CS Program participants.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Supporting DoD contractor (hereafter referred to as 'DIB company') personnel (points of contact and individuals submitting cyber 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; cyber incident reports submitted by DIB companies are identified by incident numbers, and include information detailing the cyber incident.

RECORD SOURCE CATEGORIES: The individual and participating DIB companies.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: In addition to the disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To other participating DIB companies to facilitate the sharing of information and expertise related to the DIB CS Program including cyber threat information and best practices, and mitigation strategies.

b. To contractors working with the DIB CS Program and contractors supporting government activities related to the implementation of 32 CFR part 236 and safeguarding covered defense

information and cyber incident reporting in accordance with U.S. Department of Defense Federal Acquisition Regulation Supplement (DFARS) 252.204–7009, Limitations on the use or disclosure of third-party contractor reported cyber incident information.

c. To appropriate Federal, State, local, territorial, tribal, foreign, or international agencies for the purpose of counterintelligence activities authorized by U.S. law or Executive Order, or for the purpose of executing or enforcing laws designed to protect the national security or homeland security of the United States, including those relating to the sharing of records or information concerning terrorism, homeland security, or law enforcement.

d. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

e. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

f. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

g. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

h. To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

i. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Electronic storage media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: DIB company point of contact (POC) information is retrieved primarily by company name and work division/ group and secondarily by individual POC name. DIB cyber incident reports are primarily retrieved by incident number but may also be retrieved by company name. They are not retrieved by the individual name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: The master file consisting of DIB participant information is destroyed three years after the participating company withdraws from the program, closes, or goes out of business. Other records closed annually and are destroyed 10 years after cut off.

ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS: Records are accessed by 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.

RECORD ACCESS PROCEDURES: Individuals seeking access to information about themselves contained in this system of records should address inquiries to the Office of the Secretary of Defense/Joint Staff (OSD/JS), Freedom of Information Act (FOIA) Requester Service Center, 1155 Defense Pentagon, Washington, DC 20301–1155. Signed, written requests should contain the individual's name, company name and work division/group, and the name and number of this system of records notice. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: ''I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).''

If executed within the United States, its territories, possessions, or commonwealths: ''I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).''

CONTESTING RECORD PROCEDURES: The Office of the Secretary of Defense (OSD) rules for accessing records, for contesting contents, and for appealing initial agency determinations are contained in OSD Administrative Instruction 81; 32 CFR part 311; or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether this system of records contains information on themselves should address inquiries to Director, DIB Cybersecurity Office, 6000 Defense Pentagon, ATTN: DIB CS Program, Washington, DC 20301–6000. Signed, written requests should contain the individual's name, and company name and work division/group. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: ''I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).''

If executed within the United States, its territories, possessions, or commonwealths: ''I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).''

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: May 21, 2015, 80 FR 29315; May 8, 2012, 77 FR 29616.