

**Authorities:** Public Law 113-291, Sec. 391., Reporting on Cyber Incidents with Respect to Networks and Information Systems of Operationally Critical Contractors and Certain Other Contractors; Public Law 114-92, Sec. 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 Code of Federal Regulations (CFR) part 236, "Department of Defense (DoD)'s Defense Industrial Base (DIB) Cybersecurity (CS) Activities;" and DoDI 5205.13 CE-02, "Defense Industrial Base (DIB) Cyber Security CS) Activities."

**Purpose:** Administrative management of the DIB CS Program's information sharing activities. Personal information is covered by OSD SORN DCIO 01, Defense Industrial Base (DIB) Cyber Security/Information Assurance Records, available at: <http://www.gpo.gov/fdsys/pkg/FR-2015-05-21/pdf/2015-12324.pdf>

**Routine Use(s):** 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:

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 including cyber threat information and best practices, and mitigation strategies.

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.

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.

Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense/Joint Staff compilation of systems of records notices may apply to this system. The complete list of the DoD blanket routine uses can be found online at:

<https://dpclld.defense.gov/Privacy/SORNs/>

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.

**Disclosure:** Voluntary. However, failure to provide requested information may limit the ability of the DoD to contact the individual or provide other information necessary to facilitate this program.

**Privacy Impact Assessment (PIA):** The PIA addresses the processes in place to protect information provided by DoD contractors reporting cyber incidents. The PIA for the Defense Industrial Base (DIB) Cybersecurity Activities is available at [http://dodcio.defense.gov/Portals/0/Documents/PIA\\_DIB%20CS%20program\\_Aug%202015\\_corrected.pdf?ver=2016-09-22-113831](http://dodcio.defense.gov/Portals/0/Documents/PIA_DIB%20CS%20program_Aug%202015_corrected.pdf?ver=2016-09-22-113831)

**Freedom of Information Act (FOIA).** Agency records, which may include qualifying information received from non-federal entities, are subject to request under the Freedom of Information Act (5 U.S.C. 552) (FOIA), which is implemented in the Department of Defense by DoD Directive 5400.07 and DoD Regulation 5400.7-R (see 32 C.F.R. Parts 285 and 286, respectively). Pursuant to established procedures and applicable regulations, the Government will protect sensitive nonpublic information under this Program against unauthorized public disclosure by asserting applicable FOIA exemptions, and will inform the non-Government source or submitter (e.g., DIB participants) of any such information that may be subject to release in response to a FOIA request, to permit the source or submitter to support the withholding of such information or pursue any other available legal remedies.

**Agency Disclosure Notice:**

OMB CONTROL NUMBER: 0704-0490  
OMB EXPIRATION DATE: 11/30/2022

The public reporting burden for this collection of information is estimated to average 20 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. DoD cannot receive written comments at this time due to the COVID-19 pandemic. Comments should be sent electronically to the docket listed below. Please submit electronically at the Federal Rulemaking Portal: <https://www.regulation.gov> and reference 32 CFR part 236, Docket ID: DOD-2019-OS-0112 and/or by Regulatory Information Number (RIN) 0790-AK86.