PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Defense Industrial Base (DIB) Cybersecurity (CS) Activities

2. DOD COMPONENT NAME:

DoD Chief Information Officer

3. PIA APPROVAL DATE:

07 MAR 2024

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- [x] From members of the general public
- [ ] From Federal employees
- [ ] from both members of the general public and Federal employees
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [ ] Existing DoD Information System
- [x] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The purpose of the electronic collection is to identify the industry points of contact participating in the DoD's DIB CS information sharing program and to facilitate the analysis of cyber incident reports.

As part of the administration and management of the DIB CS information sharing activities, each DIB participant provides basic identifying information for a limited number of its personnel who are authorized to serve as the primary company points of contact (POCs). The information provided for each POC includes routine business contact information (e.g., name, title, organizational unit, business email and phone), plus additional information necessary to verify the individual's authorization to receive classified information or controlled unclassified information (e.g., security clearance, citizenship). This information is required by the DIB CS program office to manage the program and interact with the companies through routine emails, phone calls, and participation in periodic meetings.

It is possible that PII, other than POC information, may be submitted to DoD in a cyber incident report. If this information is relevant and necessary to understanding the cyber incident, it will be used in the forensic analysis of the incident. If the PII is not relevant and necessary to the analysis of the cyber incident, the contractor will be notified and the PII will be purged.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

To verify information in a cyber incident report; to administer the DoD's DIB CS information sharing program; and to conduct the necessary analysis of the reported cyber incidents (e.g., for forensic analysis or damage assessment purposes).

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

The participating DIB company selects individuals to participate as the company-designated points of contact for the DIB CS information sharing program and for the submission of cyber incident reports. Reporting companies should ensure that their selected POCs have the opportunity to object/consent to sharing of their contact information with DoD prior to being identified as a POC.

There may be cases where PII is embedded in a cyber incident report. This PII is not requested by DoD and is incidental to the report. If the company deems that PII is relevant and necessary in a cyber incident report, then it is the responsibility of the company to ensure that they are authorized to share that information in the incident report. Unless the individual happens to also be one of the company-designated POCs, DoD does not have direct access to contact the individual to enable that individual to object. In many cases authorized users of a contractor's network are under notice (e.g., policy, banner) that information and data on the network may be monitored or disclosed to third parties, and/or that the network users' communications on the network are not private.

f. Do individuals have the opportunity to consent to the specific uses of their PII? ☒ Yes ☐ No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

The participating DIB company selects individuals to participate as the company-designated points of contact for the DIB CS information sharing program and for the submission of cyber incident reports. Reporting companies should ensure that their selected POCs have the opportunity to object/consent to sharing of their contact information with DoD prior to being identified as a POC.

There may be cases where PII is embedded in a cyber incident report. This PII is not requested by DoD and is incidental to the report. If the company deems that PII is relevant and necessary in a cyber incident report, then it is the responsibility of the company to ensure that they are authorized to share that information in the incident report. Unless the individual happens to also be one of the company-designated POCs, DoD does not have direct access to contact the individual to enable that individual to object. In many cases authorized users of a contractor's network are under notice (e.g., policy, banner) that information and data on the network may be monitored or disclosed to third parties, and/or that the network users' communications on the network are not private.

Additionally, there may be cases where PII included in a cyber incident report is not PII of an employee, but rather is either fictitious (i.e., is not actual PII) or is attributable to the threat actor.

In all cases, as a condition of participating in the program, the DIB company is required to ensure that all of its activities in support of the program are conducted in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

Authorities: 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 Code of Federal Regulations (CFR) part 236, "Department of Defense (DoD)'s Defense Industrial Base (DIB) Cybersecurity (CS) Activities;" and DoDI 5205.13, "Defense Industrial Base (DIB) Cybersecurity (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) Cybersecurity/Information Assurance Records, available at: https://dpcld.defense.gov/Portals/49/Documents/Privacy/SORNs/OSDJS/DCIO-01.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://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx

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: https://dodcio.defense.gov/In-the-News/Privacy-Impact-Assessments/

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: 0704-0489
OMB EXPIRATION DATE: 12/31/2024

OMB CONTROL NUMBER: 0704-0478
OMB EXPIRATION DATE: 10/31/2025
The public reporting burden for this collection of information, 0704-0489, is estimated to average 2 hours 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.

OMB CONTROL NUMBER: 0704-0490
OMB EXPIRATION DATE: 01/31/2025
The public reporting burden for this collection of information, 0704-0490, 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. Send comments regarding the burden estimate or burden reduction suggestions to the Department of Defense, Washington Headquarters Services, at whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	DoD restricts access to PII and attribution information only to those authorized personnel that have a need-to-know such information (DoD cybersecurity, LE/CI), and to DoD support services contractors who are subject to appropriate nondisclosure obligations (i.e. cyber incident reports leading to a damage assessment are provided to OUSD(R&E).
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	DoD restricts access to PII and attribution information only to those authorized personnel that have a need-to-know such information (DoD cybersecurity, LE/CI), and to DoD support services contractors who are subject to appropriate nondisclosure obligations (i.e. cyber incident reports leading to a damage assessment are provided to OUSD(R&E).
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Federal entities with missions that may be affected by a cyber incident, including those that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents, or conduct counterintelligence or law enforcement investigations, or for national security purposes, including cyber situational awareness and defense purposes consistent with the Privacy Act and applicable routine uses.
☐ State and Local Agencies	Specify.	

☒ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*

Specify. DoD restricts access to PII and attribution information only to those authorized DoD support services contractor personnel that have a need-to-know such information to support authorized DoD activities and are subject to strict nondisclosure obligations.

☒ Other *(e.g., commercial providers, colleges)*.

Specify. PII may be shared with DIB participants in the DoD's DIB CS program for cyber situational awareness and defense purposes when the PII is deemed necessary and relevant to understanding the cyber incident and approved for release by the submitting company. Additionally, there may be cases where PII included in a cyber incident report is not PII of an employee, but rather is either fictitious or attributable to the threat actor.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☒ Individuals
☐ Databases
☐ Existing DoD Information Systems
☐ Commercial Systems
☐ Other Federal Information Systems

The company provides point of contact information for designated individuals. Individuals submit cyber incident reports on behalf of their company. Cyber incident details that could include PII come from DIB contractor network or information systems and are reported by the company.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

☒ E-mail
☐ Official Form (*Enter Form Number(s) in the box below)*
☒ In-Person Contact
☒ Paper
☐ Fax
☒ Telephone Interview
☒ Information Sharing - System to System
☒ Website/E-Form
☐ Other *(If Other, enter the information in the box below)*

k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier DCIO 01, "Defense Industrial Base (DIB)"

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. DAA-0330-2015-0005-0001

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Temporary. Cut off when the participating company withdraws from the program, closes or goes out of business. Destroy 3 years after cutoff.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).

(a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

1. 10 U.S.C. 2224, Defense Information Assurance Program
2. 44 U.S.C. 3554, Federal Agency Responsibilities
3. 10 U.S.C. 391, Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors
4. 10 U.S.C. 393, Reporting on penetrations of networks and information systems of certain contractors
5. E.O. 13636, Improving Critical Infrastructure Cybersecurity
6. Presidential Policy Directive PPD-21, Critical Infrastructure, Security and Resilience
7. DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Activities, 32 Code of Federal Regulations (CFR) Part 236
8. DoDD 5505.13E, DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)
9. DoD Instruction 5205.13, Defense Industrial Base (DIB) Cybersecurity (CS) Activities
10. DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting"
11. DFARS 252.204-7018, "Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services."
12. DoD Instruction 8530.03, Cyber Incident Response
13. FAR 52.204-23, "Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities."
14. FAR 52.204-25, "Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment"

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☒ Yes ☐ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

0704-0478, Safeguarding Covered Defense Information, Cyber Incident Reporting and Cloud Computing, 10/31/2025
0704-0490, Defense Industrial Base (DIB) Cyber Security (CS)) Program Point of Contact (POC) Information, 1/31/2025
0704-0489, DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Activities Cyber Incident Reporting, 12/31/2024