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:

Department of Defense - Chief Information Officer

3. PIA APPROVAL DATE:

06/17/20

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

☐ From members of the general public

☒ From Federal employees and/or Federal contractors

☐ From both members of the general public and Federal employees and/or Federal contractors

☐ 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

☐ 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 system 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? ☒ 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.

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.

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

A Privacy Act Statement is included as part of the Incident Collection Form that includes the authorities to collect the information; the purpose or purposes for which the information is to be used; the routine uses that will be made of the information; whether providing the information is voluntary through the information sharing program or mandatory from cyber incident reporting; and the effects on the individual if he or she chooses not to provide the requested information.

In addition, acknowledgement of the Privacy Act Statement is required for access to the DoD web portal where a company applying to the DIB CS program would submit point of contact information.

h. With whom will the PII be shared through data 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	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 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

□ Existing DoD Information Systems

□ Other Federal Information Systems

□ Databases

□ Commercial 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 compan

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

☒ E-mail

☒ Face-to-Face Contact

☒ Fax

☒ Information Sharing - System to System

□ Other *(If Other, enter the information in the box below)*

□ Official Form (*Enter Form Number(s) in the box below)*

☒ Paper

☒ Telephone Interview

☒ Website/E-Form

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. □

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

(3) Retention Instructions.

PII provided for administrative management purposes are held permanently until the National Archives and Records Administration has approved the retention and disposition schedule. Access to all PII is strictly controlled and restricted to DoD to personnel with a need-to-know. DoD support services contractors, with a need-to-know, sign a non-disclosure agreement.

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. DoD Directive (DoDD) 3020.40, DoD Policy and Responsibilities for Critical Infrastructure
9. DoDD 5505.13E, DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)
10. DoD Manual 3020.45, Defense Critical Infrastructure Program (DCIP)
11. DoD Instruction 5205.13, Defense Industrial Base (DIB) Cybersecurity (CS) Activities
12. DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services

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, 09/30/2022
0704-0490, Defense Industrial Base (DIB) Cyber Security (CS)) Program Point of Contact (POC) Information, 11/30/2022
0704-0489, DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Activities Cyber Incident Reporting, 10/31/2022

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)*

□ Biometrics	□ Birth Date	□ Child Information
☒ Citizenship	□ Disability Information	□ DoD ID Number
□ Driver's License	□ Education Information	□ Emergency Contact
☒ Employment Information	□ Financial Information	□ Gender/Gender Identification
□ Home/Cell Phone	□ Law Enforcement Information	□ Legal Status
□ Mailing/Home Address	□ Marital Status	□ Medical Information
□ Military Records	□ Mother's Middle/Maiden Name	☒ Name(s)
□ Official Duty Address	□ Official Duty Telephone Phone	□ Other ID Number
□ Passport Information	□ Personal E-mail Address	□ Photo
□ Place of Birth	□ Position/Title	□ Protected Health Information (PHI)[1]
□ Race/Ethnicity	□ Rank/Grade	□ Religious Preference
□ Records	□ Security Information	□ Social Security Number (SSN) *(Full or in any form)*
□ Work E-mail Address	☒ If Other, enter the information in the box below	

Contact information (business email and business telephone number of the designated POC) is used by DoD to interact with the contractors reporting cyber incidents using the ICF, as well as part of the voluntary cybersecurity information sharing activities.

In some cases, the contractor may determine that PII, or what appears to be PII, is relevant and necessary to a cyber incident event (e.g., an individual's name and email address that may be spoofed in connection with an email phishing attempt or an email used as the delivery mechanism for malware). Electronic media may contain PII depending on the media and files provided (e.g., digital images of a potentially compromised system).

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

□ Yes □ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

□ Yes □ No

b. What is the PII confidentiality impact level[2]? ☒ Low □ Moderate □ High

[1] The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2] Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

☒ Cipher Locks
☒ Combination Locks
☒ Key Cards
☒ Security Guards
☒ Closed Circuit TV (CCTV)
☒ Identification Badges
☒ Safes
□ If Other, enter the information in the box below

(2) Administrative Controls. *(Check all that apply)*

□ Backups Secured Off-site
□ Encryption of Backups
☒ Methods to Ensure Only Authorized Personnel Access to PII
□ Periodic Security Audits
☒ Regular Monitoring of Users' Security Practices
□ If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

□ Biometrics
□ Encryption of Data at Rest
☒ Firewall
□ Role-Based Access Controls
☒ Virtual Private Network (VPN)
☒ Common Access Card (CAC)
☒ Encryption of Data in Transit
☒ Intrusion Detection System (IDS)
□ Used Only for Privileged (Elevated Roles)
□ If Other, enter the information in the box below
☒ DoD Public Key Infrastructure Certificates
☒ External Certificate Authority Certificates
□ Least Privilege Access
☒ User Identification and Password

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

POC information and mandatory cyber incident reporting is provided by defense contractors through an unclassified, secure DoD website that is access controlled.

Media provided by DoD contractors may be transmitted electronically or physically mailed to the DoD Cyber Crime Center (DC3). Upon receipt, procedures are employed to protect PII. Access is limited to personnel with a need-to-know.

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool[3]?

☒	Yes, DITPR	DITPR System Identification Number	15811
□	Yes, SIPRNET	SIPRNET Identification Number	
□	Yes, RMF tool	RMF tool Identification Number	
□	No		

If "No," explain.

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology".

Indicate the assessment and authorization status:

☒	Authorization to Operate (ATO)	Date Granted:	5/14/2014
□	ATO with Conditions	Date Granted:	
□	Denial of Authorization to Operate (DATO)	Date Granted:	
□	Interim Authorization to Test (IATT)	Date Granted:	

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

c. Does this DoD information system have an IT investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

☒ Yes □ No

If "Yes," Enter UII 007-97-05-08-02-3915-00 If unsure, consult the component IT Budget Point of Contact to obtain the UII

[3] Guidance on Risk Management Framework (RMF) tools (i.g., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at https://rmfks.osd.mil.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Mandatory coordinators are: Component CIO, Senior Component Official for Privacy, Component Senior Information Security Officer, and Component Records Officer.

a. Program Manager or Designee Name	Philip Glinatsis	(1) Title	Director, DIB CS Program
(2) Organization	DoD CIO	(3) Work Telephone	(703) 545-2220
(4) DSN		(5) E-mail address	philip.c.glinatsis.civ@mail.mil
(6) Date of Review	7/2/2020	(7) Signature	GLINATSIS.PHILIP.C HARLES.1286401437 Digitally signed by GLINATSIS.PHILIP.CHARLES.128640143 7 Date: 2020.07.02 14:15:23 -04'00'

b. Other Official *(to be used at Component discretion)*	Jeffrey Specht	(1) Title	Director, DoD Cyber Crime Center
(2) Organization	DoD Cyber Crime Center	(3) Work Telephone	
(4) DSN		(5) E-mail address	Jeffrey.Specht@dc3.mil
(6) Date of Review		(7) Signature	SPECHT.JEFFRE Y.D.1086451553 Digitally signed by SPECHT.JEFFREY.D.1086451553 Date: 2020.07.07 10:39:57 -04'00'

c. Other Official *(to be used at Component discretion)*		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	

d. Component Privacy Officer (CPO)	Lyn Kirby	(1) Title	Chief, Defense Privacy and Civil Liberties Division
(2) Organization	OCMO/OSD	(3) Work Telephone	(703) 571-0086
(4) DSN		(5) E-mail address	lyn.m.kirby.civ@mail.mil
(6) Date of Review	07/31/2020	(7) Signature	KIRBY.LYN.M.1 590283483 Digitally signed by KIRBY.LYN.M.1590283483 Date: 2020.07.31 16:33:57 -04'00'

e. Component Records Officer		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	

f. Component Senior Information Security Officer or Designee Name	John W. Wilmer, III	(1) Title	DoD Deputy Chief Information Officer for Cybersecurity
(2) Organization	DoD CIO, OSD	(3) Work Telephone	(703) 695-8705
(4) DSN		(5) E-mail address	john.w.wilmer.civ@mail.mil
(6) Date of Review:		(7) Signature	Digitally signed by WILMER.JOHN.W.III.1267975430 Date: 2020.07.17 12:53:28 -04'00'

g. Senior Component Official for Privacy (SCOP) or Designee Name		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	

h. Component CIO Reviewing Official Name	Mr. John Sherman	(1) Title	Principal Deputy Chief Information Officer
(2) Organization	DoD CIO	(3) Work Telephone	
(4) DSN		(5) E-mail address	john.b.sherman4.civ@mail.mil
(6) Date of Review		(7) Signature	

Publishing: Only Section 1 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: osd.mc-alex.dod-cio.mbx.pia@mail.mill.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Section 1.