PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Industrial Base (DIB) Cybersecurity Activities
DoD CIO

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☐ **Existing DoD Information System**
- ☒ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 15811
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☒ **Yes**
- ☐ **No**

If "Yes," enter UPI 007-97-05-08-02-3915-00

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier DCIO 01, "Defense Industrial Base (DIB) Cybersecurity Records"

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number	0704-0478; ~~0704-0491~~; 0704-0489, 0704-0490
Enter Expiration Date	11/30/2016;11/30/2016; 11/30/2016

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

1. 10 U.S.C. 2224, Defense Information Assurance Program
2. 44 U.S.C. 3554, Federal Agency Responsibilities
3. Public Law 112-239, Section 941, National Defense Authorization Act (NDAA) for FY 2013, Reports to Department of Defense on Penetrations of Networks and Information Systems of Certain Contractors
4. Public Law 113-291, Section 1632, NDAA for FY 2015, Reporting on Cyber Incidents with respect to Networks and Information Systems of Operationally Critical Contractors (10 U.S.C. Chapter 19, Cyber Matters)
5. Presidential Policy Directive PPD-21, Critical Infrastructure, Security and Resilience
6. DoD-Defense Industrial Base (DIB) Cybersecurity (CS) Activities, 32 Code of Federal Regulations (CFR) Part 236
7. DoD Directive (DoDD) 3020.40, DoD Policy and Responsibilities for Critical Infrastructure
8. DoDD 5505.13E, DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)
9. DoD Manual 3020.45, Defense Critical Infrastructure Program (DCIP)
10. DoD Instruction 5205.13, Defense Industrial Base (DIB) Cybersecurity/Information Assurance (CS/IA) Activities

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly 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-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.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Privacy risks: Unauthorized release of PII to individuals who do not have a need-to-know, or who are not bound by appropriate safeguarding and confidentiality requirements (e.g., under a non-disclosure agreement).

DoD restricts access to PII only to authorized personnel who have a need-to-know. All DoD personnel are subject to safeguarding and confidentiality obligations as federal employees or military members, and all DoD support services contractors accessing the information are required to be bound by appropriate non-disclosure agreements prior to accessing the information. DoD handling procedures are designed to ensure that PII and other sensitive information is only shared by DoD after the submitting contractor has determined that the information is relevant and necessary to cyber intrusion incidents or follow-on forensics or cyber intrusion damage assessment analysis, and that the information has been lawfully collected and is authorized for sharing with the DoD. DoD may share with law enforcement/counter intelligence for the purposes of supporting an investigation and prosecution of any individual or organization when the information appears to indicate activities that may violate laws, including those attempting to infiltrate and compromise information on a Company information system. Such dissemination must comply with the Privacy Act and all other applicable statutes, regulations, and DoD policies.

Records Management and Retention of Information: DoD complies with all federal records management requirements (e.g., 36 CFR §1220-1239) and all applicable DoD regulations and policies. Information deemed unnecessary for incident analysis is purged from DoD systems.

DoD will maintain, control, and dispose of all media provided in accordance with established DoD policies and procedures for the handling and safeguarding of PII and other sensitive information.

Compliance and Oversight Mechanisms: The DoD-DIB Cybersecurity activities are subject to review by the Defense Privacy and Civil Liberties Division (DPCLD). DPCLD works with existing DoD inspection agencies to ensure that adequate privacy and civil liberties oversight mechanisms are observed. DoD information systems used to process and store PII (or any sensitive information) have undergone a mandatory certification and accreditation process to verify that the system provides adequate measures to preserve the authenticity, integrity, availability, and confidentiality of all sensitive information residing or transiting those

systems (see DoDI 8510.01).

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate 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.

☒ **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.

☒ **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.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

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-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. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can 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/IA 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.

(2) If "No," state the reason why individuals cannot object.

j. 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.

The participating DIB company selects individuals to participate as the company-designated points of contact for the DIB CS/IA 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.

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

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

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/IA program would submit point of contact information.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.