PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Industrial Base (DIB) Cyber Security/Information Assurance 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	
☐	**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 In process

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. April 28, 2011

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	In process
Enter Expiration Date	

☐ **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.

Department of Defense (DoD) Instruction (DoDI) 5205.13, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities," January 29, 2010, directs the conduct of DIB CS/IA activities to protect unclassified DoD information that transits, or resides on, unclassified DIB information systems and networks. DoD Directive (DoDD) 5505.13E, "DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)," March 1, 2010, addresses the responsibilities of DC3, including its electronic and multimedia forensics laboratory, which is accredited by the American Society of Crime Laboratory Directors Laboratory Accreditation Board; collaboration with U.S. Government (USG) and private industry organizations; and designates DC3 as the information sharing focal point for the DIB CS/IA program. These activities, including the collection, management and sharing of information for cyber security purposes, support and implement national and DoD-specific guidance and authority, including the following:

1. Information Assurance (IA):

DoD is required by statute to establish programs and activities to protect DoD information and DoD information systems, including information and information systems operated and maintained by contractors or others in support of DoD activities. Section 2224 of title 10, U.S. Code (U.S.C.), requires DoD to establish a Defense IA Program to protect and defend DoD information, information systems, and information networks that are critical to the Department during day-to-day operations and operations in times of crisis. (10 U.S.C. § 2224(a)). The program must provide continuously for the availability,

integrity, authentication, confidentiality, non-repudiation, and rapid restitution of information and information systems that are essential elements of the Defense information infrastructure. (10 U.S.C. § 2224(b)). The program strategy also must include vulnerability and threat assessments for defense and supporting non-defense information infrastructures, joint activities with elements of the national information infrastructure, and coordination with representatives of those national critical infrastructure systems that are essential to DoD operations. (10 U.S.C. § 2224(c)). The program must provide for coordination, as appropriate, with the heads of any relevant federal agency and with representatives of those national critical information infrastructure systems that are essential to the operations of the Department regarding information assurance measures necessary to the protection of these systems. (10 U.S.C. § 2224(d)).

The Defense IA Program also must ensure compliance with federal IA requirements provided in the Federal Information Security Management Act (FISMA). (44 U.S.C. §§ 3541 et seq.). FISMA requires all federal agencies to provide information security protections for information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. (44 U.S.C. § 3544(a)(1)(A)). Agencies are expressly required to develop, document, and implement programs to provide information security for information and information systems that support the operations and assets of the agency, including those provided by another agency, contractor, or other source. (44 U.S.C. § 3544(b)).

2. Critical Infrastructure Protection (CIP):

Under Homeland Security Presidential Directive 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection," the Department of Homeland Security (DHS) leads the national effort to protect public and private critical infrastructure. (HSPD-7, ¶(7)). This includes coordinating implementation activities between federal agencies, state and local authorities, and the private sector. Regarding cyber security, these efforts are to include analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. (HSPD-7, ¶(12)).

The Department of Defense is the Sector Specific Agency (SSA) for the Defense Industrial Base (DIB) sector (HSPD-7, ¶(18)(g)), and thus engages with the DIB on a wide range of CIP matters, including but not limited to cyber security. HSPD-7 charges the SSAs to: collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector; conduct or facilitate vulnerability assessments of the sector; and encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources. (HSPD-7, ¶(19)). More specifically, regarding coordination with the private sector, HSPD-7 provides that DHS and the SSAs "will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms [to] identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices." (HSPD-7, ¶(25)). Within DoD, CIP is implemented by DoDD 3020.40, "DoD Policy and Responsibilities for Critical Infrastructure," January 14, 2010, and DoDI 3020.45, "Defense Critical Infrastructure Program (DCIP) Management" April 21, 2008.

3. Comprehensive National Cybersecurity Initiative:

National Security Presidential Directive (NSPD) 54/Homeland Security Presidential Directive (HSPD) 23, which formalizes the Comprehensive National Cyber Security Initiative (CNCI), directs each Department to improve situational awareness between the Government and private sector regarding the extent and severity of the cyber threat. Under CNCI, the Department of Homeland Security (DHS), in consultation with the heads of other SSAs, including DoD, submitted the "Project 12 Report: Improving Protection of Privately Owned Critical Network Infrastructure Through Public-Private Partnerships." This report recommends implementing real-time cyber situational awareness and promoting public-private cyber information sharing efforts.

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 information systems and information collection activities covered by this PIA are used to support key elements of the Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Program (see DoD Instruction (DoDI) 5205.13, "[DIBCS/IA] Activities," January 29, 2010), to protect unclassified DoD information that transits, or resides, on unclassified DIB information systems and networks. This includes support provided by the DIB CS/IA Program Office, the DoD Cyber Crime Center (DC3), the Damage Assessment Management Office (DAMO), and other government stakeholders.

More specifically, this PIA covers a voluntary cyber security information sharing activity between the DoD and DIB companies. In general, DoD provides cyber threat information and information assurance (IA) best practices to DIB companies to help them better protect their unclassified networks to protect DoD unclassified information; and in return, DIB companies report certain types of cyber intrusion incidents to the DoD-DIB Collaborative Information Sharing Environment (DCISE), located at DC3. The DoD analyzes the information reported by the DIB company regarding any such cyber incident, to glean information regarding cyber threats, vulnerabilities, and the development of effective response measures. In addition to this initial reporting and analysis, the DoD and DIB company may pursue, on a voluntary basis, follow-on, more detailed, digital forensics analysis or damage assessments, including sharing of additional electronic media/ files or information regarding the incident or the affected systems, networks, or information. The information sharing arrangements between the DoD and each participating DIB company are memorialized in a standardized bilateral Framework Agreement (FA).

Such DoD-DIB cyber security information sharing practices are under continuous review and improvement, including the development and testing of additional information sharing mechanisms and models. For example, the new DIB Exploratory Cybersecurity Initiative (also known as the "DIB Cyber Pilot"), builds on the existing DIB CS/IA Program and FAs, serving as a short-term proof-of-concept demonstration in which DoD would share cyber threat information and technical information directly with commercial providers of internet, network, and communications services providers. In this sharing model, the commercial service providers (CSPs) enter into a modified version of the FA that authorizes them to use the DoD-provided information to further protect participating DIB company networks. This modified information sharing model allows the DIB companies the option of acquiring such additional cyber security protections from commercial providers, rather than each DIB company independently deploying the information directly on its own networks. This Pilot utilizes all of the incident reporting, forensics analysis, and damage assessment procedures already established under the DIB CS/IA program and FAs, and thus the sharing of PII for the Exploratory Pilot is also covered by this PIA.

Although these DIB CS/IA Program information sharing activities are focused on sharing cyber security related information, the operational implementation of this sharing arrangement involves sharing and managing PII in two supporting ways: (i) for program administration and management purposes, the DIB companies share with DoD the typical business contact information for its personnel that are serving as company points of contact for the program activities or specific cyber incidents; and (ii) although it is not typical or expected, there is always the potential that information provided by a DIB company regarding any specific cyber incident may include PII that is incidental to or embedded within the cyber security information being shared. Each of these circumstances is discussed in more detail below:

1. DIB CS/IA Program Administration and Management:

As part of the administrative management of the DIB CS/IA Program's information sharing activities, each participating DIB company 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/IA program office to manage the program and interact with the companies through routine emails, phone calls, and participation in periodic classified meetings. A DIB company that is not yet participating in the Program may also provide POC information to the DIB CS/IA Program office in order to discuss Program application procedures or related information regarding the Program.

In addition to the designation of a limited number of primary POCs for the DIB company's overall participation in the DIB CS/IA Program, additional POC information may be provided in the individual incident reports submitted by the company. In most cases, the DIB companies report incidents using a DIB CS/IA Program standardized Incident Collection Form (ICF), which is submitted as the initial incident report to the DoD-DIB Collaborative Information Sharing Environment (DCISE) at DC3. The ICF includes the basic POC information (e.g., name, organizational unit, business email and phone) for the DIB company representative who is submitting the initial report. The ICF also allows the reporting company to provide the same basic POC information for other company personnel that are knowledgeable about, or otherwise relevant for, the reported incident (e.g., POCs for incident response, technical issues, or the affected business unit). In some cases, a company may elect to report the incident without using the ICF; and companies may report incidents through a variety of communications channels, including email, fax, or by phone, if necessary.

Collecting this type of POC information is the only element of this information sharing activity in which the DIB CS/IA program intentionally collects PII; however, there are other portions of the information sharing activities that present the potential for the DIB companies to provide DoD with PII that is incidental to, or embedded within, other cyber security information being shared—resulting in an inadvertent collection of PII.

2. Cyber Incident Response and Analysis:

Although it is not typical or expected, it is nevertheless possible that a DIB company may voluntarily submit PII to DoD in connection with the initial cyber incident reporting or response activities, or during follow-up digital forensics or damage assessment activities. Accordingly, the Program is designed to provide appropriate handling and safeguards in the event that PII is (inadvertently) collected in these circumstances.

For example, when providing the initial incident report on the ICF, the DIB company provides a description of the cyber incident, including technical and contextual details regarding any or all relevant aspects of the incident. In some cases, the DIB company may determine that PII, or what appears to be PII, is relevant in describing the 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). The ICF allows the company to describe the incident in two levels of detail and sensitivity: (i) a fully detailed version that may contain attribution or other sensitive information (e.g., PII) that that the company is providing for internal DCISE use; and (ii) an alternative description that provides only such information that the company is authorizing to be released outside the DCISE for cyber security purposes (e.g., as part of an automated "alert" process that immediately forwards only this company pre-approved information to all participating DIB companies). Subsequently, the DCISE also follows up with the DIB company to confirm the nature and extent of information that the DIB company authorizes for release outside the DCISE for cyber security purposes (except in cases when the company has indicated that it does not desire this additional pre-release review).

In addition, the DoD and DIB companies have recognized that, in some cases, after the initial incident report and preliminary investigation, a more complete analysis of the event may be necessary. Accordingly, on a voluntary basis, DIB companies may share additional information about potentially compromised information systems with the DoD for this purpose. This information may include PII or other sensitive information that the DIB company determines is relevant for the analysis, but the DIB companies may elect to limit the nature and extent of any sensitive information to be shared, due to legal, contractual, or other restrictions (e.g., the DIB company determines that it is not authorized to share certain PII or third-party proprietary information with the DoD, even if it would be relevant to the cyber event analysis).

Similarly, as part of the follow-up for each reported incident, the DIB company reviews the potentially compromised systems or networks and reports to DoD regarding the presence of files or information associated with DoD programs, systems, or military applications. When the reported cyber intrusion affects systems containing such DoD information, the DIB companies will preserve and share with DoD the unclassified files on threat-accessed systems that pertain to Government programs, unless there are legal or contractual reasons that preclude sharing (e.g., the images may contain PII or third-party proprietary information that are subject to nondisclosure prohibitions). The DoD's Damage Assessment Management Office (DAMO), an organizational element of the Under Secretary of Defense for Acquisition, Technology and Logistics, reviews the available information to determine whether a more complete damage assessment is warranted.

The short-term DIB Cyber Pilot also utilizes the incident reporting procedures already established for the DIB

CS/IA Program, although it is anticipated that the DIB companies will typically be reporting less detailed information regarding incidents detected by the DIB companies' commercial service providers (CSPs), given the limited proof-of-concept nature of the Pilot and the fact that it was the CSP, rather than the DIB company, that detected the event. DIB companies participating in the voluntary 90-day proof-of-concept pilot notify DC3 of an incident when they determine an incident occurred based on an alert from their commercial service provider. Consistent with the reporting procedures for the existing DIB CS/IA Program, the DIB companies participating in the Pilot will include PII in their incident reporting and follow-up analysis only if the DIB company determines that the PII is relevant and material to the understanding of the technical attributes of the incident, and that there are no legal, contractual, or other restrictions on sharing that PII with the USG. There is no incident reporting from the CSP to the USG under the Pilot, although that CSPs may voluntarily provide the USG with end-of-pilot lessons learned or other general feedback regarding the Pilot activities (e. g., technical or operational issues and solutions arising during the exercise)--none of which will include PII.

These information sharing mechanisms are intended to enhance a participating DIB company's ability to detect and defend against cyber intrusions and other malicious activity occurring on their networks, in order to better protect Defense information. In doing so, the DIB CS/IA Program has developed uniform procedures and safeguards (e.g., set forth in the standardized FAs) designed to ensure that the DIB companies share information with DoD only if it is relevant to the forensics or damage assessment analysis, and only after the DIB company verifies that it is authorized to share the information with the DoD for these purposes.

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

There are minimal risks associated with the PII collected in connection with the DoD-DIB cyber security information sharing activities under the DIB CS/IA Program. The Program's information sharing activities implement administrative, technical, and electronic protections to ensure compliance with all applicable DoD policies and procedures regarding the collection and handling of PII and other sensitive information, including but not limited to the following:

- DoDD 5400.11, "DoD Privacy Program", May 8, 2007
- DoD 5400.11-R, "Department of Defense Privacy Program", May 14, 2007
- DoDI 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," February 12, 2009
- DoD CIO memorandum, "Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)", August 18, 2006
- DA&M memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information", June 05, 2009
- DoDI 8500.02, "Information Assurance Implementation," February 6, 2003
- DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007
- DoDI 5200.1, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008 (Revised June 13, 2011)
- DoD 5200.1-R, "Information Security Program," January 14, 1997
- DoDI 5015.2, "DoD Records Management Program," March 6, 2000

(These references are publicly available, e.g., at http://www.dtic.mil/whs/directives/ or http://dpclo.defense.gov/privacy/About_The_Office/policy_guidance.html.)

The Program is also structured around several key elements that are designed to ensure that risks are effectively addressed to safeguard privacy:

- All PII received by the DoD is provided voluntarily by authorized DIB company representatives, subject to mutually agreed upon restrictions (e.g., in the FA);
- The nature of the PII being intentionally collected is limited to ordinary business contact information for DIB company personnel;
- PII is inadvertently collected only if submitted by a DIB company that has determined that the PII is relevant to cyber incident response and analysis activities, and that the PII is authorized to be shared with the DoD for these purposes;
- Once collected, access and use of PII is limited to authorized personnel that need the information for cyber security or other lawful purposes;
- All DIB CS/IA Program and supporting personnel receiving access to the collected PII are required to

undergo training and are subject to appropriate nondisclosure restrictions; and
• The PII is maintained for only so long as necessary for DIB CS/IA Program activities, and is managed and disposed of in accordance with applicable records management requirements.

Additional details regarding these risk mitigations and safeguards are discussed below.

* Collection of Information:

The DIB CS/IA information sharing activities covered by this PIA are focused on sharing cyber security related information, and thus the Program seeks to minimize the collection and management of PII except as necessary to support the program. The operational implementation of this sharing arrangement involves sharing and managing PII in two supporting or incidental ways: (i) for program administration and management purposes, the DIB companies share with DoD the typical business contact information for its personnel that are serving as company points of contact for the program activities or specific cyber incidents; and (ii) for cyber incident response and analysis purposes, although it is not typical or expected, there exists the potential that information provided by a DIB company regarding any specific cyber incident may include PII that is incidental to, or embedded in, the information being shared for the cyber security analysis.

As discussed previously, the DIB CS/IA Program intentionally collects PII regarding DIB company POCs only for routine program administration and management purposes. This PII does not involve any particularly sensitive personal information – it is limited to the individual's typical contact information that is routinely shared in the ordinary course of business (e.g., name, title, organizational division, business email and phone), including other information (e.g., security clearance, citizenship) that is necessary to verify the individual's authorization to receive classified or other controlled unclassified information under the program. Any other PII collected under the Program is inadvertently collected, in that it is provided to DoD by a participating DIB company based on that company's determination that the PII is relevant to the incident response and analysis, and that there are no legal, contractual, or other restrictions on sharing that PII with the USG for these purposes.

Additional details on the nature and circumstances of PII collection for these purposes are discussed in more detail in Section 2.g.(1) above.

* Use and Management of Collected Information:

The DIB company POC information may not be a particularly sensitive type of PII, it is nevertheless tightly controlled within the DIB CS/IA Program – in the same manner and for the similar purposes, that the Program controls DIB company "attribution information" (i.e., information that identifies a company or its programs, whether directly or indirectly, by the grouping of information that can be traced back to that company). Although the name of a DIB company or its programs, or the basic contact information for the company's POCs, might not ordinarily be considered particularly sensitive, the association of that company or its specific POCs with particular cyber security activities, or with particular cyber security incidents, may be treated as sensitive. Accordingly, the DIB CS/IA Program restricts access to such PII and attribution information only to those authorized personnel who have a need-to-know such information for duties in support of the DIB CS/IA Program, and are subject to strict nondisclosure obligations. For example, all USG personnel and contractors directly supporting the DIB CS/IA Program (including the Program Office, DC3, and DAMO personnel or contractors) who require access to PII or attribution information must sign standardized nondisclosure agreements requiring training and providing strict guidelines on the handling and protecting of that information.

Regarding information provided for incident response and analysis, DC3 will maintain, control, and dispose of all media provided by DIB companies in accordance with established DoD policies and procedures for the handling and safeguarding of PII and other sensitive information, and DC3 also implements specialized handling procedures to maintain its accreditation as a digital and multimedia forensics laboratory. DC3 personnel determine that PII is necessary for subsequent analysis in furtherance of its DIB CS/IA activities before such data is further processed or retained. Information deemed unnecessary for subsequent analysis is purged immediately. In accordance with NARA regulation and 36 CFR §1220-1239, program records are retained for a minimum of three (3) years, and tracking/ticketing system records are retained for a minimum of two (2) years. The media are protected using procedural controls that are the same as, or similar to, those DC3 uses to handle evidence that it processes as part of criminal investigations. Access to electronic media/ files that may have PII or other sensitive information, is strictly controlled and limited to those participating in

formal DIB cyber intrusion analyses or damage assessments. The electronic media/files are maintained by the digital and multimedia forensics laboratory–the files and media do not leave DC3, physically or electronically.

The Program's information sharing procedures are designed to ensure that PII and other sensitive information is shared and processed by DoD only after the submitting DIB Company has determined that the information is relevant 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. When sharing electronic images or files with the DoD for forensics or damage assessment activities, the DIB companies will identify the types of sensitive information (e.g., PII, proprietary, export controlled) that may be contained in the shared files. In addition, when the DoD is performing its analysis on the files, it may discover PII (or other sensitive information) that had not been identified by the DIB company when the information was submitted. If this occurs, all investigative work involving that PII ceases, the DIB company is notified that the PII (or sensitive information) was discovered, and the DIB company provides guidance as to the disposition of that information.

* Dissemination of Information:

For cyber security purposes, DC3, based on analysis of specific cyber threats, releases threat information containing indicators developed from numerous data sources (e.g., government, DIB companies, open source). DC3 will disseminate cyber threat information that may contain PII only after the information has been reviewed and approved for release, including coordination with the source of the PII. For example, release of cyber threat indicators derived from information provided by government sources are coordinated with key government stakeholders, such as USCYBERCOM and NSA. Similarly, indicators derived from information contained in DIB company incident reporting will be disseminated only after coordination with the reporting company (regardless of whether the indicator contains PII).
When cyber threat information is shared with DIB companies under the Program, the DIB company is required to ensure that unclassified threat information is shared with authorized company personnel that have a need-to-know the information for the company's internal cyber security activities. Typically, the unclassified portion of threat information products may be shared with Company network security personnel. The DIB companies are prohibited from sharing the threat information products outside of the company's U. S. based information systems without specific written Government authorization.

The Director, DC3 (DDC3), or designee, must approve any dissemination of information by DC3 for law enforcement/counter intelligence purposes to support 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 other applicable statutes, regulations, and DoD policies, including those references listed above (section 2.g.(2)).

* Records Management and Retention of Information:

The DIB company POC information provided to support the DIB CS/IA administration and management process is maintained only so long as the designated POC(s) continue to represent the participating company for the Program. When the DIB CS/IA program office is notified that a DIB company POC is being replaced, the POC information databases are updated and outdated PII is archived in accordance with records management requirements.

Inadvertently collected PII that may be submitted by DIB companies in connection with incident reporting and response is reviewed by DC3 personnel to determine whether that PII is necessary for subsequent analysis in furtherance of its DIB CS/IA activities before such data is further processed or retained. Information deemed unnecessary for subsequent analysis is purged from DC3 systems. Information determined to be relevant is maintained, controlled, and disposed of when no longer reasonably necessary for intrusion investigation, forensics analysis, and damage assessment activities (or other legal, audit, or operational purposes). The time it takes to complete a cyber intrusion forensics analysis and damage assessment will vary. Some of the assessments will be more complex and require more time than others.

In all cases, the management and disposal of this information will comply with all applicable DoD records management procedures and requirements, and records disposition schedules. In accordance with NARA regulation and 36 CFR §1220-1239, program records are retained for a minimum of three (3) years, and

tracking/ticketing system records are retained for a minimum of two (2) years.

* Compliance and Oversight Mechanisms:

The DIB CS/IA baseline program and opt-in pilot have been subject to review by and consultation with the Defense Privacy and Civil Liberties Office (DPCLO). DC3 and DPCLO will work with existing DoD inspection agencies to ensure that adequate privacy and civil liberties oversight mechanisms exist. All 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 8010.01). In addition, DC3 undergoes extensive inspection by the American Society of Crime Lab Directors to ensure that DC3 information handling procedures are reliable, valid, and repeatable in accordance with standards necessary for accreditation as a digital forensics laboratory.

* Additional Considerations: Will the networks that store or process the PII be monitored? How would participating entities know that their networks are subject to monitoring?

None of these DIB CS/IA activities involve any DoD or USG personnel performing any monitoring of DIB company or other private networks. The DIB companies are responsible for the conduct of any monitoring of their own networks, and for ensuring that there are no legal, contractual, or other restrictions on sharing of PII or any other sensitive information with the DoD. The only PII received by DoD under these activities is PII that is provided directly to DoD by authorized DIB company personnel.

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. The DIB CS/IA Program restricts access to PII and attribution information only to those authorized personnel that have a need-to-know such information for duties in support of the DIB CS/IA Program (or other authorized DoD cybersecurity, LE/CI, or other lawful purposes), and that are subject to appropriate nondisclosure obligations. PII inadvertently collected on an ICF or electronic media is maintained at DC3 with strict accountability and need-to-know on those DoD and support contractor personnel having access to the files. All USG personnel and contractors supporting the DIB CS/IA Program (including the Program Office, DC3 and DAMO personnel or contractors supporting the Program) who require access to PII or attribution information must sign standardized nondisclosure agreements requiring training and providing strict guidelines on the handling and protecting of that information.

☒ **Other DoD Components.**

Specify. The DIB CS/IA Program restricts access to PII and attribution information only to other authorized DoD Component personnel that are authorized to receive the information under the FA, based one a need-to-know such information for duties in support of the DIB CS/IA Program (or other authorized DoD cybersecurity, LE/CI, or other lawful purposes), and that are subject to appropriate nondisclosure obligations. PII inadvertently collected on an ICF or electronic media ismaintained at DC3 with strict accountability and need-to-know on those DoD and support contractor personnel having access to the files. All other DoD Component personnel and contractors directly supporting the DIB CS/IA Program (including the Program Office, DC3 and DAMO personnel or contractors supporting the Program) who require access to PII or attribution information must sign standardized nondisclosure agreements

requiring training and providing strict guidelines on the handling and protecting of that information.

☒ **Other Federal Agencies.**

Specify. PII is shared with other federal agency authorized personnel only for cybersecurity purposes (as authorized by the DIB companies under the FA, and following the incident response and follow-on analysis coordination procedures previously discussed), and in support of authorized LE/CI activities (or other lawful purposes). Only such PII as authorized by the company will be released outside of the DoD.

☐ **State and Local Agencies.**

Specify.

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

Specify. The DIB CS/IA Program restricts access to PII and attribution information only to those authorized support contractor personnel that have a need-to-know such information for duties in support of the DIB CS/IA Program (or other authorized DoD cybersecurity, LE/CI, or other lawful purposes), and that are subject to strict nondisclosure obligations. PII inadvertently collected on an ICF or electronic media is maintained at DC3 with strict accountability and need-to-know on those USG and DoD support contractor personnel having access to the files. All USG personnel and contractors supporting the DIB CS/IA Program (including the Program Office, DC3 and DAMO personnel or contractors supporting the Program) who require access to PII or attribution information must sign standardized nondisclosure agreements requiring training and providing strict guidelines on the handling and protecting of that information. PII that is derived from DIB company submitted information and is included in DC3 threat products will be shared with other DIB companies participating in the DIB CS/IA Program, as authorized under the FA, and following the incident response and follow-on analysis coordination procedures previously discussed.

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

Specify. In any other case, DoD would not share the PII except after obtaining the appropriate permission (e.g., from the DIB company or the individual identified by the PII).

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.

When the DIB company POC information is intentionally collected directly from an individual who is being designated as a POC, he/she can object to the collection of PII at that time.

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

DIB company POC information may also be intentionally collected from a DIB company representative that is

providing contact info for other DIB company POCs, and thus these other POCs do not have the opportunity to object at this point of collection. Providing such routine business POC information to facilitate the DIB CS/IA Program administration and management is agreed upon as part of the DoD-DIB Framework Agreement, and is a routine use of such information for the Program. Participating DIB companies voluntarily provide all such information.

All other PII under this Program is inadvertently collected. DIB companies also voluntarily report network intrusions and compromises of DoD program information. PII is not requested in the reports, however, the DIB company may include relevant PII in the incident reporting and response process.

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.

When the DIB company POC information is intentionally collected directly from an individual who is being designated as a POC, he/she is provided the opportunity to consent or not consent to specific uses of PII when they are presented with a Privacy Act Statement.

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

DIB company POC information may also be intentionally collected from a DIB company representative that is providing contact info for other DIB company POCs, and thus these other POCs do not have the opportunity to consent or withhold consent for specific uses at the point of collection. Providing such routine business POC information to facilitate the DIB CS/IA Program administration and management is agreed upon as part of the DoD-DIB Framework Agreement, and is a routine use of such information for the Program. Participating DIB companies voluntarily provide all such information.

All other PII under this Program is inadvertently collected. DIB companies also voluntarily report network intrusions and compromises of DoD program information. PII is not requested in the reports, however, the DIB company may include relevant PII in the incident reporting and response process.

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.

Privacy Act Statement to include 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 or mandatory and the effects on the individual if he or she chooses not to provide the requested information.