de: 6001-FR

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2024-OS-0089]

Proposed Collection; Comment Request

AGENCY: Office of the DoD Chief Information Officer, Department of Defense (DoD).

ACTION: 60-day information collection notice.

SUMMARY: In compliance with the *Paperwork Reduction Act of 1995*, the Office of the DoD Chief Information Officer (CIO) announces a proposed public information collection and seeks public comment on the provisions thereof. Comments are invited on: whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; the accuracy of the agency's estimate of the burden of the proposed information collection; ways to enhance the quality, utility, and clarity of the information to be collected; and ways to minimize the burden of the information collection on respondents, including through the use of automated collection techniques or other forms of information technology.

DATES: Consideration will be given to all comments received by [INSERT 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

Mail: Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350-1700.

Instructions: All submissions received must include the agency name, docket number and title for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at http://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: To request more information on this proposed information collection or to obtain a copy of the proposal and associated collection instruments, please write to Director of Defense Industrial Base (DIB) Cybersecurity (CS) Program and Director of DOD CIO Cybersecurity Policy and Partnerships, ATTN: Kevin Dulany, Washington, DC 20301, or call: 703-604-3167.

SUPPLEMENTARY INFORMATION:

TITLE; ASSOCIATED FORM; AND OMB NUMBER: DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Program Point of Contact Information; OMB Control Number 0704-0490.

NEEDS AND USES: DoD's DIB CS Program enhances and supports DIB CS participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems. The operational implementation of this Program requires DoD to collect, share, and manage point of contact (POC) information for Program administration and management purposes. The Government will collect typical business POC information from all DIB CS participants to facilitate communication and share cyber threat information. To implement and execute this Program within their companies, DIB CS participants provide POC information to DoD during the application process to join the Program. This information includes company name and identifiers such as cage code and mailing address, employee names and titles, corporate email addresses, and corporate telephone numbers of company-identified POCs. DIB CS Program POCs include the Chief Executive Officer (CEO), CIO, Chief Information Security Officer (CISO), and Corporate or Facility Security Officer, or their

equivalents, as well as those administrative, policy, technical staff, and personnel designated to interact with the Government in executing the DIB CS Program (e.g., typically 3-10 company designated POCs however the upper limit is at the company's discretion). After joining the Program, DIB CS participants provide updated POC information to DoD when personnel changes occur.

The DIB CS Program implements statutory authorities to established programs and activities to protect sensitive DoD information, including when such information resides on or transits information systems operated by contractors in support of DoD activities. Authorities include 32 Code of Federal Regulations Part 236, "DoD's DIB CS Activities," which authorizes the voluntary DIB CS Information Sharing Program. In addition, the Federal Information Security Modernization Act of 2014 authorizes DoD to oversee agency information security policies and practices, for systems that are operated by DoD, a contractor of the Department, or another entity on behalf of DoD that process any information, the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on DoD's mission. Activities under this information collection policy also support DoD's critical infrastructure protection responsibilities, as the sector specific agency for the DIB sector (see Presidential Policy Directive 21 (PPD–21), ''Critical Infrastructure Security and Resilience,'' available at https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

The DIB CS Program is focused on sharing cyber threat information and cybersecurity best practices with DIB CS participants. DoD needs to collect POC information to implement, manage, and administer the Program, and to share cyber threat information with participants. The Government will collect business POC information from all DIB CS participants to facilitate emails, teleconferences, meetings, and other Program activities.

The DIB CS Program uses a web portal (https://dibnet.dod.mil) to gather POC information from DoD contractors when they elect to participate in the Program. Companies

select the "DIB CS Member Login" button to start the application process. Applicants will then be prompted to sign into the application with a valid DoD-approved medium assurance certificate. They are then directed to a DoD Information System Standard Notice and Consent banner that indicates they are accessing a U.S. Government information system and must click the "I Agree" button in order to continue. The next page is the DoD Privacy Statement that includes the Authorities, Purpose, Routine Use(s), Disclosure, Privacy Impact Assessment, Freedom of Information Act Request disclaimers, and an Agency Disclosure Notice, which must be agreed to by the company, by clicking the "I Agree" button, in order to proceed with the application.

Applicants are then required to complete the POC fields that are provided (i.e., Company Name, Company Representative, CEO, CIO, CISO, and any additional POCs). The online application process does not allow applicants to submit the information unless they certify that the information provided is accurate by checking the "Certify Application" box. After entering all contact information, applicants click on the "Submit Application" button that automatically sends an email to the DIB CS Program Office that an application has been submitted.

If companies want to update their POC information, they can access the portal using their DoD-approved medium assurance certificates. Only designated company representatives and the DIB CS Program system administrators may view or update company POC information.

AFFECTED PUBLIC: Businesses or other for-profit; Not-for-profit Institutions.

ANNUAL BURDEN HOURS: 312.

NUMBER OF RESPONDENTS: 935.

RESPONSES PER RESPONDENT: 1.

ANNUAL RESPONSES: 935.

AVERAGE BURDEN PER RESPONSE: 20 minutes.

FREQUENCY: On occasion.

Dated: July 30, 2024.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer,

Department of Defense.

[FR Doc. 2024-17110 Filed: 8/1/2024 8:45 am; Publication Date: 8/2/2024]