of the Armed Forces. The information is used to provide government reviewing officials with necessary information to ensure that both the law and due process considerations are accounted for, including information sufficient for a decision maker to determine that the request is based on a valid judgment and that the SCRA has been complied with.

Affected Public: Individuals or households.

Annual Burden Hours: 1,392

Number of Respondents: 2,783.

Responses per Respondent: 1.

Annual Responses: 2,783

Average Burden per Response: 30 minutes.

Frequency: On occasion.

Dated: July 24, 2024.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2024–17112 Filed 8–1–24; 8:45 am]

BILLING CODE 6001–FR–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD–2024–OS–0090]

Proposed Collection; Comment Request

AGENCY: Office of the 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 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 October 1, 2024.

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) Activities Cyber Incident Reporting; OMB Control Number 0704–0489.

Needs and Uses: DoD designated the DoD Cyber Crime Center (DC3) as the single focal point for receiving all cyber incident reporting affecting the unclassified networks of DoD contractors from industry and other government agencies. DoD collects cyber incident reports using the Defense Industrial Base Network (DIBNet) portal (*https://dibnet.dod.mil*). Mandatory reporting requirements are addressed in a separate information collection under Office of Management and Budget (OMB) Control Number 0704–0478 entitled ''Safeguarding Covered Defense Information, Cyber Incident Reporting, and Cloud Computing'' authorizing the collection of mandatory cyber incident reporting in accordance with 10 United States Code (U.S.C.) 393: ''Reporting on Penetrations of Networks and Information Systems of Certain Contractors,'' 10 U.S.C. 391: ''Reporting on Cyber Incidents with Respect to Networks and Information Systems of Operationally Critical Contractors and Certain Other Contractors, and 50 U.S.C. 3330: ''Reports to the Intelligence Community on Penetrations of Networks and Information Systems of Certain Contractors.

This information collection supports the voluntary sharing of cyber incident information from DoD contractors in accordance with 32 Code of Federal Regulations part 236, ''DoD- DIB CS Activities,'' which authorizes the DIB CS Program. Sharing cyber incident information is critical to DoD's understanding of cyber threats against DoD information systems, programs, and warfighting capabilities. This information helps DoD to inform and mitigate adversary actions that may affect DoD information resident on or transiting unclassified defense contractor networks. 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 processes 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 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 information collection requests data from the reporting companies to enable DoD to better understand the technical details of or related to a cyber-incident, including its potential adverse effect on the company's unclassified information system and the effect, if any, on DoD information residing on or transiting the company's information system; or a company's ability to provide operationally critical support to DoD. The collection includes a request for a company point of contact if DoD has questions regarding the shared information.

Defense contractors are encouraged to share information including cyber threat indicators that they believe may be of value in alerting the Government and others, as appropriate, to adversary activity so that we can develop mitigation strategies and proactively counter threat actor activity. Cyber incidents that are not compromises of covered defense information or do not adversely affect the contractor's ability to perform operationally critical support, may be of interest to the DIB and DoD for situational awareness purposes.

The information collection is based on the DoD contractor's internal assessment and determination that cyber information should be shared with DoD. Once the defense contractor determines that a report will be valuable to the community, they submit a cyber-incident report using the Incident Collection Format (ICF) that can be accessed via the web portal (*https://dibnet.dod.mil*).

DoD established this portal as the single reporting site for cyber incident information, whether mandatory or voluntary. A defense contractor selects the ''Report a Cyber Incident'' button. The defense contractor will then be prompted for their DoD-approved medium assurance certificate to gain access to the ICF. The contractor is then directed to a Privacy Act Statement web page that clearly states all cyber incident reports are stored in accordance with the DIB CS Activities System of Record Notice. Contractors are then allowed to access the ICF and input data. Once a defense contractor completes the ICF, they are given a preview of the ICF to ensure that all the information they are providing is correct. After verifying the information is correct, the defense contractor will then click the ''submit'' button. A reporting submission ID number is provided when the report is submitted. DoD uses this number to track the report and actions related to the report.

The report is analyzed by cyber threat experts at DC3 and they, in turn, develop written products that include analysis of the threat, mitigations, and indicators of adversary activity. These anonymized products are shared with authorized DoD personnel, other Federal agencies and designated points of contact in defense companies participating in the DIB CS Program. The products developed by DC3 do not contain company attribution, proprietary or personal information, but are vital to improving network security within the Government and the DIB.

Affected Public: Businesses or other for-profit; Not-for-profit Institutions.

Annual Burden Hours: 85,000.

Number of Respondents: 8,500.

Responses per Respondent: 5.

Annual Responses: 42,500.

Average Burden per Response: 2 hours.

Frequency: On occasion.

Dated: July 30, 2024.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2024–17109 Filed 8–1–24; 8:45 am]

BILLING CODE 6001–FR–P

DEPARTMENT OF DEFENSE

Office of the Secretary

Defense Science Board; Notice of Federal Advisory Committee Meeting

AGENCY: Under Secretary of Defense for Research and Engineering, Defense Science Board, Department of Defense (DoD).

ACTION: Notice of Federal advisory committee meeting.

SUMMARY: The DoD is publishing this notice to announce that the following Federal Advisory Committee meeting of the Defense Science Board (DSB) will take place.

DATES: Closed to the public Monday, August 26, 2024 from 8:00 a.m. to 4:30 p.m., closed to the public Tuesday, August 27, 2024 from 8:00 a.m. to 4:30 p.m., closed to the public Wednesday, August 28, 2024 from 8:00 a.m. to 4:30 p.m., closed to the public Thursday, August 29, 2024 from 8:00 a.m. to 4:30 p.m., and closed to the public Friday, August 30, 2024 from 8:00 a.m. to 12:00 p.m..

ADDRESSES: The address of the closed meetings is 1 University Circle, Monterey, CA 93943.

FOR FURTHER INFORMATION CONTACT: Ms. Elizabeth J. Kowalski, Designated Federal Officer (DFO): (703) 571–0081 (Voice), (703) 697–1860 (Facsimile), *elizabeth.j.kowalski.civ@mail.mil,* (Email) Mailing address is Defense Science Board, 3140 Defense Pentagon, Washington, DC 20301–3140. Website: *http://www.acq.osd.mil/dsb/.* The most up-to-date changes to the meeting agenda can be found on the website.

SUPPLEMENTARY INFORMATION: This meeting is being held under the provisions of chapter 10 of title 5, United States Code (U.S.C.) (commonly known as the ''Federal Advisory Committee Act'' or ''FACA''); section 552b(c) of title 5, U.S.C.; and sections 102–3.140 and 102–3.150 of title 41, Code of Federal Regulations (CFR).

Purpose of the Meeting: The mission of the DSB is to provide independent advice and recommendations on matters relating to the DoD's scientific and technical enterprise. The objective of the meeting is to obtain, review, and evaluate classified information related to the DSB's mission. The DSB will discuss the 2024 DSB Summer Study on Advanced Capabilities for Potential Future Conflict and classified strategies for continued development of symmetric and asymmetric capabilities.

Agenda: The meeting will begin on Monday, August 26, 2024 at 8:00 a.m. DSB DFO Executive Director, Elizabeth Kowalski, will provide brief administrative remarks. Dr. Eric Evans, DSB Chair, will provide opening remarks and a classified overview of the objectives of the 2024 Summer Study on Advanced Capabilities for Potential Future Conflict. Next, Dr. David Honey, Deputy Under Secretary of Defense for Research and Engineering (DUSD(R&E)), will provide remarks regarding the objectives of the 2024 Summer Study on Advanced Capabilities for Potential Future Conflict. Next, the DSB will conduct a dry run of the current summary of findings on the development of symmetric and asymmetric capabilities that will characterize future conflicts. Following a break, members will discuss classified strategies that best enable DoD's continued development of symmetric and asymmetric capabilities that will characterize future conflicts. The session will adjourn at 4:30 p.m. The meeting will continue Tuesday, August 27, 2024, at 8:00 a.m. The DSB will discuss classified strategies that best enable DoD's continued development of symmetric and asymmetric capabilities that will characterize future conflicts, with a break midday. The session will adjourn at 4:30 p.m. On Wednesday, August 28, 2024 at 8:00 a.m., the DSB will proceed through a dry run of the current summary of findings on the development of symmetric and asymmetric capabilities that will characterize future conflicts. Following a break, members will discuss classified strategies that best enable DoD's continued development of symmetric and asymmetric capabilities that will characterize future conflicts. The session will adjourn at 4:30 p.m. On Thursday, August 29, 2024, at 8:00 a.m., the DSB will discuss classified strategies that best enable DoD's continued development of symmetric and asymmetric capabilities that will characterize future conflicts, with a break midday. The session will adjourn at 4:30 p.m. On the final day, Friday, August 30, 2024, the meeting will begin at 8:00 a.m. The DSB will proceed through a Dry Run of the current summary of findings on the development of symmetric and asymmetric capabilities that will characterize future conflicts. Members will deliberate and vote on the finalized product. The meeting will adjourn at 12:00 p.m.

Meeting Accessibility: In accordance with section 1009(d) of title 5, U.S.C. and section 102–3.155 of title 41 CFR, the DoD has determined that the DSB meeting will be closed to the public. Specifically, the DUSD(R&E), in