

equipment; classified and unclassified software and software support; publications, manuals, and technical documentation; precision measurement, calibration, lab equipment, and technical support services; studies and surveys; and other related elements of aircraft maintenance and program support.

(iv) *Military Department: Air Force (PK-D-QAP)*

(v) *Prior Related Cases, if any: PK-D-NAP, PK-D-SAF, PK-D-QAJ, PK-D-QCX*

(vi) *Sales Commission, Fee, etc., Paid, Offered, or Agreed to be Paid: None known at this time.*

(vii) *Sensitivity of Technology Contained in the Defense Article or Defense Services Proposed to be Sold: None*

(viii) *Date Report Delivered to Congress: September 7, 2022*

* As defined in Section 47(6) of the Arms Export Control Act.

POLICY JUSTIFICATION

Pakistan—F-16 Case for Sustainment

The Government of Pakistan has requested to consolidate prior F-16 sustainment and support cases to support the Pakistan Air Force F-16 fleet by reducing duplicate case activities and adding additional continued support elements. Included are U.S. Government and contractor engineering, technical, and logistics services for follow-on support of Pakistan's F-16 fleet to include participation in F-16 Aircraft Structural Integrity Program, Electronic Combat International Security Assistance Program, International Engine Management Program, Engine Component Improvement Program, and other technical coordination groups; aircraft and engine hardware and software modifications and support; aircraft and engine spare repair/return parts, accessories and support equipment; classified and unclassified software and software support; publications, manuals, and technical documentation; precision measurement, calibration, lab equipment, and technical support services; studies and surveys; and other related elements of aircraft maintenance and program support. The estimated total cost is \$450 million.

This proposed sale will support the foreign policy and national security objectives of the United States by improving the security of a partner nation that is a force for political stability in the region by allowing Pakistan to retain interoperability with U.S. and coalition forces in ongoing

counterterrorism efforts and in preparation for future contingency operations.

The proposed sale will improve Pakistan's capability to meet current and future threats by continuing the sustainment of its F-16 fleet, which is the Pakistan Air Force's premier multi-role jet fighter and greatly improves Pakistan's ability to project combat power in support of counterterrorism through its robust air-to-ground capability. Pakistan will have no difficulty absorbing these articles and services into its armed forces.

The proposed sale of this equipment and support will not alter the basic military balance in the region.

The principal contractor will be Lockheed Martin Corporation, Fort Worth, TX. There are no known offsets proposed in conjunction with this sale.

Implementation of this proposed sale will not require the assignment of any additional U.S. Government or contractor representatives to Pakistan.

There will be no adverse impact on U.S. defense readiness as a result of this proposed sale.

[FR Doc. 2024-17041 Filed 8-1-24; 8:45 am]

BILLING CODE 6001-FR-P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2024-OS-0087]

Proposed Collection; Comment Request

AGENCY: Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense (DoD).

ACTION: 60-Day information collection notice.

SUMMARY: In compliance with the *Paperwork Reduction Act of 1995*, the Defense Health Agency 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 Defense Finance and Accounting Service, 8899 E 56th St., Indianapolis, IN 46249, ATTN: Ms. Kellen Stout, (317) 212-1801.

SUPPLEMENTARY INFORMATION:

Title; Associated Form; and OMB Number: Involuntary Allotment Application; DD Form 2653; OMB Control Number 0730-0018.

Needs and Uses: This collection of information is in response to requests for involuntary allotments. Before responding to a request, the responsible government official must have information that identifies both the applicant and the member against whom the involuntary allotment is sought; proves that the request is based on a valid court judgment; shows that the judgment comports with the provision of the Soldiers and Sailors Civil Relief Act (SCRA); and enables consideration for whether exigencies of military duty caused the absence of the member from a judicial proceeding upon which the judgment is based. With the exception of information concerning exigencies of military duty, an applicant for an involuntary allotment must provide required information before a government official can act on the applicant's request. The information from the DD Form 2653 is used by DFAS officials to determine whether an involuntary allotment should be established against the pay of a member

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.