Center, Seattle, WA
Contracting Activity: FEDERAL AVIATION ADMINISTRATION, DEPT OF TRANS
Service Type: Janitorial/Custodial
Mandatory for: United States Geological Survey Building: Colorado School of Mines, Golden, CO
Mandatory Source of Supply: Bayaud Industries, Inc., Denver, CO
Contracting Activity: OFFICE OF POLICY, MANAGEMENT, AND BUDGET, NBC ACQUISITION SERVICES DIVISION
Service Type: Facility Management, Grounds Maintenance Service
Mandatory for: Wheeler Army Air Field, Schofield, HI
Tripler Army Medical Center, Tripler AMC, HI
Schofield Barracks, Schofield, HI
Helemano Military Reservation, Wahiawa, HI
Fort Shafter, HI
Mandatory Source of Supply: Lanakila Pacific, Honolulu, HI
Contracting Activity: DEPT OF THE ARMY, 0413 AQ HQ
Service Type: Janitorial/Custodial
Mandatory for: Northwestern Bank Building,Washington, DC
Mandatory Source of Supply: Melwood Horticultural Training Center, Inc., Upper Marlboro, MD
Contracting Activity: FEDERAL PRISON SYSTEM, TERMINAL ISLAND, FCI

Patricia Briscoe,

Deputy Director, Business Operations (Pricing and Information Management).

[FR Doc. 2019–10277 Filed 5–16–19; 8:45 am]

BILLING CODE 6353–01–P

CONSUMER PRODUCT SAFETY COMMISSION

Sunshine Act Meeting

TIME AND DATE: Tuesday, May 21, 2019, 10:00 a.m.–12:00 p.m.

PLACE: Hearing Room 420, Bethesda Towers, 4330 East-West Highway, Bethesda, MD.

STATUS: Commission Meeting—Open to the Public.

MATTERS TO BE CONSIDERED: Decisional Matter: Fiscal Year 2019 Mid-Year Review.

A live webcast of the Meeting can be viewed at *https://www.cpsc.gov/live.*

CONTACT PERSON FOR MORE INFORMATION: Alberta E. Mills, Office of the Secretariat, Office of the General Counsel, U.S. Consumer Product Safety Commission, 4330 East-West Highway, Bethesda, MD 20814, (301) 504–7923.

Dated: May 14, 2019.

Alberta E. Mills,

Secretary of the Commission.

[FR Doc. 2019–10386 Filed 5–15–19; 11:15 am]

BILLING CODE 6355–01–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DOD–2019–OS–0058]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary, DoD.

ACTION: Notice of a modified system of records.

SUMMARY: The Office of the Secretary of Defense (OSD) proposes to modify a system of records notice entitled ''Defense Industrial Base (DIB) Cybersecurity (CS) Activities Records,'' DCIO 01. The primary use of this system is to facilitate the sharing of cybersecurity threat information and best practices among the companies that make up the Defense Industrial Base (DIB). When incidents are received, they are analyzed for cyber threats and vulnerabilities in order to develop response measures as well as improve U.S. Government and DIB understanding of advanced cyber security threat activity.

DATES: Comments will be accepted on or before June 17, 2019. This proposed action will be effective the date following the end of the comment period unless comments are received which result in a contrary determination.

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

* *Federal Rulemaking Portal: http://www.regulations.gov*.

Follow the instructions for submitting comments.

* *Mail:* Department of Defense, Office of the Chief Management Officer, Directorate for Oversight and Compliance, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350–1700.

Instructions: All submissions received must include the agency name and docket number 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: Ms. Luz D. Ortiz, Chief, Records, Privacy and Declassification Division (RPD2), 1155 Defense Pentagon, Washington, DC 20301–1155, or by phone at (571) 372–0478.

SUPPLEMENTARY INFORMATION: The Office of the Secretary of Defense proposes to modify a system of records subject to the Privacy Act of 1974, 5 U.S.C. 552a, the Defense Industrial Base (DIB) Cybersecurity (CS) Activities Records, DCIO 01. The sharing of cybersecurity threat information incident information is critical to DoD's understanding of cyber threats against DoD information, programs and warfighting capabilities systems. 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 2002 (FISMA) 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.

As a result of reviewing this system of records notice, the OSD proposes to modify this system by updating the following sections: Authorities, purpose, categories of records, routine uses, retrieval of records, retention and disposal, record access procedures, contesting record procedures, notification procedures, and history.

The OSD notices for systems of records subject to the Privacy Act of 1974, as amended, are published in the **Federal Register** and are available from the address in **FOR FURTHER INFORMATION CONTACT** or at the Defense Privacy, Civil Liberties, and Transparency Division website at *https://defense.gov/privacy*.

The proposed systems reports, as required by the Privacy Act, as amended, were submitted on February 1, 2019, to the House Committee on Oversight and Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to Section 6 to OMB Circular No. A–108, ''Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act,'' revised December 23, 2016 (December 23, 2016, 81 FR 94424).

Dated: May 13, 2019.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER

Defense Industrial Base (DIB) Cybersecurity (CS) Activities Records, DCIO 01.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Defense Industrial Base (DIB) Cybersecurity Program, 6000 Defense Pentagon, ATTN: DIB CS Program, Washington, DC 20301–6000.

DoD Cyber Crime Center, 911 Elkridge Landing Road, Linthicum, MD 21090–2991.

SYSTEM MANAGER(S):

Director, DIB Cybersecurity, 6000 Defense Pentagon, ATTN: DIB CS Program, Washington, DC 20301–6000, 703–604–3167, *OSD.DIBCSIA@MAIL.MIL*.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

10 U.S.C. 391, Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors; 10 U.S.C. 393, Reporting on penetrations of networks and information systems of certain contractors; 10 U.S.C. 2224, Defense Information Assurance Program; 50 U.S.C. 3330, Reports to the intelligence community on penetrations of networks and information systems of certain contractors; 32 CFR 236, Department of Defense (DoD)'s Defense Industrial Base (DIB) Cybersecurity (CS) Activities; and DoDI 5205.13, Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities.

PURPOSE(S) OF THE SYSTEM:

To facilitate communications and the sharing of cyber threat information among DIB CS Program participants.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Supporting DoD contractor (hereafter referred to as 'DIB company') personnel (points of contact and individuals submitting cyber incident reports) providing DIB company information.

CATEGORIES OF RECORDS IN THE SYSTEM:

DIB company point of contact information includes name, company name and mailing address, work division/group, work email, and work telephone number; cyber incident reports submitted by DIB companies are identified by incident numbers, and include information detailing the cyber incident.

RECORD SOURCE CATEGORIES:

The individual and participating DIB companies.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to the disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To other participating DIB companies to facilitate the sharing of information and expertise related to the DIB CS Program including cyber threat information and best practices, and mitigation strategies.

b. To contractors working with the DIB CS Program and contractors supporting government activities related to the implementation of 32 CFR part 236 and safeguarding covered defense information and cyber incident reporting in accordance with U.S. Department of Defense Federal Acquisition Regulation Supplement (DFARS) 252.204–7009, Limitations on the use or disclosure of third-party contractor reported cyber incident information.

c. To appropriate Federal, State, local, territorial, tribal, foreign, or international agencies for the purpose of counterintelligence activities authorized by U.S. law or Executive Order, or for the purpose of executing or enforcing laws designed to protect the national security or homeland security of the United States, including those relating to the sharing of records or information concerning terrorism, homeland security, or law enforcement.

d. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

e. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

f. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

g. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

h. To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

i. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Electronic storage media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

DIB company point of contact (POC) information is retrieved primarily by company name and work division/group and secondarily by individual POC name. DIB cyber incident reports are primarily retrieved by incident number but may also be retrieved by company name. They are not retrieved by the individual name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The master file consisting of DIB participant information is destroyed three years after the participating company withdraws from the program, closes, or goes out of business. Other records closed annually and are destroyed 10 years after cut off.

ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS

Records are accessed by personnel with security clearances who are properly screened, trained, under a signed confidentiality agreement, and determined to have ''need to know.'' Access to records requires DoD Common Access Card (CAC) and PIN. Physical access controls include security guards, identification badges,

key cards, cipher locks, and combination locks.

RECORD ACCESS PROCEDURES:

Individuals seeking access to information about themselves contained in this system of records should address inquiries to the Office of the Secretary of Defense/Joint Staff (OSD/JS), Freedom of Information Act (FOIA) Requester Service Center, 1155 Defense Pentagon, Washington, DC 20301–1155. Signed, written requests should contain the individual's name, company name and work division/group, and the name and number of this system of records notice. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: ''I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).''

If executed within the United States, its territories, possessions, or commonwealths: ''I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).''

CONTESTING RECORD PROCEDURES:

The Office of the Secretary of Defense (OSD) rules for accessing records, for contesting contents, and for appealing initial agency determinations are contained in OSD Administrative Instruction 81; 32 CFR part 311; or may be obtained from the system manager.

NOTIFICATION PROCEDURES:

Individuals seeking to determine whether this system of records contains information on themselves should address inquiries to Director, DIB Cybersecurity Office, 6000 Defense Pentagon, ATTN: DIB CS Program, Washington, DC 20301–6000. Signed, written requests should contain the individual's name, and company name and work division/group. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: ''I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).''

If executed within the United States, its territories, possessions, or commonwealths: ''I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).''

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

May 21, 2015, 80 FR 29315; May 8, 2012, 77 FR 29616.

[FR Doc. 2019–10207 Filed 5–16–19; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

Notice of Intent To Prepare an Environmental Impact Statement (EIS) for the Long Range Discrimination Radar (LRDR) at Clear Air Force Station (CAFS)

AGENCY: Missile Defense Agency, Department of Defense.

ACTION: Notice of intent.

SUMMARY: The Missile Defense Agency (MDA) announces its intention to prepare an Environmental Impact Statement (EIS) in accordance with the National Environmental Policy Act (NEPA) of 1969 and the Council on Environmental Quality Regulations for Implementing the Procedural Provisions of NEPA. MDA began construction of the LRDR following a 2016 Environmental Assessment (EA) and Finding of No Significant Impact (FONSI). Due to threat evolution, operational requirements have created the need to expand the current Special Use Airspace (SUA) at Clear Air Force Station (AFS) to protect nearby aircraft. Several potential designs of the additional SUA have been developed. The MDA is preparing this EIS to evaluate potential environmental impacts that could result from the LRDR SUA alternatives. The Department of Defense has not selected a preferred alternative for the proposed SUA.

DATES: Scoping meetings will be held in the Alaskan communities of Anderson, Fairbanks and Anchorage during June 2019. Notification of the meeting locations, dates, and times will be published and announced in local news media prior to public scoping meetings.

The MDA invites public comments on the scope of the LRDR EIS during a 30-day public scoping period beginning with publication of this notice in the **Federal Register**. Comments will be accepted on or before June 17, 2019.

ADDRESSES: Written comments, statements, and/or concerns regarding the scope of the EIS or requests to be added to the EIS distribution list should be addressed to MDA CAFS EIS and sent by email to *info@cleareis.com,* by facsimile 907–644–2022, or by U.S. Postal Service to Clear EIS c/o HDR, Inc., 2525C Street, Suite 500, Anchorage, AK 99503. Electronic or facsimile comments are preferred. If sending comments by U.S. Postal Service, please do not submit duplicate electronic or facsimile comments. All comments, including names and addresses, will be included in the administrative record.

FOR FURTHER INFORMATION CONTACT: Mark Wright, MDA Public Affairs at 256–450–1599 or by email: *mda.info@mda.mil.* Additional information can be found at MDA's website: *https://www.mda.mil/news/nepa_documents.html.*

SUPPLEMENTARY INFORMATION: In accordance with 40 Code of Federal Regulations (CFR) 1501.6, cooperating agencies for consultation, review, and comment on the EIS include the Federal Aviation Administration (FAA) and U.S. Air Force (USAF). Other cooperating agencies may be identified during the scoping process.

An initial EA was prepared in April 2016 and resulted in a FONSI in June 2016 to support the construction and operation of the LRDR. A detailed analysis of all resource categories was assessed in the EA. Since that time, the adversary threat evaluation has evolved requiring changes to the LRDR's plans for operation, which in turn required MDA to reexamine the LRDR's operational tempo and battlespace coverage. To meet these more challenging requirements, LRDR operational and system procedures were adapted, resulting in expanded requirements for a Special Use Airspace (SUA) at CAFS that will provide continual protection for aircraft from LRDR High Intensity Radiated Fields (HIRF).

Restricted Area R–2206 is currently in effect at CAFS. Designed and implemented over 50 years ago to support the original Ballistic Missile Early Warning System (BMEWS) and its replacement, the Upgraded Early Warning Radar (UEWR), R–2206 will no longer be sufficient to protect aircraft from HIRF levels that will be generated by the more powerful LRDR in its expanded role discussed in this notice. Alternative designs for the additional Restricted Area have been developed. The EIS will analyze potential environmental impacts from each alternative. Our preliminary indications are that the majority of impacts will be in the areas of socioeconomics and airspace. However, to the extent these impacts differ from those analyzed in the 2016 EA, we will analyze them in this EIS process.