Contract Rates

Regular Time: Services provided during any 8-hour shift.

Overtime: Services provided outside the inspector's normal work schedule.

In addition to any hourly service charge, a night differential fee equal to 10 percent of the employee's hourly salary will be charged for each hour of service provided after 6:00 p.m. and before 6:00 a.m. A guarantee of payment is required for all contracts equal to three months of service or $10,000, whichever is greater.

Non-Contract Rates

Regular time: Services provided within the inspector's normal work schedule, Monday through Friday.

Overtime: Services provided outside the inspector's normal work schedule.

Any services under contract in excess of the contracted hours will be charged at the non-contract rate.

Contract Rates

Non-HACCP Contracts

REGULAR TIME $238
OVERTIME $357
SUNDAY & HOLIDAYS $476

HACCP/QMP Contracts

HACCP REGULAR $238
HACCP OVERTIME $357
HACCP SUNDAY & HOLIDAYS $476

All Non-Contract Work Rates

REGULAR TIME $357
OVERTIME $536
SUNDAY & HOLIDAYS $714

Certificates

All certificate requests, whether or not a product inspection was conducted, will be billed at a set flat rate of $97 per request.

Additional information about, and applications for, Program services and fees may be obtained from NMFS (see **FOR FURTHER INFORMATION CONTACT**).

Dated: August 28, 2023.

Alexa Cole,

Director, Office of International Affairs, Trade, and Commerce, National Marine Fisheries Service.

[FR Doc. 2023–18886 Filed 8–31–23; 8:45 am]

BILLING CODE 3510–22–P

COMMODITY FUTURES TRADING COMMISSION

Sunshine Act Meetings

TIME AND DATE: 9:00 a.m. EDT, Friday, September 8, 2023.

PLACE: Virtual meeting.

STATUS: Closed.

MATTERS TO BE CONSIDERED: Enforcement matters. In the event that the time, date, or location of this meeting changes, an announcement of the change, along with the new time, date, and/or place of the meeting will be posted on the Commission's website at *https://www.cftc.gov/.*

CONTACT PERSON FOR MORE INFORMATION: Christopher Kirkpatrick, 202–418–5964.

Authority: 5 U.S.C. 552b.

Dated: August 30, 2023.

Robert Sidman,

Deputy Secretary of the Commission.

[FR Doc. 2023–19077 Filed 8–30–23; 4:15 pm]

BILLING CODE 6351–01–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD–2023–OS–0075]

Privacy Act of 1974; System of Records

AGENCY: Department of Defense (DoD).

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the DoD is establishing a new Department-wide system of records titled, ''Information Technology Access and Audit Records,'' DoD–0019. This system of records covers DoD's maintenance of records related to requests for user access, attempts to access, granting of access, records of user actions for DoD information technology (IT) systems, and user agreements. This includes details of programs, databases, functions, and sites accessed and/or used, and the information products created, received, or altered during the use of IT systems. This new system of records will be included in the DoD's inventory of record systems.

DATES: This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before October 2, 2023. The Routine Uses are effective at the close of the comment period.

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

* *Federal Rulemaking Portal: https://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, Attn: 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 *https://www.regulations.gov* as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Rahwa Keleta, Privacy and Civil Liberties Division, Directorate for Privacy, Civil Liberties, and Freedom of Information, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Department of Defense, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350–1700; *OSD.DPCLTD@mail.mil;* (703) 571–0070.

SUPPLEMENTARY INFORMATION:

I. Background

DoD is establishing ''Information Technology Access and Audit Records (ITAAR)'', DoD–0019, as a DoD-wide Privacy Act system of records. A DoD-wide System of Records Notice (SORN) supports multiple DoD paper or electronic recordkeeping systems operated by more than one DoD component that maintain the same kind of information about individuals for the same purpose. Establishment of DoD-wide SORNs helps DoD standardize the rules governing the collection, maintenance, use, and sharing of personal information in key areas across the enterprise. DoD-wide SORNs also reduce duplicative and overlapping SORNs published by separate DoD components. The creation of DoD-wide SORNs is expected to make locating relevant SORNs easier for DoD personnel and the public, and create efficiencies in the operation of the DoD privacy program.

The purpose of this system is to control and track individual user access to and activity on networks, computer systems, applications, databases, or other digital technologies controlled by DoD Offices and Components. DoD may use the records in this system to investigate potential or alleged improper use or other improper activity by a system user, which may be a DoD employee, contractor, or other individual. Records from this system may be shared with or used by the appropriate investigative or cybersecurity organizations within the Office or Component with which the individual user is affiliated, other DoD

Components, and other agencies with investigative and cybersecurity authority. The records may also be used for statistical data and reporting purposes, to inform decisions concerning hardware or software upgrades, and communications technology requirements.

DoD SORNs have been published in the **Federal Register** and are available from the address in **FOR FURTHER INFORMATION CONTACT** or at the Privacy, Civil Liberties, and Freedom of Information Directorate website at *https://dpcld.defense.gov.*

II. Privacy Act

Under the Privacy Act, a ''system of records'' is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A–108, DoD has provided a report of this system of records to the OMB and to Congress.

Dated: August 24, 2023.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER:

Information Technology Access and Audit Records (ITAAR), DoD–0019.

SECURITY CLASSIFICATION:

Unclassified and classified.

SYSTEM LOCATION:

Department of Defense (Department or DoD), located at 1000 Defense Pentagon, Washington, DC 20301–1000, and other Department installations, offices, or mission locations. Information may also be stored within a government-certified cloud, implemented and overseen by the Department's Chief Information Officer (CIO), 6000 Defense Pentagon, Washington, DC 20301–6000.

SYSTEM MANAGER(S):

The system managers are as follows:

A. Principal Director for Resources, Department of Defense, Chief Information Officer, 6000 Defense Pentagon, Washington, DC 20301–6000, *osd.pentagon.dod-cio.mbx.dod-records-officer@mail.mil.*

B. To obtain information on the system managers at the Military Departments, Combatant Commands, Defense Agencies, Field Activities, or other DoD components with oversight of the records, please visit *www.FOIA.gov* to contact the component's Freedom of Information Act (FOIA) office.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Public Law 113–283, The Federal Information Security Modernization Act of 2014, as amended (44 U.S.C. Chapter 35, Subch. II); 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 142, Chief Information Officer; 5 U.S.C. 301, Departmental Regulations; 10 U.S.C Section 164, Commanders of Combatant Commands: Assignment; Powers and Duties; 18 U.S.C. 1029, Fraud and Related Activity in Connection with Access Devices; 18 U.S.C. 1030, Fraud and Related Activity in Connection with Computers; Section 922 of the National Defense Authorization Act for FY 2012 (Pub. L. 112–81), ''Insider Threat Detection''; Executive Order (E.O.) 10450, Security Requirements for Government Employees, as amended; E.O. 14028, Improving the Nation's Cybersecurity; E.O. 13526, ''Classified National Security Information''; E.O. 13587, ''Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information''; DoD Directive 5205.16, ''The DoD Insider Threat Program''; DoD Instruction (DoDI) 8500.01, ''Cybersecurity,''; DoDI 8530.01, ''Cybersecurity Activities Support to DoD Information Network Operations,'' and E.O. 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to:

A. Control and to track individuals' access to and use of classified and unclassified DoD networks, information systems, devices, applications, databases, and other digital technologies (collectively, technologies) controlled by DoD Offices and Components; ensure the ongoing confidentiality, availability, and integrity of DoD technologies and data; ensure no conflicts of interest defend DoD technologies and data from adverse actors; and detect and report threats or vulnerabilities;

B. Review DoD-funded award applicants'/recipients' information to monitor individual user compliance with applicable Terms of Use;

C. Maintain information necessary to support investigations into or adverse actions resulting from alleged or possible improper use or other improper activity by an employee, contractor or other individual relating to use or access to DoD Office, Component and common technologies and data;

D. Refer record(s) that appear to indicate a violation or potential violation of law to the appropriate disciplinary, law enforcement, intelligence, counterintelligence, security or cybersecurity organization within or outside of DoD for investigation or other action;

E. Using statistical data from this system: assess system or network efficiency; calculate workloads; make business decisions regarding upgrading hardware, software, and communications technology to meet changing use requirements; and

F. Generate reports related to the purposes above.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Civilian and military personnel, contractor employees, and other individuals who request or are granted access to DoD Office, Component, and common technologies and data.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records include:

A. Access Request Records: Records created as part of the process of determining user eligibility and need for access to specific technologies, such as requests for access to DoD Office, Component, and common technologies and data; grants or denials of such requests; justifications and other information supporting requests for access; and records documenting the suspension or revocation of access for misuse, non-use, or other reasons.

B. Identity records: Identifying, status, and contact information about the individual, such as the individual's name, date of birth, DoD identification (ID) Number/Electronic Data Exchange Personal Identifier (EDIPI), citizenship, work addresses and telephone numbers, office symbol, computer and Voice Over Internet Protocol (VOIP) logon addresses, contractor/employee status, verification of need-to-know, training status, and security clearance data.

C. System Access Records: Records created as part of the user identification and authorization process to gain access to systems, such as user agreements; user profiles; login files; password files; audit trail files and extracts; system usage files; and cost-back files used to assess charges for system use.

D. email addresses.

E. Internet Protocol (IP) addresses.

F. Machine Access Control (MAC) addresses.

G. Audit trails of user activities.

H. Technical support data.

I. Telework status, activity, and location (*e.g.,* city/state).

J. Contractors: information may also include company name, contract number, contract value, and contract expiration date.

K. Funding award holders: information may also include name, email, digital persistent identifier, grant or award number, funding value, and award expiration date.

RECORD SOURCE CATEGORIES:

Typically, information in the record is originally supplied by the record subject, their supervisors, and personnel security staff. Some data, such as user identification codes, are assigned or supplied by the Information Technology staff. Details about system access and use are typically supplied by the Information Technology system, which includes applications, networks, and databases.

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

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, all or a portion of the records or information 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 contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government when necessary to accomplish an agency function related to this system of records.

B. 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.

C. 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.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. 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.

F. 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.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines 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.

H. 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.

I. To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or other review as authorized by the Inspector General Act of 1978, as amended.

J. To such recipients and under such circumstances and procedures as are mandated by Federal statute, treaty, or other international agreement.

K. To Federal, state, or local agencies or professional organizations or associations, maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, or administrative or disciplinary information, or disciplinary records related to suspended or revoked licenses, if necessary to obtain information relevant to a DoD component or agency decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

L. To a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, funding awards, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

M. To foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

N. To foreign or non-DoD law enforcement for the purpose of counterintelligence activities authorized by U.S. Law or Executive Order or for the purpose of enforcing laws which protect the national security of the United States.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records may be stored locally on digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by individual's name, DoD ID number/EDIPI, digital persistent identifier, or date of action. In some instances, records may be retrieved by other identifiers assigned by the DoD Office or Component.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

User identification records generated according to preset requirements are retained in accordance with General Records Schedule (GRS) 3.2, Item 30. Records may be destroyed when no longer needed for business use.

User identification records associated with systems that are highly sensitive or potentially vulnerable are retained in accordance with GRS 3.2, Item 31. Records may be destroyed 6 years after the password is altered or the user account is terminated. These records may be retained longer if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

DoD safeguards records in this system of records according to applicable rules,

policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, DoD has established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including Common Access Card (CAC) authentication and password; physical token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities. Contractor personnel must pass a background investigation and receive a security clearance. Contractors must also sign nondisclosure documents.

RECORD ACCESS PROCEDURES:

Individuals seeking access to their records should follow the procedures in 32 CFR part 310. Individuals should address written inquiries to the DoD component with oversight of the records, as the component has Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system of records. The public may identify the contact information for the appropriate DoD office through the following website: *www.FOIA.gov.* Signed written requests should contain the name and number of this system of records along with the full name, current address, and email address of the individual. 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 appropriate 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:

Individuals seeking to amend or correct the content of records about them should follow the procedures in 32 CFR part 310.

NOTIFICATION PROCEDURES:

Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

DoD has exempted records maintained in this system from 5 U.S.C. 552a(c)(3); (d)(1), (2), (3), and (4); (e)(1), (e)(4)(G), (H), and (I); and (f) of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(1) and (k2). In addition, when exempt records received from other systems of records become part of this system, the DoD also claims the same exemptions for those records that are claimed for the system(s) of records from which they originated and claims any additional exemptions set forth here. An exemption rule for this system has been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(1), (2), and (3), and (c), and published in 32 CFR part 310.

HISTORY:

None.

[FR Doc. 2023–18682 Filed 8–31–23; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF EDUCATION

[Docket No.: ED–2023–SCC–0156]

Agency Information Collection Activities; Comment Request; Charter Online Management and Performance System (COMPS) SE Grant Profile

AGENCY: Office of Elementary and Secondary Education (OESE), Department of Education (ED).

ACTION: Notice.

SUMMARY: In accordance with the Paperwork Reduction Act (PRA) of 1995, the Department is proposing a new information collection request (ICR).

DATES: Interested persons are invited to submit comments on or before October 31, 2023.

ADDRESSES: To access and review all the documents related to the information collection listed in this notice, please use *http://www.regulations.gov* by searching the Docket ID number ED–2023–SCC–0156. Comments submitted in response to this notice should be submitted electronically through the Federal eRulemaking Portal at *http://www.regulations.gov* by selecting the Docket ID number or via postal mail, commercial delivery, or hand delivery. If the *regulations.gov* site is not available to the public for any reason, the Department will temporarily accept comments at *ICDocketMgr@ed.gov.* Please include the docket ID number and the title of the information collection request when requesting documents or submitting comments. Please note that comments submitted after the comment period will not be accepted. Written requests for information or comments submitted by postal mail or delivery should be addressed to the Manager of the Strategic Collections and Clearance Governance and Strategy Division, U.S. Department of Education, 400 Maryland Ave. SW, LBJ, Room 6W203, Washington, DC 20202–8240.

FOR FURTHER INFORMATION CONTACT: For specific questions related to collection activities, please contact Stephanie Jones, (202) 453–7835.

SUPPLEMENTARY INFORMATION: The Department, in accordance with the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3506(c)(2)(A)), provides the general public and Federal agencies with an opportunity to comment on proposed, revised, and continuing collections of information. This helps the Department assess the impact of its information collection requirements and minimize the public's reporting burden. It also helps the public understand the Department's information collection requirements and provide the requested data in the desired format. The Department is soliciting comments on the proposed information collection request (ICR) that is described below. The Department is especially interested in public comment addressing the following issues: (1) is this collection necessary to the proper functions of the Department; (2) will this information be processed and used in a timely manner; (3) is the estimate of burden accurate; (4) how might the Department enhance the quality, utility, and clarity of the information to be collected; and (5) how might the Department minimize the burden of this collection on the