4310-VH-P

DEPARTMENT OF THE INTERIOR

Bureau of Safety and Environmental Enforcement

[DOI-2021-0007; 212E1700D2 EECC000000 ET1EX0000.G40000]

Privacy Act of 1974; System of Records

AGENCY: Bureau of Safety and Environmental Enforcement, Interior.

ACTION: Notice of a modified system of records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, as amended, the Department of the Interior (DOI) is issuing a public notice of its intent to modify the Bureau of Safety and Environmental Enforcement (BSEE) system of records, BSEE-01, Investigations Case Management System (CMS). DOI is publishing this revised system of records notice to propose a new breach routine use; modify four existing routine uses; update the system manager address; remove references to a cloud system; and provide general and administrative updates in accordance with the Office of Management and Budget Circular (OMB) A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

DATES: This modified system will be effective upon publication. New or modified routine uses will be effective [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]. Submit comments on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: You may send comments identified by docket number [DOI-2021-0007] by any of the following methods:

- Federal eRulemaking Portal: *http://www.regulations.gov*. Follow the instructions for sending comments.
- Email: DOI_Privacy@ios.doi.gov. Include docket number [DOI-2021-0007] in

the subject line of the message.

- U.S. mail or hand-delivery: Teri Barnett, Departmental Privacy Officer, U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC 20240.

Instructions: All submissions received must include the agency name and docket number [DOI-2021-0007]. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Rowena Dufford, Associate Privacy Officer, Bureau of Safety and Environmental Enforcement, 45600 Woodland Road, Sterling, VA 20166, privacy@bsee.gov or 703-787-1257.

SUPPLEMENTARY INFORMATION:

I. Background

BSEE maintains the BSEE-01, Investigations Case Management System (CMS), system of records. The purpose of this system of records is to manage, track and report civil administrative investigations related to operations on the Outer Continental Shelf (OCS). BSEE conducts investigations on safety concerns, environmental risks and incidents which includes but is not limited to reportable injuries, the loss or damage of property, and possible violations of Federal laws and regulations.

While BSEE conducts civil administrative investigations rather than criminal investigations the Bureau may make referrals of possible criminal activity to internal and external law enforcement organizations as appropriate for investigation. Records include known or suspected civil violations; information related to possible criminal activities; incident-related information and observations from other sources; protection efforts; information to justify funding requests and expenditures; investigator training; referrals

and/or recommendations related to incident investigations; and evidence.

Incident and non-incident data related to activity occurring on the OCS is collected in support of investigations, regulatory enforcement, homeland security, and security (physical, personnel, stability, environmental, and industrial) activities. This may include data documenting investigation activities, enforcement recommendations, recommendation results, property damage, injuries and fatalities, and analytical or statistical reports. CMS allows for BSEE management to make informed decisions on recommendations for enforcement, civil penalties, and other administrative actions.

BSEE is publishing this notice to update the system manager address, revise the policies and practices for storage of records section, remove use of a cloud provider in the administrative, technical and physical safeguards section, and make administrative updates to comply with the Office of Management and Budget (OMB) Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

Additionally, BSEE is changing the routine uses from a numeric to an alphabetic list and modifying routine uses A, B, and I to provide additional clarification on external organizations or comply with Federal requirements. Routine use A was modified to further clarify disclosures to the Department of Justice or other Federal agencies when necessary in relation to litigation or judicial proceedings. Modified routine use B clarifies disclosures to a congressional office to respond to or resolve an individual's request made to that office. Modified routine use I allows BSEE to share information with an expert, consultant, grantee, or contractor (including employees of the contractor) of DOI that performs services requiring access to these records on DOI's behalf to carry out the purposes of the system. BSEE is also proposing to modify routine use J and add new routine use K to allow BSEE to share information with appropriate Federal agencies or entities when reasonably necessary to respond to a breach of personally identifiable

information and to prevent, minimize, or remedy the risk of harm to individuals or the Federal Government, or assist an agency in locating individuals affected by a breach in accordance with OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.

This system contains investigatory records related to law enforcement activities that are exempt from certain provisions of the Privacy Act, 5 U.S.C. 552a(k)(2). On January 10, 2020, DOI published a final rule in the *Federal Register* at 85 FR 1282 to amend the DOI Privacy Act regulations at 43 CFR 2.254. This allows DOI, on a case-by-case basis, to withhold records from individuals seeking their records.

II. Privacy Act

The Privacy Act of 1974, as amended, embodies fair information practice principles in a statutory framework governing the means by which Federal agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to records about individuals that are maintained in a "system of records." A "system of records" is a group of any 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. The Privacy Act defines an individual as a United States citizen or lawful permanent resident. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DOI by complying with DOI Privacy Act regulations at 43 CFR Part 2, Subpart K, and following the procedures outlined in the Records Access, Contesting Record, and Notification Procedures sections of this notice.

The Privacy Act requires each agency to publish in the *Federal Register* a description denoting the existence and character of each system of records that the agency maintains and the routine uses of each system. The revised INTERIOR/BSEE-01, Investigations Case Management System, system of records notice is published in its

entirety below. In accordance with 5 U.S.C. 552a(r), DOI has provided a report of this system of records to OMB and to Congress.

III. Public Participation

You should be aware your entire comment including your personally identifiable information, such as your address, phone number, email address, or any other personal information in your comment, may be made publicly available at any time. While you may request to withhold your personally identifiable information from public review, we cannot guarantee we will be able to do so.

SYSTEM NAME AND NUMBER:

INTERIOR/BSEE-01, Investigations Case Management System (CMS).

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records in this system are maintained and centrally managed by the Department of the Interior, Bureau of Safety and Environmental Enforcement (BSEE), 1849 C Street NW, Washington, DC 20240. Records are also located at BSEE regional offices and regional sub-offices, and at DOI contractor locations. A current listing of these offices may be obtained by writing to the System Manager or by visiting the BSEE Web site at http://www.bsee.gov.

SYSTEM MANAGER(S):

CMS System Administrator, Bureau of Safety and Environmental Enforcement, National Investigations Program, 45600 Woodland Rd, Mail Stop VAE-DIR-SIID, Sterling, VA 20166.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Outer Continental Shelf Lands Act of 1953, 43 U.S.C. 1331-1356b; and Oil and

Gas and Sulphur Operations in the Outer Continental Shelf, 30 CFR 250.

PURPOSE(S) OF THE SYSTEM:

The primary purpose of the CMS system of records is to conduct and document incident investigations related to operations on the OCS. CMS is used to manage known and suspected civil violations; capture, integrate, and share incident-related information and observations from other sources; measure performance of investigative programs and management of investigations; meet incident reporting requirements; analyze and prioritize investigative efforts; provide information to justify funding requests and expenditures; provide employee training; provide referrals to appropriate criminal law enforcement agencies for individuals suspected of committing crimes on or in support of activities conducted on the OCS; collect and preserve evidence; and investigate and prevent injuries on the OCS.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals covered in the system include current and former BSEE employees, potential employees, and contractors; other employees and contractors of Federal, tribal, state, and local law enforcement organizations; complainants, informants, suspects, and witnesses; members of the general public, including individuals and/or groups of individuals involved with incidents related to operations on the OCS; and individuals or corporations being investigated due to their involvement in incidents occurring on the OCS.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system includes incident reports, investigative activity reports, personnel records, investigative training records, and records related to incidents occurring on the OCS. Records may contain the following information: names, Social Security numbers, gender, date of birth, place of birth, citizenship status, race or ethnicity, home and work addresses, personal and official phone numbers, personal and official email addresses,

emergency contact information, other contact information, medical information, work history, educational history, affiliations, employer information, associated case or activity number, identification numbers assigned to individuals, and other data that may be included in records compiled during investigations.

Incident reports and records may include attachments such as photos, videos, sketches, audio recordings, email and text messages, medical reports, personnel records, written statements, witness interviews, depositions, evidence and information obtained in the course of an investigation, evidence in support of the Action Referral Memoranda and Case Closure Memoranda, administrative agreements, action determinations, company documentation, and other documents related to incidents occurring on the OCS. Incident reports may also include information concerning criminal activity and documentation related to the response and outcome of an incident. Records in this system also contain information concerning Federal, tribal, state and local law enforcement officers such as an officer's name, contact information, station, and career history.

This system may also contain the names and addresses of business entities, which are not subject to the Privacy Act. However, records pertaining to individuals acting on behalf of corporations and other business entities may reflect personal information that is covered by this system of records notice.

RECORD SOURCE CATEGORIES:

Sources of information in the system include Department, bureau, office and program officials, employees, contractors, and other individuals who are associated with or represent DOI; officials from other Federal, tribal, state and local law enforcement organizations, including DOJ, the Federal Bureau of Investigation, and the Department of Homeland Security, among others; and complainants, informants, suspects, victims, and witnesses.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOI as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other Federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

(1) DOI or any component of DOI;

(2) Any other Federal agency appearing before the Office of Hearings and Appeals;

(3) Any DOI employee or former employee acting in his or her official capacity;

(4) Any DOI employee or former employee acting in his or her individual capacity when DOI or DOJ has agreed to represent that employee or pay for private representation of the employee; or

(5) The United States Government or any agency thereof, when DOJ determines that DOI is likely to be affected by the proceeding.

B. To a congressional office when requesting information on behalf of, and at the request of, the individual who is the subject of the record.

C. To the Executive Office of the President in response to an inquiry from that office made at the request of the subject of a record or a third party on that person's behalf, or for a purpose compatible with the reason for which the records are collected or maintained.

D. To any criminal, civil, or regulatory law enforcement authority (whether Federal, state, territorial, local, tribal or foreign) when a record, either alone or in conjunction with other information, indicates a violation or potential violation of law –

criminal, civil, or regulatory in nature, and the disclosure is compatible with the purpose for which the records were compiled.

E. To an official of another Federal agency to provide information needed in the performance of official duties related to reconciling or reconstructing data files or to enable that agency to respond to an inquiry by the individual to whom the record pertains.

F. To Federal, state, territorial, local, tribal, or foreign agencies that have requested information relevant or necessary to the hiring, firing or retention of an employee or contractor, or the issuance of a security clearance, license, contract, grant or other benefit, when the disclosure is compatible with the purpose for which the records were compiled.

G. To representatives of the National Archives and Records Administration (NARA) to conduct records management inspections under the authority of 44 U.S.C. 2904 and 2906.

H. To state, territorial and local governments and tribal organizations to provide information needed in response to court order and/or discovery purposes related to litigation, when the disclosure is compatible with the purpose for which the records were compiled.

I. To an expert, consultant, grantee, or contractor (including employees of the contractor) of DOI that performs services requiring access to these records on DOI's behalf to carry out the purposes of the system.

J. To appropriate agencies, entities, and persons when:

(1) DOI suspects or has confirmed that there has been a breach of the system of records;

(2) DOI has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOI (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 DOI's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

K. To another Federal agency or Federal entity, when DOI 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.

L. To the Office of Management and Budget (OMB) during the coordination and clearance process in connection with legislative affairs as mandated by OMB Circular A-19.

M. To the Department of the Treasury to recover debts owed to the United States.

N. To the news media and the public, with the approval of the Public Affairs Officer in consultation with counsel and the Senior Agency Official for Privacy, where there exists a legitimate public interest in the disclosure of the information, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

O. To DOJ, the Federal Bureau of Investigation, the Department of Homeland Security, and other Federal, state and local law enforcement agencies for the purpose of reporting possible violations of Federal laws and regulations, referring criminal related activities, and providing information exchange on law enforcement activity.

P. To agency contractors, grantees, or volunteers for DOI or other Federal agencies that assist in the performance of a contract, grant, cooperative agreement, or

other activity related to this system of records and who need to have access to the records in order to perform the activity.

Q. To any of the following entities or individuals for the purpose of providing information on incident investigations, personal injuries, or the loss or damage of property:

(1) Individuals involved in such incidents;

(2) Persons injured in such incidents;

(3) Owners of property damaged, lost or stolen in such incidents, and/or representatives, administrators of estates, and/or attorneys.

The release of information under these circumstances should only occur when it will not interfere with ongoing investigations or law enforcement proceedings; risk the health or safety of an individual; or reveal the identity of an informant or witness that has received an explicit assurance of confidentiality. Also, Social Security numbers and other sensitive identifying personal information should not be released under these circumstances unless this information belongs to the individual requestor.

R. To any criminal, civil, or regulatory authority (whether Federal, state, territorial, local, tribal or foreign) for the purpose of providing background search information on individuals for legally authorized purposes, including but not limited to background checks on individuals residing in a home with a minor or individuals seeking employment opportunities requiring background checks.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are stored in electronic media and paper files. All records are accessed only by authorized personnel who have a need to access the records in the performance of their official duties. Paper records are contained in file folders and stored in locked file

cabinets. Records obtained in a paper format and converted into electronic files in CMS may be temporarily stored or accessed on DOI network computers, email systems, and approved removable hard drives.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information may be retrieved by first name, middle name, or last name, home and work addresses, personal and official phone numbers, personal and official email addresses, employer information, and associated case or activity number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in this system are maintained under BSEE Bucket 5 – Regulatory Oversight and Stewardship (N1-473-12-5), which has been approved by NARA. Records maintained under Item 5F(2)(a), Major Incident Investigative Records, include final reports that document major incidents requiring investigative panels and other reports selected as significant by BSEE, and have a permanent retention. Electronic records are transferred to NARA 15 years after cut-off, and hardcopy reports are transferred to NARA 25 years after cut-off. Records maintained under Item 5F(2)(b), All Other Incident Investigative and Related Records, include records that do not result in the appointment of a panel or are not selected as significant by BSEE. These records have a temporary disposition and are destroyed 25 years after cut-off. Other administrative records are maintained under BSEE Bucket-1, Administrative Records (N1-473-12-001), which has been approved by NARA. Records maintained under Item IG(1), Administrative Function Files/Audits and Investigation Files, have a temporary disposition, and are cut off at the end of the fiscal year when activity is completed and destroyed 10 years after cut off. Approved disposition methods for temporary records include shredding or pulping paper records, and erasing or degaussing electronic records in accordance with NARA guidelines and Departmental policy.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

The records contained in this system are safeguarded in accordance with 43 CFR 2.226 and other applicable security rules and policies. During normal hours of operation, paper records are maintained in locked file cabinets under the control of authorized personnel. Computerized records systems follow the National Institute of Standards and Technology standards as developed to comply with the Privacy Act of 1974, 5 U.S.C. 552a; Paperwork Reduction Act of 1995, 44 U.S.C. 3501-3521; Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551-3558; and the Federal Information Processing Standards 199: Standards for Security Categorization of Federal Information and Information Systems. Computer servers in which electronic records are stored are located in secured contractor facilities with physical, technical and administrative levels of security to prevent unauthorized access to the network and information assets. Security controls include encryption, firewalls, audit logs, and network system security monitoring.

Access to records in the system is limited to authorized personnel who have a need to access the records in the performance of their official duties. Electronic data is protected through user identification such as usernames, passwords, database permissions and software controls. These security measures establish different access levels for different types of users. Each user's access is restricted to only the functions and data necessary to perform their job responsibilities.

System administrators and authorized users are trained and required to follow established internal security protocols, complete all security, privacy, and records management training, and sign the DOI Rules of Behavior. Contract employees with access to the system must also complete mandatory security and privacy training, sign DOI Rules of Behavior, and are monitored by their Contracting Officer Representative and the agency Security Manager.

RECORD ACCESS PROCEDURES:

DOI has exempted portions of this system from the access procedures of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). DOI will make access determinations on a case by case basis.

An individual requesting records on himself or herself should send a signed, written inquiry to the System Manager identified above. The request should describe the records sought as specifically as possible. The request envelope and letter should both be clearly marked "PRIVACY ACT REQUEST FOR ACCESS." A request for access must meet the requirements of 43 CFR 2.238.

CONTESTING RECORD PROCEDURES:

DOI has exempted portions of this system from the amendment procedures of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). DOI will make amendment determinations on a case by case basis.

An individual requesting corrections or the removal of material from his or her records should send a signed, written request to the System Manager identified above. A request for corrections or removal must meet the requirements of 43 CFR 2.246.

NOTIFICATION PROCEDURES:

DOI has exempted portions of this system from the notification procedures of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). DOI will make notification determinations on a case by case basis.

An individual requesting notification of the existence of records on himself or herself should send a signed, written inquiry to the System Manager identified above. The request envelope and letter should both be clearly marked "PRIVACY ACT INQUIRY." A request for notification must meet the requirements of 43 CFR 2.235.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

This system contains civil and administrative law enforcement investigatory

records that are exempt from certain provisions of the Privacy Act, 5 U.S.C. 552a(k)(2). Pursuant to 5 U.S.C. 552a(k)(2) of the Privacy Act, DOI has exempted portions of this system from the following subsections of the Privacy Act: (c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f). In accordance with 5 U.S.C. 553(b), (c) and (e), DOI promulgated a rule, which was published in the *Federal Register* at 85 FR 1282 (January 10, 2020), to amend the DOI Privacy Act regulations at 43 CFR 2.254 to claim exemptions for this system.

Additionally, the CMS may contain records from numerous sources compiled for investigatory purposes. To the extent that copies of records from other source systems of records are exempt from certain provisions of the Privacy Act, DOI claims the same exemptions for those records that are claimed for the original primary systems of records from which they originated.

The exemptions from one or more provisions of the Privacy Act may be waived on a case-by-case basis where a release would not interfere with or adversely affect investigations or enforcement activities.

HISTORY:

81 FR 67386 (September 30, 2016).

Teri Barnett,
Departmental Privacy Officer,
Department of the Interior.

[FR Doc. 2021-20094 Filed: 9/16/2021 8:45 am; Publication Date: 9/17/2021]