4310-VH-P

DEPARTMENT OF THE INTERIOR

Bureau of Safety and Environmental Enforcement

167E1700D2 EEAA010000 ET1EX0000.SZH000

Privacy Act of 1974, as amended; Notice of a New System of Records

AGENCY: Bureau of Safety and Environmental Enforcement, Interior.

ACTION: Notice of creation of a new system of records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, as amended, the Department of the Interior is issuing a public notice of its intent to create the Bureau of Safety and Environmental Enforcement, "Investigations Case Management System," system of records. The system will enable the Bureau of Safety and Environmental Enforcement to conduct and document incident investigations related to the Outer Continental Shelf and employee misconduct investigations. The Investigations Case Management System stores, tracks and analyzes reportable injuries, the loss or damage of property, possible violations of Federal laws and regulations, and investigation information related to operation of the Outer Continental Shelf to identify safety concerns or environmental risks. This newly established system will be included in the Bureau of Safety and Environmental Enforcement's inventory of record systems.

DATES: Comments must be received by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This new system will be effective [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Any person interested in commenting on this notice may do so by: submitting comments in to Teri Barnett, Departmental Privacy Officer, U.S. Department

of the Interior, 1849 C Street NW, Mail Stop 7456 MIB, Washington, DC 20240; hand-delivering comments to Teri Barnett, Departmental Privacy Officer, U.S. Department of the Interior, 1849 C Street NW, Mail Stop 7456 MIB, Washington, DC 20240; or e-mailing comments to *Privacy@ios.doi.gov*.

FOR FURTHER INFORMATION CONTACT: Rowena Dufford, Bureau of Safety and Environmental Enforcement Privacy Act Officer, 45600 Woodland Road, Mail Stop VAE-MSD, Sterling, VA, 20166; or email at *Rowena.Dufford@bsee.gov*.

SUPPLEMENTARY INFORMATION:

I. Background

The Department of the Interior (DOI), Bureau of Safety and Environmental Enforcement (BSEE), maintains the Investigations Case Management System (CMS) system of records. CMS is an incident investigation management and reporting application that will enable BSEE to conduct and document civil administrative investigations related to incidents, operations on the Outer Continental Shelf (OCS), and employee misconduct investigations. The CMS will store, track and analyze reportable injuries, the loss or damage of property, possible violations of Federal laws and regulations, and investigation information related to operations on the OCS to identify safety concerns or environmental risks.

The CMS is used to conduct civil administrative investigations and is not used for the conduct of criminal investigations. However, the CMS does support referrals of possible criminal activity to internal and external law enforcement organizations as appropriate for investigation. The CMS manages known or suspected civil violations; provides law enforcement agencies with appropriate referral information related to

possible criminal activities; captures, integrates, and shares incident related information and observations from other sources; analyzes and prioritizes protection efforts; provides information to justify funding requests and expenditures; assists in managing investigator training; tracks referrals and/or recommendations related to incident investigations; and manages and preserves evidence.

Incident and non-incident data related to activity occurring on the OCS will be 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 will also provide information for BSEE management to make informed decisions on recommendations for enforcement, civil penalties, and other administrative actions.

In a notice of proposed rulemaking, which is published separately in the Federal Register, DOI is proposing to exempt records maintained in this system from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2).

The system will be effective as proposed at the end of the comment period (the comment period will end 30 days after the publication of this notice in the Federal Register), unless comments are received which would require a contrary determination. DOI will publish a revised notice if changes are made, based upon a review of the comments received.

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' personal information. 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 for which information about an individual is retrieved by the name 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. As a matter of policy, DOI extends administrative Privacy Act protections to all individuals. 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, 43 CFR Part 2, Subpart K.

The Privacy Act requires each agency to publish in the Federal Register a description denoting the type and character of each system of records that the agency maintains and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses of their records, and to assist individuals to more easily find such records within the agency. Below is the description of the BSEE-01, Investigations Case Management System, system of records.

In accordance with 5 U.S.C. 552a(r), DOI has provided a report of this system of records to the Office of Management and Budget and to Congress.

III. Public Disclosure

Before including your address, phone number, e-mail address, or other personal

identifying information in your comment, you should be aware that your entire comment including your personal identifying information, may be made publicly available at any time. While you can ask us in your comment to withhold your personal identifying information from public review, we cannot guarantee that we will be able to do so.

Dated: September 27, 2016

Signed: _____
Teri Barnett
Departmental Privacy Officer

SYSTEM NAME:

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

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, 1849 C Street, NW, Washington, DC 20240. Records are also located at Bureau of Safety and Environmental Enforcement 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 website at http://www.bsee.gov.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals covered in the system include current and former Bureau of Safety and Environmental Enforcement (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 Outer Continental Shelf (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.

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.

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

The primary purpose of the CMS system of records is to conduct and document incident investigations and employee misconduct investigations related to operations on the Outer Continental Shelf. The CMS will be 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.

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:

(1) (a) To any of the following entities or individuals, when the circumstances set forth in paragraph (b) are met:

(i) The U.S. Department of Justice (DOJ);

(ii) A court or an adjudicative or other administrative body;

(iii) A party in litigation before a court or an adjudicative or other administrative body; or

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

(b) When:

(i) One of the following is a party to the proceeding or has an interest in the proceeding:

(A) DOI or any component of DOI;

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

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

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

(E) The United States, when DOJ determines that DOI is likely to be affected by

the proceeding; and

(ii) DOI deems the disclosure to be:

(A) Relevant and necessary to the proceeding; and

(B) Compatible with the purpose for which the records were compiled.

(2) To a congressional office in response to a written inquiry that an individual covered by the system, or the heir of such individual if the covered individual is deceased, has made to the office.

(3) 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.

(4) 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.

(5) 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.

(6) 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.

(7) 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.

(8) 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.

(9) To an expert, consultant, 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.

(10) To appropriate agencies, entities, and persons when:

(a) It is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; and

(b) DOI has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interest, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and

(c) The disclosure is made to such agencies, entities and persons who are reasonably necessary to assist in connection with the DOI's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

(11) 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.

(12) To the Department of the Treasury to recover debts owed to the United States.

(13) 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.

(14) 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.

(15) 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.

(16) 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:

(a) Individuals involved in such incidents;

(b) Persons injured in such incidents;

(c) 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.

(17) 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 STORING, RETRIEVING, ACCESSING, RETAINING AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Electronic records are stored and maintained in a password-protected cloud system that is compliant with the Federal Information Security Modernization Act of 2014. 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 for submission into the CMS may be temporarily stored or accessed on DOI network computers, email systems, and approved removable hard drives.

RETRIEVABILITY:

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.

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. Cloud hosting will only be provided by approved DOI cloud vendors. A privacy impact assessment was conducted to ensure appropriate controls and safeguards are in place to protect the information within the system.

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.

RETENTION AND DISPOSAL:

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 fifteen years after cut-off, and hardcopy reports are transferred to NARA twenty-five 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 twenty-five 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 ten 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 384 Departmental Manual 1 and NARA guidelines.

SYSTEM MANAGER AND ADDRESS:

CMS System Administrator, Bureau of Safety and Environmental Enforcement, National Investigations Program, 1849 C Street, NW, Mail Stop 5438 MIB, Washington, DC 20240.

NOTIFICATION PROCEDURES:

DOI is proposing to exempt portions of this system from the notification procedures of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). An individual requesting notification of the existence of records on himself or herself should send a signed, written inquiry to the System Manager previously identified. 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.

RECORDS ACCESS PROCEDURES:

DOI is proposing to exempt portions of this system from the access procedures of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). An individual requesting records on himself or herself should send a signed, written inquiry to the System Manager previously identified. 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 RECORDS PROCEDURES:

DOI is proposing to exempt portions of this system from the amendment procedures of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). An individual requesting corrections or the removal of material from his or her records should send a signed, written request to the System Manager previously identified. A request for corrections or removal must meet the requirements of 43 CFR 2.246.

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; and complainants, informants, suspects, victims, and witnesses.

EXEMPTIONS CLAIMED 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 has promulgated a rule, which was published separately in today's Federal Register.

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.

[FR Doc. 2016-23706 Filed: 9/29/2016 8:45 am; Publication Date: 9/30/2016]