Adapted Privacy Impact Assessment

Waterfront Mobile Application

April 7, 2023

Contact

Bureau of Ocean Energy Management
Associate Privacy Officer
1849 C Street NW
Washington, DC 20240
571-474-7967
boemprivacy@boem.gov

SECTION 1: Specific Purpose of the Agency's Use of the Third-Party Website or Application

1.1 What is the specific purpose of the agency's use of the third-party website or application and how does that use fit with the agency's broader mission?

The mission of the Bureau of Ocean Energy Management (BOEM) is to manage the development of U.S. Outer Continental Shelf (OCS) energy and mineral resources in an environmentally and economically responsible way. The bureau tries to be as transparent as possible to make sure that the public is informed of its actions in pursuit of responsible development of the nation's ocean energy and mineral assets by:

- Sending announcements on BOEM programs to the public and media.
- Publishing important regulatory actions and environmental analyses for public comment.
- Holding meetings with the public, industry, non-governmental organizations, scientists, and others to learn from them and share information about bureau programs.
- Keeping BOEM's website updated.

BOEM often uses social media and other third-party tools as a supplemental way to disseminate information to the public and stakeholder groups. Waterfront is a cloud-based, geospatial mobile application platform developed by Ithaca Clean Energy, LTD that enables marine stakeholders to share information with each other. Waterfront users can share their vessel and gear information, record ecological observations, exchange direct chats with other users, view and apply for posted job opportunities, participate in polls, comment on posts, and view shared events and information (e.g., locations of hazards and survey ships, buoys, and any other marine infrastructure that may be temporarily or permanently set in place) based on their geolocation and/or specific selected geographical area(s) of interest. Participating BOEM programs and offices and offshore wind project developers pay for licenses to use a Web-based dashboard to efficiently manage their dissemination of information to other Waterfront users.

BOEM's use of Waterfront will enhance the bureau's delivery of information to marine stakeholders, facilitate feedback on bureau notices and rulemakings, and increase government transparency. The BOEM Office of Public Affairs is responsible for coordinating with participating BOEM programs and offices to ensure that information made available to Waterfront users through official BOEM accounts is appropriate and approved for public dissemination in accordance with the DOI Digital Media Policy.

1.2 Is the agency's use of the third-party website or application consistent with all applicable laws, regulations, and policies? What are the legal authorities that authorize the use of the third-party website or application?

Participating BOEM programs and offices are responsible for using Waterfront consistent with applicable laws, regulations, and policies, including those regarding

accessibility, privacy, records management, information quality, and intellectual property. They will identify specific legal authorities that cover any activities they promote on the mobile application platform in BOEM Privacy Notices, as appropriate.

Legal authorities that authorize typical BOEM use of Waterfront include the following: Paperwork Reduction Act (44 U.S.C. 3501); Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001 (Public Law 106-554); Office of Management and Budget (OMB) Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, an Integrity of Information Disseminated by Federal Agencies; Presidential Memorandum on Transparency and Open Government, January 21, 2009; OMB M-10-06, Open Government Directive, December 8, 2009; OMB Memorandum for the Heads of Executive Department Agencies, and Independent Regulatory Agencies on Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act, April 7, 2010; OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010; Presidential Memorandum on Building a 21st Century Digital Government, May 23, 2012; OMB Circular A-130, Managing Information as a Strategic Resource, July 28, 2016; OMB Memorandum M-17-06, Policies for Federal Agency Public Websites and Digital Services, November 8, 2016; and 470 DM 2.

SECTION 2: Any PII that is Likely to Become Available to the Agency Through the Use of the Third-Party Website or Application

2.1 What PII will be made available to the agency?

Waterfront requires individuals to register to access the mobile application's features. To create a free Waterfront account, individuals must provide their full name, email address, and the password they will use to log into the mobile application. Users can add more information to their profile at their discretion (i.e., occupation, profile photo, phone number, vessel information, and gear information).

BOEM Waterfront users can view any information that Waterfront users have voluntarily shared with the Waterfront user community. By default, a user's chat availability, vessel information, and gear information are not visible to any other Waterfront users. Users can edit their Settings to enable or restrict access to their information at any time.

Waterfront users may provide information directly to BOEM while using the mobile application. The username and other shared profile information of individuals who have commented on a BOEM post or have sent a direct chat to BOEM will be viewable by authorized BOEM official Waterfront account managers.

Waterfront users may also voluntarily provide information (e.g., their email address, name, phone number, and other shared information) to BOEM through official BOEM email addresses, pages, or websites that the bureau has shared on the mobile application platform. Participating BOEM programs and offices will collect the minimum PII necessary to facilitate the collection's purpose and provide a Privacy Notice for review at each collection point.

2.2 What are the sources of the PII?

Sources of the PII are Waterfront users world-wide, which may include members of the general public, mariners, commercial fishers, Federal employees and contractors, offshore wind farm company representatives, and non-governmental organization personnel.

2.3 Will the PII be collected and maintained by the agency?

BOEM programs and offices using Waterfront must coordinate with the BOEM Records Officer to determine the record status of content on Waterfront to ensure compliance with Federal and Departmental records management policy.

According to the U.S. National Archives and Records Administration (NARA),[1] social media content is likely to be a Federal record if the answer to any of the following questions is "yes":

- Does it contain evidence of an agency's policies, business, or mission?
- Is the information only available on the social media site?
- Does the agency use the tool to convey official agency information?
- Is there a business need for the information?

Electronic messages (i.e., electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals) created or received in the course of agency business (whether on agency networks and devices or hosted by third-party providers) are also Federal records and must be scheduled for disposition.

BOEM will maintain PII that becomes available to the bureau while using the mobile application or through interactions outside of Waterfront if the interactions create Federal records. Waterfront users may provide PII to the bureau through direct chats to official BOEM accounts or comments on official BOEM posts. Waterfront users may also voluntarily provide PII information to BOEM through official BOEM email addresses, pages, or websites that the bureau has shared on the mobile application platform.

When user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of Departmental or bureau policy, BOEM may maintain information about the user interaction (including, but not limited to, username, name, profile photo, contents of postings, and any other available personal information) to notify the appropriate agency officials or law enforcement organizations as required by law.

[1] NARA (2013) *Guidance on Managing Social Media Records*, *NARA Bulletins*. NARA. Available at: https://www.archives.gov/records-mgmt/bulletins/2014/2014-02.html (Accessed: March 27, 2023).

Any BOEM programs or offices proposing to use Waterfront in a way beyond those described in this Adapted PIA must coordinate with the BOEM APO and other bureau officials to assess compliance with applicable Federal laws, regulations, and policies before proceeding.

2.4 Do the agency's activities trigger the Paperwork Reduction Act (PRA) and, if so, how will the agency comply with the statute?

When sponsoring an information collection online, or in any other form or format, agencies must comply with the PRA's requirement to maximize the utility of information collected, maintained, used, shared, and disseminated while minimizing the burden imposed on the public. Typical BOEM use of Waterfront will not invoke the PRA. Any planned use of Waterfront that will invoke the PRA will require a complete PIA exclusive to the use of the mobile application for that purpose and coordination with the BOEM Information Collection Clearance Officer.

BOEM will not direct Waterfront users to official BOEM pages or websites to provide information to the bureau for any purpose that invokes the PRA without coordinating with the BOEM APO and the BOEM Information Collection Clearance Officer to determine PIA and other requirements for the information collection.

SECTION 3: The Agency's Intended or Expected Use of the PII

3.1 Generally, how will the agency use the PII described in Section 2.0?

BOEM's official presence on Waterfront is to enhance the bureau's delivery of information to marine stakeholders, facilitate feedback on bureau notices and rulemaking, and increase government transparency. Waterfront users may provide information directly to BOEM while using Waterfront or through interactions outside of the mobile application. If applicable, BOEM will use this information to respond to a comment or question or fulfill a user's request. See the specific examples listed in Section 3.2 below.

Also, there may be unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or a violation of Departmental or bureau policy. In these cases, BOEM may use information about the user interaction to notify the appropriate agency officials or law enforcement organizations as required by law.

3.2 Provide specific examples of the types of uses to which PII may be subject.

Waterfront users can comment on BOEM posts, send direct chats to official BOEM accounts, and may voluntarily provide information (e.g., their email address, name, phone number, and other shared information) to BOEM through official BOEM email addresses, pages, or websites that the bureau has shared on the mobile application platform.

Examples of how BOEM may use the PII:

- If a user has asked a question via a comment, direct chat, or email, BOEM will use the minimum information required to respond with the requested information.

- If a user provides information on an official BOEM page or website to sign up to receive electronic subscriptions to bureau notifications or publications, BOEM will use the minimum information required to provide the requested subscription services.

- If a user provides information on an official BOEM page or website to participate in a meeting sponsored by the bureau, BOEM will use the minimum information required to deliver meeting updates and access credentials (if applicable).

- If a user provides information via Regulations.gov (or an alternative way) to officially comment on a published BOEM notice, the bureau will retain submitted comments and PII as a matter of public record as disclosed in the published public comment notice.

- When user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or a violation of Departmental or bureau policy, BOEM may use information about the user interaction (including, but not limited to, username, name, profile photo, contents of postings, and any other available personal information) to notify the appropriate agency officials or law enforcement organizations as required by law.

SECTION 4: Sharing or Disclosure of PII

4.1 With what entities or persons inside or outside the agency will the PII be shared, and for what purpose will the PII be disclosed?

Waterfront is a third-party mobile application. BOEM is not responsible for how Waterfront may access or use the information posted on the mobile application platform. All Waterfront users have an opportunity to review the Waterfront Privacy Policy before they provide their information to create a user account. The Waterfront Privacy Policy outlines what PII and non-personal data the service collects from users and how it uses the information. The Waterfront Privacy Policy details the limited circumstances in which the service will share information with third parties to perform assigned tasks on its behalf and advises users to review the privacy policy of third-party websites and services linked within the mobile application to understand their privacy practices.

Participating BOEM programs and offices do not actively collect PII from Waterfront users through the mobile application. If a Waterfront user interacts with BOEM on the platform, BOEM may internally use the information that becomes available to the bureau for the purpose of communicating and interacting with the user to provide information or requested services. If a Waterfront user provides BOEM with information outside of the mobile application for an authorized purpose, BOEM must provide a Privacy Notice at the point of collection to disclose the bureau's authorization to collect the information, the purpose of the collection, and any sharing of the information (if applicable).

There may be unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of Departmental or bureau policy. BOEM may maintain and use information about the user interaction to notify the appropriate agency officials or law enforcement organizations.

4.2 What safeguards will be in place to prevent uses beyond those authorized under law and described in this PIA?

It is DOI policy that bureaus and offices access and use social media tools in a responsible manner. Official use of social media to communicate and engage with the public must be in accordance with all applicable Federal laws, regulations, and policies, including those regarding accessibility, privacy, records management, information quality, and intellectual property.

In accordance with the DOI Digital Media Policy, official social media accounts must have a primary point of contact who is responsible for managing account security, overseeing employee access and training, and distributing guidance. The contact must be a full-time, permanent federal employee. Before gaining access to an official social media account, employees must complete mandatory social media training and sign DOI's social media user agreement. BOEM employees are also required to complete annual mandatory security, privacy, and records management training to ensure an understanding of their responsibility to protect individual privacy and appropriately manage bureau records.

Only approved BOEM personnel will have access to manage official BOEM Waterfront accounts and create official postings to share bureau information that has been reviewed and approved for dissemination. Except for official BOEM postings, the bureau does not control the content available on the Waterfront mobile application platform. Ithaca Clean Energy, LTD is responsible for protecting its users' privacy and the security of user data within the mobile application. Waterfront users are subject to the application owner's Privacy Policy and Terms and Conditions and must use their own discretion with respect to the personal information they provide to Waterfront or make available to the user community.

SECTION 5: Maintenance and Retention of PII

5.1 How will the agency maintain the PII, and for how long?

The Federal Records Act (44 U.S.C. 3301) defines Federal records as any material that is recorded, made, or received in the course of Federal business, regardless of its form or characteristics and is appropriate for preservation. Social media content that meets this definition must be managed according to the applicable laws and regulations. The statute and its implementing regulations place responsibility with each agency to determine what Federal records they create or receive.

In accordance with the DOI Digital Media Policy, BOEM does not use third-party websites and applications as the sole venue for disseminating information related to official bureau functions. Posts that participating BOEM programs and offices publish on the Waterfront mobile application platform represent official announcements that the

bureau provides in other publicly available formats. In most cases, BOEM will maintain these records in accordance with Departmental Records Schedule (DRS) 3 – Policy DAA-0048-2013-0008-0008, Public Affairs Records, which applies to records of all DOI activities devoted to the exchange of information between DOI and its stakeholders in support of the DOI mission. These records have a Permanent disposition and are cut off at the end of the fiscal year in which the event occurred or the publication was produced. BOEM will transfer these records to NARA 15 years after cutoff.

BOEM will maintain PII that becomes available to the bureau while using the mobile application or through interactions outside of Waterfront if the interactions create Federal records. Electronic messages created or received in the course of agency business are Federal records. Some types of electronic messages, such as email messages, are more likely to contain substantive information and thus are likely to require retention for several years, or even permanently. Current business practices make it more likely other types of electronic messages, such as chat and text messages, contain transitory information or information of value for a much shorter period. General information requests sent to BOEM electronically are covered under DRS 1 – Administrative DAA-0048-2013-0001-0003, Administration Records of Specific Temporary Value. These records have a temporary disposition, are cut off when 90 days old, and are destroyed when no longer needed.

When records provide information that may be used in the conduct of an investigation and are copied and/or forwarded on for potential use by an investigator, the original owner of the record must acknowledge that these may be used for evidentiary purposes that require further preservation. Records disposition (whether destruction or retirement) can be suspended in the case of active litigation or investigation, but only with active communication from the investigating office (or the solicitor). Otherwise, records will be maintained for the time indicated in the approved records schedule and disposed of accordingly.

In cases in which users have provided PII to BOEM outside of the mobile application while submitting an official public comment, retention periods may vary depending on the program, notice, or purpose of the rulemaking or publication. Records of public comments are retained and disposed of in accordance with applicable DOI records schedules that have been approved by NARA based on the subject or function and records series. Most public comments related to Federal Register notices fall under the DOI DRS. Records related to Federal Register notices are covered by DRS 1 – Administrative DAA-0048-2013-0001-0001, Short-term Administration Records, which have a temporary disposition and are destroyed 3 years after cut-off. Records related to rulemaking are covered by DRS 3, Policy DAA-0048-2013-0008-0010, Final Regulations, which have a Permanent disposition and are transferred to NARA 15 years after cut-off.

BOEM programs and offices must coordinate with the BOEM Records Officer to ensure that appropriate records schedules are in place to cover the records they may create while using Waterfront. In accordance with NARA Guidelines and Departmental policy, approved disposition methods include shredding or pulping for paper records and degaussing or erasing for electronic records. Prior to the disposition (destruction or transfer) of any record, employees must verify and validate the status of the record as it relates to standing records freezes and litigation holds.

5.2 Was the retention period established to minimize privacy risk?

BOEM programs and offices routinely minimize privacy risk by limiting their collection of PII to what is necessary to facilitate and manage official bureau activities. It is the policy of DOI that social media tools be accessed and used in accordance with all applicable Federal laws, regulations, and policies, including those regarding records management. In cases where PII is part of records that support bureau business, BOEM will retain the records in accordance with the applicable NARA-approved schedule(s). BOEM programs and offices will retain PII that is not part of a Federal record subject to NARA retention requirements as needed, then promptly destroy it in accordance with approved destruction methods to minimize privacy risk.

SECTION 6: How the Agency will Secure PII

6.1 Will privacy and security officials coordinate to develop methods of securing PII?

Security officials and the BOEM APO must coordinate to identify and mitigate the risks posed by any third-party service that a BOEM program or office has proposed for use. Following review of a completed PTA for Waterfront, the BOEM APO recommended a security compliance review and determined that an Adapted PIA would be required to assess the distinct privacy risks generated by the bureau's use of the mobile application and provide public notice.

Annual privacy and security training courses ensure employees and other users of DOI information assets have access to new and emerging best practices in protecting DOI information systems and data. Without this awareness, the Department faces an increased risk of its ability to accomplish mission objectives. All employees and other users with access to Federal information or information systems must complete annual Information Management and Technology (IMT) Awareness Training. Individuals with significant privacy and security responsibilities must also complete role-based training. These training practices help ensure that individuals take appropriate actions when using DOI systems and networks. Security officials and the BOEM APO will coordinate with the BSEE/BOEM DOI Talent Data Steward to assign training and monitor completion to ensure that BOEM employees understand their security and privacy responsibilities.

6.2 How will the agency secure PII? Describe how the agency will limit access to PII, and what security controls are in place to protect the PII.

The DOI website Privacy Policy instructs individuals to review the privacy policy and terms of service of third-party service providers before using them to understand how and when they collect, use, or share users' personal information. The Waterfront Privacy Policy specifies what PII and non-personal data the service collects from users and how it uses the information.

Participating BOEM programs and offices do not actively use Waterfront to collect PII from users. In limited cases, BOEM may maintain PII that becomes available to the bureau through its use of Waterfront. In these cases, BOEM will employ the appropriate technical, physical, and administrative controls to secure the PII.

Only authorized BOEM employees can use the licensed BOEM Waterfront accounts. All BOEM employees must review the DOI Digital Media Policy, complete social media training, and sign the user agreement before getting access to an official social media account. The primary contact for a social media account is responsible for making sure that employees complete these requirements and must also remove account access for employees who no longer need it within 24 hours.

BOEM Waterfront users must protect their user credentials and avoid the storage of records in locations accessible to individuals who do not have an official need-to-know. Access to the DOI network is restricted to authorized users with multi-factor authentication controls, servers are located in secured facilities behind restrictive firewalls, and access to databases and files is controlled by the system administrator and restricted to authorized personnel based on an official need-to-know. Other security controls include continuously monitoring threats and rapid response to incidents. All DOI employees are required to complete annual IMT Training and sign the Information Systems Security Rules of Behavior Acknowledgment. BOEM employees must report any suspected or confirmed privacy breach immediately to their supervisor and local IT help desk, the BOEM APO, or the DOI Computer Incident Response Center (CIRC).

There may be unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or a violation of Departmental or bureau policy. In these cases, BOEM may use information about the user interaction to notify the appropriate agency officials or law enforcement organizations as required by law. BOEM will secure such information in accordance with the applicable DOI privacy and security policies.

SECTION 7: Identification and Mitigation of Other Privacy Risks

7.1 What other privacy risks exist, and how will the agency mitigate those risks?

Waterfront receives personal data about users directly from them during the account creation process and when users add information to their profile. Shared PII could be used by unintended persons to commit fraud or identity theft, target users with unsolicited or fraudulent communications, or for other harmful or unlawful purposes. Waterfront users can mitigate privacy risk by controlling the viewability of their PII via their profile settings and through discretion with respect to the personal information they provide in uploaded documents, posts, comments, or direct communications with other Waterfront users.

There are also privacy risks associated with the use of location information within the mobile application. Waterfront provides "just-in-time" disclosures and obtains users' affirmative express consent before accessing sensitive location services on the mobile device for the first time. Waterfront also provides independent opt-out features so that users may customize the mobile application's features (e.g., opting out of location-based services and sharing gear pins anonymously) while still choosing to use other application services, where appropriate. Waterfront does not share the identification and location of a user’s mobile device with BOEM.

Waterfront is a third-party mobile application. Waterfront users are subject to Waterfront's Privacy Policy and Terms and Conditions. The Waterfront Privacy Policy explains what information the service collects, how it uses the information, and the limited circumstances in which it may share the information. BOEM examines the privacy policy and practices of third-party websites and applications to evaluate the risks and determine whether the site or service is appropriate for BOEM's use. The BOEM APO will monitor any changes to Waterfront's Privacy Policy and update this Adapted PIA, as necessary. Waterfront users are responsible for evaluating Waterfront Privacy Policy changes and determining for themselves whether the changes introduce any risks they are not willing to accept.

All Waterfront users must guard their account against compromise by protecting their account information, regularly updating their password, and taking appropriate action if their account is compromised. Although both BOEM and Waterfront employ physical, technical, and administrative controls to help prevent security breaches, neither can guarantee that a breach will never occur. In the event of a breach on the platform, Waterfront will take reasonable steps to investigate the situation and, where appropriate, notify affected individuals in accordance with any applicable laws and regulations.

Neither BOEM nor Waterfront are responsible for the contents of any linked site that they do not manage. The Waterfront Privacy Policy reminds users that the service does not accept any responsibility or liability for the privacy and security policies of third-party websites or services linked to or from the mobile application. Users must exercise caution before proceeding to any third-party service or entering into any transaction with third parties. Users must also be cautiously aware of the information they share with integrated applications and should take care to avoid disclosing sensitive PII, which could be used by unintended persons to commit fraud or identity theft, or for other harmful or unlawful purposes. BOEM posts reviewed and approved official information for public dissemination on the Waterfront mobile application so any privacy risk of unauthorized disclosure of personal data by the bureau is mitigated. If BOEM posts an external link that leads to a third-party website or any other location that is not part of an official government domain, BOEM will provide notice explaining that visitors are being directed to a non-government website that may have different privacy policies (and risks) from those of BOEM's official pages or website.

Users who have any questions about Waterfront's privacy practices may contact the service directly. Waterfront users can also choose to delete their account at any time and visit official BOEM websites and pages to access publicly available bureau information. Waterfront users who have provided PII to third-party services and websites linked within the mobile application must contact those third parties to withdraw consent in accordance with the respective Privacy Policy of the third parties.

There is a risk that third-party accounts or content may misrepresent agency authority or affiliation. Certain third-party accounts, social media websites, or content may not be officially authorized by, or affiliated with BOEM, even where they appear to represent BOEM or the U.S. Federal Government. Interacting with such unauthorized accounts may expose users to the privacy or security risks described above. Participating BOEM programs and offices will make every reasonable effort to label or identify their official user accounts in ways that would help users distinguish them from any unauthorized accounts or pages.

Minimizing the collection and retention of PII is a basic privacy principle. Participating BOEM programs and offices using Waterfront do not actively collect the PII of users on the mobile application platform and will direct users to official bureau pages and websites if they are requesting PII from individuals. There is a risk that BOEM programs and offices may not conduct a PTA to assess a proposed collection's privacy risks. As a consequence, BOEM may collect more information than necessary to fulfill a mission-related purpose, may lack a legal authority to collect the information, or may fail to provide an adequate privacy notice to individuals at the point of collection. Annual mandatory privacy training and supplemental privacy awareness campaigns will help BOEM employees understand their privacy responsibilities to ensure that privacy risks are identified and mitigated before engaging the public.

7.2 Does the agency provide appropriate notice to individuals informing them of privacy risks associated with the use of the third-party website or application?

All Waterfront users have an opportunity to review the Waterfront Privacy Policy and Terms and Conditions and must acknowledge that they accept them prior to creating a user account. The Waterfront Privacy Policy specifies what PII and non-personal data the service collects from its users and how it uses, processes, and stores the information. If Waterfront makes minor changes to its Privacy Policy, the service will post the modified Privacy Policy on its website. Waterfront will notify users of any modifications that will materially change their rights via an email and/or a prominent notice posted on the owner's website.

This Adapted PIA provides notice to the public on the bureau's use of Waterfront. Participating BOEM programs and offices will also ensure, to the extent feasible, that they display appropriate branding and provide notice to individuals on the privacy implications of their use of Waterfront within the mobile application by:

- Reminding users that Waterfront is a non-government third-party application and BOEM has no control over any external service's access restrictions or privacy procedures;
- Informing users on how they will handle PII that becomes available to them through user interaction on the mobile application platform; and
- Directing users to the DOI website Privacy Policy for additional information on DOI bureau and office use of third-party websites and applications.

In accordance with the DOI Digital Media Policy, DOI bureaus and offices should also include a disclaimer when posting content on third-party websites that explains that DOI bureaus and offices are only responsible for quality of the information they post using their official accounts and not for the quality of the information posted by other users.

SECTION 8: Creation or Modification of a System of Records

8.1 Will the agency's activities create or modify a "system of records" under the Privacy Act of 1974?

Typical BOEM use of Waterfront will not create or modify a Privacy Act system of records, as participating BOEM programs and offices do not actively use the service to solicit PII from other mobile application users. However, records created through interactions with Waterfront users may create a system of records. In rare cases, BOEM may use the information provided by a Waterfront user and/or the contents of posts or direct chats to notify the appropriate agency officials or law enforcement organizations of the evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of Departmental or bureau policy. The bureau's maintenance of this information may create a system of records. Also, BOEM activities publicized on Waterfront but not conducted through the mobile application may create a system of records.

BOEM programs and offices that will create a system of records through their use of Waterfront or activities promoted through use of the mobile application must a) coordinate with the BOEM APO to identify the applicable SORN or the need to publish a new one and b) provide an appropriate notice to individuals and maintain the records in accordance with the applicable SORN. The BOEM APO will also update this Adapted PIA as required to provide notice.

8.2 Provide the name and identifier for the Privacy Act system of records.

INTERIOR/DOI-08, DOI Social Networks - 76 FR 44033 (July 22, 2011); modification Published 86 FR 50156 (September 7, 2021) covers the following types of records:

- Records created through interactions with Waterfront users (either within the mobile application or beyond Waterfront).
- Records created when Waterfront users provide BOEM with their information through official BOEM email addresses, pages, or websites to receive information regarding an upcoming event, notification of an emergency or breaking news, or provide feedback about a program.
- Records about user interactions that indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of Departmental or bureau policy to notify the appropriate agency officials or law enforcement organizations.

The eRulemaking Program helps DOI manage a central, electronic repository for all DOI rulemaking materials and dockets, which include the rulemaking itself, Federal Register notices, supporting materials such as scientific or economic analyses, and public comments. The electronic repository also includes non-rulemaking dockets. DOI uses Regulations.gov to accept public comments electronically and the Federal Document Management System for comment analysis. Each DOI bureau and office manages its own docket and can only access the comments or supporting materials submitted on its own rulemakings. BOEM may use Waterfront to publicize requests for public comment

and will direct individuals to Regulations.gov to submit comments on regulatory documents published in the Federal Register. INTERIOR/DOI-21, eRulemaking Program - 85 FR 33701 (June 2, 2020) covers the personal information provided by any individuals (including public citizens and representatives of Federal, state, Tribal, or local governments; businesses; and industries) while submitting a comment or supporting materials on a Federal agency rulemaking.

BOEM may use Waterfront to publicize official bureau events that require the bureau to collect and maintain information from visitors, guests, and other individuals to facilitate their access to DOI facilities while ensuring the safety and security of DOI facilities and their occupants. INTERIOR/DOI-46, Physical Security Access Files - 85 FR 3406 (January 21, 2020) Final Rule for Privacy Act Exemptions - 86 FR 49927 (September 7, 2021) covers the bureau's collection of this information.