# Adapted Privacy Impact Assessment

# Constant Contact

**7/14/2021**

## Contact

Bureau of Ocean Energy Management
Associate Privacy Officer
1849 C Street, NW
Washington, DC 20240
202-208-7160
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 development of U.S. Outer Continental Shelf energy and mineral resources in an environmentally and economically responsible way. BOEM programs and offices often use approved third-party tools to disseminate mission-related information to stakeholders. One of these tools is Constant Contact, a Web-based email marketing service that BOEM can use to facilitate and manage subscription services. Individuals interested in receiving email messages from BOEM can subscribe to receive messages based on their interests and needs and may unsubscribe at any time.

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?

BOEM programs and offices are responsible for using Constant Contact in accordance with applicable laws, regulations, and policies and will identify specific legal authorities that cover their activities in Privacy Notices, as appropriate. Legal authorities that authorize typical BOEM use of Constant Contact include the following: Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.); Presidential Memorandum, Building a 21st Century Digital Government, May 23, 2012; Presidential Memorandum on Transparency and Open Government, January 21, 2009; OMB M-10-06, Open Government Directive, December 8, 2009; OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010; OMB Memorandum on Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act, April 7, 2010; OMB Circular A-130, Managing Information as a Strategic Resource, July 28, 2016; and 110 Departmental Manual 5, Office of Communications.

## 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?

Limited PII will become available to authorized BOEM users of Constant Contact. BOEM Constant Contact users will not have access to any of the data that Constant Contact collects to manage its services and business beyond what the user's program or office collects directly from individuals to facilitate and manage their use of the service.

Authorized BOEM Constant Contact users are responsible for creating subscription signup pages for their BOEM program or office and specifying what information individuals must provide to complete the subscription process. BOEM will require subscribers to provide an email address (personal or business-related). In limited cases, individuals may also voluntarily provide additional information (e.g., their name and organization). Only authorized BOEM Constant Contact users will have access to subscriber lists for their respective BOEM program or office. Primary BOEM Constant

Contact users designated as Account Owners have full access to Constant Contact and complete ownership of the subscriber lists they manage on behalf of a BOEM program or office. Secondary BOEM Constant Contact users (designated as Account Managers by Account Owners) can create and send communications on behalf of a BOEM program or office, as well as manage the subscriber lists owned by the respective primary user. BOEM Constant Contact users designated as Campaign Creators by Account Owners cannot access or modify subscriber lists.

2.2 What are the sources of the PII?

BOEM programs and offices that use Constant Contact to send email messages to subscribers collect information directly from individuals who voluntarily sign up to receive email messages on topics of interest. Subscribers may be employees or contractors of BOEM or other DOI bureaus and offices, members of the public, industry representatives, non-governmental organization representatives, members of research or educational institutions, or federal, state, local, or tribal officials.

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

BOEM programs and offices providing subscription services through Constant Contact collect limited PII and will maintain subscriber data on the Constant Contact platform as long as necessary to facilitate and manage subscription services. Subscribers may unsubscribe and thereby remove their information from the platform at any time.

Individuals may also contact BOEM through the contact information that BOEM programs and offices have posted on their Web or subscription pages. In these cases, an individual's name, email address, and any other information they voluntarily provide in their message will become available to BOEM. BOEM will use this information to address their questions, provide a service, or fulfill a request, if applicable. Email messages that meet the definition of records in the Federal Records Act (44 U.S.C. § 3101) are covered under the same disposition schedule as all other federal records. BOEM will preserve such emails and maintain them for varying periods of time if those emails meet the definition of federal records. BOEM programs and offices will delete emails that are not federal records when they no longer need them. The DOI website Privacy Policy instructs individuals not to send sensitive PII to DOI bureaus and offices via email.

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

Typical BOEM use of Constant Contact will not invoke the Paperwork Reduction Act (PRA). Any planned use of Constant Contact or subscription-related activities that will invoke the PRA will require a complete PIA exclusive to the Constant Contact use or subscription-related activity, as well as coordination with the BOEM Information Collection Clearance Officer.

## 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 programs and offices that use Constant Contact to disseminate information to subscribers are responsible for developing content for distribution and specifying what limited information subscribers must provide during the signup process. BOEM programs and offices will use the information only for the purposes stated in the subscription-specific BOEM Privacy Notice that bureau programs and offices will provide to subscribers at the point of collection.

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

The Constant Contact Privacy Notice specifies what PII and non-personal data the service collects from users and how Constant Contact uses the information to manage and improve its delivery of services. BOEM programs and offices using Constant Contact will collect PII directly from subscribers. Individuals interested in receiving email messages from BOEM on topics of interest can voluntarily submit their email address through a Constant Contact signup form on the BOEM website. BOEM programs and offices will use the information they collect from subscribers only for the purposes stated in subscription-specific BOEM Privacy Notices. Alternatively, individuals who wish to subscribe to receive emails from BOEM on specific topics can also submit their information to a BOEM program or office via phone, email, or in writing for the purpose of being added to a subscription list. In these cases, the accommodating BOEM program or office will make every effort to provide access to the appropriate BOEM Privacy Notice prior to manually adding the subscriber's information to the applicable subscriber list. Subscribers can leave a list at any time by clicking on the "Unsubscribe" link at the bottom of an email they have received from BOEM through Constant Contact. Subscribers may also contact the BOEM program or office to request removal from a list or an update to their contact information.

If individuals contact BOEM via the contact information that the bureau has provided on a BOEM Web or subscription page, BOEM will use their information to address their questions, provide a service, or fulfill a request, if applicable. Email messages that meet the definition of records in the Federal Records Act (44 U.S.C. § 3101) are covered under the same disposition schedule as all other federal records. BOEM will preserve such emails and maintain them for varying periods of time if those emails meet the definition of federal records. BOEM programs and offices will delete emails that are not federal records when they no longer need them.

## 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?

The Constant Contact Privacy Notice outlines what PII and non-personal data the service collects from users and how it uses the information to manage and improve its delivery of services; provide users with requested information or technical support; facilitate users' movements through the Constant Contact "Sites" or their use of products and services; and to diagnose problems with Constant Contact servers or products and

services, in connection with Constant Contact security and compliance programs. Constant Contact may also occasionally enter into contracts with carefully selected third parties so that they can assist Constant Contact in providing customer service, fraud detection, or other services to users. Contracts with such third parties prohibit them from using any of users' personal information for any purpose beyond the purpose for which it was shared.

By completing a Constant Contact subscription signup form created by a BOEM program or office, individuals are granting Constant Contact permission to share their information with the respective BOEM program or office that initiated the collection. BOEM may share information with internal and external parties on a need-to-know basis for the purposes stated in subscription-specific BOEM Privacy Notices. If individuals contact BOEM via the contact information the bureau has provided on a BOEM Web or subscription page, BOEM will use their information to address their questions, provide a service, or fulfill a request, if applicable. In doing so, BOEM may share PII with other BOEM programs and offices, DOI bureaus and offices, or external stakeholders, as necessary and permissible by privacy policy.

To the extent that records BOEM creates while using Constant Contact are considered Privacy Act records, BOEM will maintain them consistent with the Privacy Act and will not disclose such records by any means of communication to any person or another agency unless disclosure is pursuant to the prior written request by, or with the prior written consent of, the individual to whom the record pertains, or if the disclosure is otherwise consistent with the Privacy Act.

There may be unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the U.S. Government, a threat to the public, or an employee violation of DOI policy. In such instances, BOEM may share information collected through its use of Constant Contact 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?

BOEM employees and contractors are required to complete security, privacy, and records management training to ensure they understand their responsibilities to protect individual privacy and appropriately manage information before they acquire access to the DOI network and information systems and annually thereafter. BOEM employees and contractors with significant privacy responsibilities are also required to complete role-based privacy training on an annual basis.

BOEM programs and offices planning to use Constant Contact must first review the BOEM Constant Contact Adapted PIA and consult with the BOEM Associate Privacy Officer (APO) to ensure that the planned use of Constant Contact will comply with applicable federal and DOI privacy policies. BOEM programs and offices using Constant Contact are responsible for the communications they issue. Official mission-related email messages that BOEM programs and offices send using Constant Contact must be reviewed and approved for distribution by appropriate officials to mitigate any risks posed by the unauthorized disclosure of personal or privileged data.

BOEM programs and offices will maintain subscription information on the Constant Contact platform as long as necessary to facilitate and manage subscription services. Only primary and secondary BOEM Constant Contact users will have access to data stored in the accounts they manage on behalf of their respective BOEM program or office. All BOEM officials who have access to the data stored in Constant Contact must use the information in accordance with the purposes expressed in the BOEM Privacy Notice and are not permitted to share subscriber information with individuals who do not have an official need-to-know. BOEM Constant Contact users must also safeguard their user credentials. If a subscription manager leaves or changes roles, the BOEM program or office must revoke the departing individual's account access to prevent unauthorized use of Constant Contact.

The Constant Contact Terms & Conditions (Terms) require users to provide subscribers with information regarding Constant Contact's use of subscriber data by either providing subscribers with access to the About Our Service Provider link or including substantially similar disclosure so that subscribers are aware of how their data is used by them and Constant Contact. The Terms also require users to adopt and comply with their own "customer privacy policy" to provide notice to subscribers of their data collection and use practices, including their practices with respect to data that they obtain from Constant Contact. BOEM programs and offices will provide all subscribers with access to the Constant Contact Privacy Notice and Security Statement, as well as upfront notice to individuals on the collection, use, maintenance, and disposition of PII that becomes available to the bureau while using Constant Contact. The Constant Contact Privacy Notice puts limitations on the types of PII that users may collect from individuals while using the service. All Constant Contact users must agree that they will not import or incorporate into any contact lists or other content they upload to Constant Contact servers any of the following information: Social Security numbers, national insurance numbers, credit cards, passwords, security credentials, or sensitive personal or health information of any kind.

The Constant Contact Email Permission Policy, incorporated into the service's Terms, requires all users' contact lists to be permission-based. Attending a bureau-sponsored event or providing comments on a *Federal Register* notice does not confer an individual's consent to receive communications from BOEM through Constant Contact services. For example, a BOEM program or office that hosts a public meeting cannot import the email addresses of attendees into Constant Contact for the purpose of adding them to a subscription list unless the attendees have affirmatively provided their consent. Individuals who feel that BOEM is sending them unsolicited email can report the issue to Constant Contact. Adding or importing contacts that go against the permission policy of Constant Contact's anti-spam policy may result in the termination of the account of the non-compliant BOEM program or office.

Constant Contact requires that every email BOEM sends through the service contain an "unsubscribe" link that allows subscribers to remove themselves from the mailing list. The unsubscribe link must remain operational for at least 60 days after the date on which the BOEM program or office sent the message. Primary and secondary BOEM Constant Contact users must process any unsubscribe requests they receive within 10 days of their receipt. Processing subscription update requests promptly ensures that BOEM programs and offices are not sending unsolicited messages. Individuals wishing to be re-added to a subscription list may complete the subscription signup process.

## SECTION 5: Maintenance and Retention of PII

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

BOEM programs and offices using Constant Contact will maintain subscriber information on the Constant Contact platform no longer than is useful for facilitating and managing subscription services. Individuals may unsubscribe at any time, after which point the BOEM program or office will no longer retain their information on the Constant Contact platform.

BOEM programs and offices must retain the records they create while using Constant Contact in accordance with DOI policy and records retention schedules approved by the National Archives and Records Administration (NARA). BOEM programs and offices must coordinate with the BOEM Records Officer to ensure that an appropriate records schedule is in place prior to using Constant Contact. BOEM programs and offices must also be mindful of any active litigation holds. Approved methods for the disposition of records include shredding, burning, tearing, and degaussing in accordance with NARA guidelines and 384 Departmental Manual 1.

5.2 Was the retention period established to minimize privacy risk?

BOEM programs and offices mitigate privacy risk by limiting their collection of PII to what is necessary to facilitate and manage subscription services and refraining from collecting sensitive PII. BOEM programs and offices using Constant Contact will retain data on the Constant Contact platform as long as they continue to use the service for approved purposes. Individuals may unsubscribe at any time to have their information removed from a list. 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?

Prior to using Constant Contact, BOEM programs and offices must coordinate with the BOEM APO to confirm that their proposed use of the service complies with federal and DOI privacy requirements. The BOEM APO will liaison with security officials, as necessary, to analyze acceptable risks, resolve potential issues, and develop methods of securing PII and other information that becomes available to BOEM programs and offices through their use of Constant Contact.

There are mandatory requirements for BOEM employees and contractors to complete security and privacy awareness training and sign the DOI Rules of Behavior form before they acquire access to the DOI network and information systems and annually thereafter. Some BOEM employees and contractors may be required to complete role-based security and privacy training. Privacy and security officials will coordinate with the Bureau DOI Talent Coordinator to ensure that employees and contractors have fulfilled their training obligations, as required.

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.

Constant Contact is an independently operated third-party service that controls access to user data stored within its system. BOEM encourages subscribers to review the Constant Contact Privacy Notice to understand how and when Constant Contact collects, uses, and shares their information. Constant Contact is responsible for protecting the security of user data stored on the Constant Contact platform. Constant Contact has implemented privacy and security controls to protect individual privacy and minimize privacy risks. The security of Constant Contact websites is managed on multiple levels, including Physical, Network, Host, Software, and User Account Security. Constant Contact maintains internal security policies and procedures in support of its ongoing operations. Access to resources is granted only to those who reasonably require access based on their responsibilities. Constant Contact will never use contact lists for any purpose other than those described in the service's Privacy Notice. BOEM programs and offices will collect only the information needed to facilitate and manage subscription services. By completing the subscription signup process, individuals are giving Constant Contact permission to share the requested information with BOEM Constant Contact users.

All BOEM employees must coordinate with their supervisor and other appropriate officials to ensure that physical, technical, and administrative safeguards are in place to protect the records in their custody. Primary and secondary BOEM Constant Contact users can help protect PII collected through Constant Contact by safeguarding their user credentials and avoiding the storage of records on shared networks or folders accessible to individuals who do not have an official need-to-know. BOEM primary and secondary users must create and manage their Constant Contact account using their official BOEM email address while using DOI-approved devices, not personal devices. All BOEM Constant Contact users must report any compromise of their accounts or related records to the appropriate Constant Contact and DOI officials in accordance with established procedures.

BOEM employees and contractors are responsible for safeguarding all information they remove from their official duty station and information they create at any alternative workplace in accordance with the Federal Records Act, Privacy Act, Freedom of Information Act, and other federal laws, regulations, and DOI policies. BOEM employees and contractors may share Constant Contact and subscription-related records only with authorized officials using approved sharing methods. If a BOEM Constant Contact user leaves or changes roles, the respective BOEM program or office must revoke the departing individual's account access.

Access to the DOI network is restricted to authorized users with password 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 the need-to-know principle. Other security controls include continuously monitoring threats, rapid response to incidents, and mandatory security and privacy training.

Constant Contact implements methods to secure data on multiple levels, including physical, network, host, software, and user account security. Constant Contact requires

that information is handled with appropriate levels of encryption in accordance with service policies and standards. Administrative access to Constant Contact's infrastructure is limited strictly to authorized users with multi-factor authentication. Constant Contact regularly undergoes security reviews, including external and internal scanning for vulnerabilities on an ongoing basis. All vulnerabilities discovered are reviewed by internal security and addressed in accordance with the level of severity. Constant Contact has a documented Cybersecurity Incident Response Plan, a 24×7 Command Monitoring Center, and an incident response third party on retainer. The Cybersecurity Incident Response Plan undergoes annual tabletop testing and is updated as necessary. Upon commencing employment, all Constant Contact employees receive information security training and are contractually obligated to confidentiality clauses to ensure that they adhere to Constant Contact's commitment to security and confidentiality. Constant Contact's information security awareness and training programs require employees to complete annual security refresher training. Where Constant Contact engages third parties to process customer data on its behalf, they do so in accordance with Constant Contact's written instructions under a duty of confidentiality and they are required to implement appropriate technical and administrative measures to ensure the data is secure.

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 DOI policy. In these cases, BOEM may share information collected through its use of Constant Contact to notify the appropriate agency officials or law enforcement organizations as required by law. BOEM will secure such information in accordance with 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?

BOEM follows established procedures to identify, evaluate, and address any new additional privacy requirements that may result from new statutes, regulations, and policies. BOEM will evaluate any new changes to Constant Contact and the Constant Contact Privacy Notice as necessary (and annually, at a minimum) to assess privacy risks and determine whether the bureau's continued use of the service is appropriate. Other privacy risks generated by BOEM's use of Constant Contact include those introduced through the collection or importation of unnecessary subscriber information, the use of PII beyond those expressed in the BOEM Privacy Notice, the unauthorized disclosure of personal data or proprietary information, the integration of third-party applications, and misrepresentation by other Constant Contact users.

All BOEM programs and offices using Constant Contact must limit their collection or importation of information to that which is necessary to facilitate and manage subscription services. Requiring individuals to provide more information than is necessary infringes upon the privacy rights of subscribers and serves no authorized purpose. BOEM programs and offices must provide subscribers with access to a Privacy Notice to inform individuals of how they handle information that becomes available to them through their use of Constant Contact. BOEM programs and offices must use collected information in accordance with the uses described in the BOEM Privacy Notice. Primary and secondary BOEM Constant Contact users are not permitted to

export subscription data to use for purposes other than those stated in the BOEM Privacy Notice. BOEM programs and offices using Constant Contact will consult with the BOEM APO to ensure that they are providing a proper Privacy Notice to subscribers. Any BOEM programs and offices that would like to expand their use of Constant Contact beyond those presented in this PIA must coordinate with the BOEM APO to complete a separate PIA for that specific use and collection of information.

There are risks posed by privacy breaches at the service and bureau levels. If Constant Contact learns of a security breach, it will notify affected BOEM users to enable them to take appropriate protective steps. To reduce the risk of bureau-level breaches, BOEM Constant Contact users must safeguard their user credentials, share collected information only with others who have an official need-to-know, and store records in repositories accessible only to others who have a legitimate business need to access the information. All BOEM employees receive training on the appropriate use and sharing of PII. BOEM officials authorized to use Constant Contact must review and approve proposed content prior to distribution to prevent the unauthorized disclosure of personal data or privileged information. If PII is confirmed or suspected to have become available to individuals who do not have an official need-to-know, BOEM employees and contractors are required to immediately report the compromise of PII to their supervisor and local IT help desk or the BOEM APO. Breaches may also be reported directly to the DOI Computer Incident Response Center (DOI-CIRC). Timely reporting and response enable the agency to take immediate steps in accordance with the DOI Privacy Breach Response Plan to mitigate any harm resulting from the compromise.

Beyond its official communications, BOEM has no control over access restrictions or procedures on the Constant Contact platform or the content distributed by other parties through the service. BOEM programs and offices using Constant Contact may distribute communications that contain links that direct subscribers to other third-party websites and services. Any sites or applications not developed and hosted by BOEM are governed by their own terms of use and privacy policies. Neither BOEM nor Constant Contact is responsible for the contents of any linked site or application. There is a risk that other entities that distribute content through Constant Contact 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 privacy or security risks. BOEM will make every reasonable effort to label or identify its official accounts and pages in ways that would help users distinguish it from any unauthorized accounts or pages. BOEM will also inform Constant Contact about any accounts purporting to represent BOEM, seek their removal, and warn users about such accounts.

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?

BOEM will ensure, to the extent feasible, that subscribers are aware that the bureau is sponsoring the subscription activity and will provide notice to individuals on the privacy implications of the bureau's use of Constant Contact through this Adapted PIA and access to a subscription-specific BOEM Privacy Notice as well as the Constant Contact Privacy Notice and Terms & Conditions. Individuals who do not complete the subscription signup process can access bureau content on the BOEM website.

The Privacy Notice that BOEM programs and offices will provide to respondents will include a link to the bureau's official website and the DOI website Privacy Policy, as well as explain:

- That Constant Contact is controlled and operated by a third-party and is not operated by the U.S. Government;
- That the DOI website Privacy Policy does not apply to Constant Contact;
- The purpose of the collection of information and how BOEM will use PII that becomes available to the bureau; and
- What SORN applies if a system of records is created.

The Constant Contact Privacy Notice specifies what PII and non-personal data the service collects from users and how it uses the information to manage and improve its services. DOI informs the public through its website Privacy Policy of the Department's use of pages on third-party websites and applications.

## 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?

Generally, BOEM's use of Constant Contact will not create or modify a system of records under the Privacy Act of 1974. BOEM programs and offices that will create a system of records through their use of Constant Contact must provide appropriate notice to individuals and maintain the records in accordance with the applicable SORN.

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

The DOI-08, DOI Social Networks SORN will apply in most cases in which BOEM programs and offices may create a system of records through their use of Constant Contact. BOEM Constant Contact activities not covered by the DOI-08, DOI Social Networks SORN may require the publication of a new or modified SORN to provide appropriate notice to the public.