United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: govDelivery	**System Owner:** Shirley Fan
Preparer: Shirley Fan	**Office:** Office of the Administrator (AO)
Date: 12/14/23	**Phone:** 202-280-8610
Reason for Submittal: New PIA__x__ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐ **Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).** **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**	

Provide a general description/overview and purpose of the system:

The govDelivery email marketing tool helps the Environmental Protection Agency's (EPA) public affairs offices ensure effective and efficient communications with its diverse internal and external audiences. This tool will allow EPA programs to connect with people using multiple outreach methods, including email, short messaging services (SMS)/text messages, really simple syndication (RSS) feeds. EPA will use the various outreach methods to message subscribers about various topics such as regulations, requirements for regulated facilities, grants, research on environmental issues, raising environmental awareness through education, new information available on the EPA website, and opportunities to engage with EPA. The tool will enable EPA to efficiently and effectively reach stakeholders; better understand its stakeholders and their information needs; and grow its subscriber base and track subscribe engagement over time.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

44 U.S.C. 3501, Paperwork Reduction Act of April 7, 2010; 5 U.S.C 301, Departmental Regulations;
The Presidents January 21, 2009 memorandum on Transparency and Open Government;
Presidential Memorandum on Building a 21st Century Digital Government, May 23, 2012;
OMB Memorandum M-10-06, Open Government Directive, December 8, 2009;
OMB Memorandum for the Heads of Executive Department Agencies, and Independent Regulatory Agencies, Social Media, Web-Based Interactive Technologies

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

A system security plan will be completed once an Authorization-to-Use (ATU) is issued.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

N/A

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

The data will be stored in a Cloud. The CSP is FedRAMP approved. It's a Software as Service (SaaS).

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

The system collects personal emails and phone numbers from members of the public and EPA employees.

2.2 What are the sources of the information and how is the information collected for the system?

For voluntary signups to govDelivery listservs, the PII that is collected via the signup is filled out by the subscriber and fed directly into govDelivery. In other words, the email addresses and phone numbers are collected from an online signup that EPA employees and members of the public fill out to get onto the govDelivery listserv. Additionally, Office of the Administrator (AO) employees will be able to send emails to all personnel with EPA

email addresses through a connection between Enterprise Identity Data Warehouse (eIDW), a system that contains attributes about individuals that have EPA email addresses and govDelivery. The emails and phone numbers of personnel with EPA email addresses is contained in the eIDW.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

For voluntary signups to govDelivery listservs, the PII that is stored within govDelivery is collected directly from the subscriber and fed directly into govDelivery. It's up to the subscriber to make sure his or her information is correct. For messages that are required to be sent to EPA personnel, contractors grantees, their email addresses are pulled from the eIDW.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

There is a low risk to the source or method of collection.

Mitigation:

PII is collected directly from individuals providing the information.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

govDelivery will have access control levels in place that only allows administrators with password protected accounts to access PII provided by subscribers. Any unauthorized access is able to be tracked and identified through administrator logs.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

The access controls are documented in the EPA Rules of Behavior for govDelivery Administrators, and the vendor's Information Security Manual and Information Security Policies.

3.3 Are there other components with assigned roles and responsibilities within the system?

Yes, a selected group of EPA public affairs staff outside and inside of the Office of Administrator has access to information within govDelivery. The selected group of EPA public affairs staff has a need to know.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

EPA contractors, subcontractors, and grantees are authorized to use govDelivery on behalf of EPA will have access to the data in the system. The contractors have the appropriate FAR clauses in their contract.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

The EPA Records Control Schedule for the govDelivery system is 1022. Subscriber information is deleted upon request of the subscriber and on termination of a govDelivery email marketing account (the email address is maintained for the minimum period of time required to support legal opt-out requirements). Generally speaking, the vendor follows National Institute of Standards and Technology (NIST) guidelines and US customer data protection requirements and meets all requirements associated with their International Organization for Standardization (ISO) 27001 and Federal Risk and Authorization Management Program **(**FedRAMP) authorizations. Data and records are cleansed from computer media through National Archives and Records Administration (NARA) approved procedures. Backups are destroyed in line with their retention policy (backups are retained for one year and then destroyed).

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

There is a risk that information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule.

Mitigation:

govDelivery maintains all records with PII in accordance with applicable records retention or disposition schedules approved by NARA or based on the need and relevancy of the data in the support of the Office of Ad mission. Some records are maintained as permanent records due to their continuing historical value; all other temporary records are disposed of in accordance with

approved records schedules.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

The vendor also shares personal data with agents and sub-processors (for purposes such as developing and improving network security), government authorities as permitted, necessary or required by law, and as part of a business transaction (e.g. the vendor changes ownership to a new organization).

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

Sharing information with third parties allows the vendor to perform the contract they have entered with their customers on whose behalf they provide these services.

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

Information is not shared outside of the agency. Agreements between the vendor and outside parties are required to address security rules and requirements for the exchange of information, procedures to ensure traceability and non-repudiation, technical requirements for information transmission, procedures for notifying both sender and recipient when a fault occurs, and responsibilities and roles in the event of an information security incident.

4.4 Does the agreement place limitations on re-dissemination?

The vendor's agents and sub-processors are required to use subscriber data in accordance with the vendor's privacy policy, which places limitations on re-dissemination. Likewise, EPA's govDelivery Rules of Behavior for Administrators places limitations on how EPA-managed accounts re-disseminate govDelivery information.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

N/A

Mitigation:

N/A

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

We have developed a Rules of Behavior document that EPA administrators will be required to follow to prevent the unauthorized use of data from govDelivery. Agreements between the vendor and outside parties who need to access EPA information are required to address security rules and requirements for the exchange of information, procedures to ensure traceability and non-repudiation, technical requirements for information transmission, procedures for notifying both sender and recipient when a fault occurs, and responsibilities and roles in the event of an information security incident.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

All EPA users are required to take annual information security and privacy awareness training. The vendor's specific authorized personnel, contractors, subcontractors, and agencies are required to take formal security training initially and annually.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Users of govDelivery may misuse and inappropriately disseminate information.

Mitigation:

EPA require auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. EPA employee assigned to maintain the EPA systems have job duties that require them to design, develop, and optimize the system within the security accreditation environment. Furthermore, each employee is required to undergo annual security awareness training that addresses his or her duties and responsibilities to protect the data.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

EPA uses govDeliver to help EPA public affairs' offices communicate with members of the public on information on grants, research on environmental issues, raising environmental awareness through education, new information available on the EPA website, and opportunities to engage with EPA.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes___ No__X_. If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.*)

The information is retrieved by topics to which users subscribed.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

This PIA assesses the potential effect of the privacy of individuals whose information is maintained in the govDelivery. A system of records notice is not required because information is retrieved by EPA topics to which users subscribed.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

There is minimal risk that the information stored by the system on behalf of EPA will be misused or improperly handled.

Mitigation:

govDelivery administrators, the vendors, and the vendor's agents and sub-processors must use multifactor authentication to access listserv subscriber information. EPA will require administrators of its instances of govDelivery to change their passwords quarterly. Only administrators, the vendor, and the vendor's agents and sub-processors who have a need to know are authorized to view the PII stored in the system.

***If no SORN is required, STOP HERE.**

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

Individuals can unsubscribe from the listserv at any time and their information will be removed consistent with what is written in Section 3.5.

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk: N/A

Mitigation: N / A

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk: N / A

Mitigation: N/A