Privacy Impact Assessment (PIA) Template

GOV DELIVERY
(Name of the Information System or Information Collection)

April 2024
Date

System/Collection Overview
GovDelivery is an existing web-based software system that is used to send emails to FHFA staff, stakeholders, and other external parties (i.e., media). The purpose of the system is to strengthen FHFA's internal communications through *Fresh Facts*, the Agency-wide e-newsletter, Agency-wide emails, and external communications. The system allows for greater coordination between offices, timely and accurate communication to staff, and consistency with FHFA's branding guidelines. GovDelivery maintains the email addresses of FHFA employees, as well as certain external parties, including members of the media and stakeholders. GovDelivery also maintains the emails and newsletters that it distributes, which contain names and photographs. The system is provided by vendor Granicus and is Federal Risk and Authorization Management Program (FedRAMP) authorized.

Section 1.0 Characterization of the Information

The following questions define the scope of the information requested and/or collected as well as reasons for its collection as part of the System/Collection being procured or developed. The questions address all information collected, with emphasis on the collection of PII, such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information types (e.g., contact information, demographic information, employment information) are being collected, used, disseminated, or maintained in the System/Collection?	Names, email addresses, and photographs.
1.2	What or who are the sources of the information provided to FHFA and included in the System/Collection?	FHFA employees, staff, members of the media, and external stakeholders.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	GovDelivery is used to share information with FHFA staff and the public, as necessary.
1.4	How is the information provided to or otherwise obtained by the System/Collection?	FHFA employee email addresses are captured by the system via Active Directory. External stakeholders email addresses are entered into the system by staff from lists of stakeholders who have previously requested that FHFA inform them about certain topics of interest. Media email addresses are also entered into the system by staff from FHFA's Meltwater subscription service, in which members of the media subscribe to request information on topics of interest.

1.5	Are Social Security Numbers (SSNs) being collected or used in the System/Collection? • If yes, describe in detail: 1) The business justification for collecting or using SSNs; 2) The consequences if SSNs are not collected or used; and 3) How the SSNs will be protected while in use, in transit and in storage. • If no, state "N/A" in the response section.	N/A

Section 2.0 Uses of the Information

The following questions delineate the use of information.

#	Question	Response
2.1	How will the information be used and for what purpose?	FHFA uses the GovDelivery system to communicate with staff via email and to share internal information, e.g., FHFA's agency-wide newsletter. The system is also used to share information with members of the public.
2.2	Describe any types of measures or processes in place to ensure that information is only used in the manner for which it was collected.	The Office of Congressional Affairs and Communications (OCAC) limits access to only FHFA staff who have a business need to use the system to send communications to employees and the public for business purposes. Only those designated employees are permitted access to the system as administrators and their permissions and access is limited to their business need.

Section 3.0 Retention

The following questions outline how long information will be retained after the initial collection.

#	Question	Response
3.1	How long is the information retained?	Content is stored in the system indefinitely.
3.2	Has a retention schedule been approved by FHFA's Records Management Office and National Archives and Records Administration (NARA)? If yes, provide the corresponding General Record Schedule (GRS) or FHFA specific Records Schedule number.	Yes. The applicable retention is FHFA's Comprehensive Records Schedule (CRS) Item 1.2 Official Agency Communications, Congressional Relations, and Publications - Public communications, Congressional correspondence and reporting, and official agency publications not covered elsewhere in this schedule, including FHFA's Annual Report to Congress, Strategic Plan, Performance and Accountability Report, press releases, media advisories, statements, testimonies, research papers, authorizations, and official speeches not covered by Item 1.1. These are Permanent records that will be transferred to the National Archives when they are 30 years old.

Section 4.0 Notice, Access, Redress and Correction

The following questions are directed at notice to the individual, the individual's right to consent to uses of the information, the individual's right to decline to provide information, and the individual's ability to ensure the accuracy of the information collected about them.

#	Question	Response
4.1	Is the information in this System/Collection retrieved by an individual's name or personal identifier such as an SSN or other identification? • If no, please put "no" in the Response section. • If yes, the System/Collection will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)). Please provide the SORN(s) name and number or indicate that a SORN is in progress.	No.
4.2	How is notice about the collection of PII provided to individuals prior to the collection for the System/Collection (e.g., direct notice, Privacy Act Statement or public notice, SORN)? If notice is not provided, explain why not.	Employees will be provided direct notice when they are asked to submit information, including PII to OCAC for use in the *Fresh Facts* newsletter. Notice is not provided to FHFA staff regarding the collection of their email address because it is not collected directly from individuals but from Active Directory. Notice is also not provided to members of the public because each individual (stakeholder and media) has requested that FHFA provide agency information to them via their email address.

4.3	Is an individual's response to the request for information voluntary or mandatory?	Voluntary.
4.4	What are the consequences if an individual declines to provide the information?	If an individual declines to provide their email address to FHFA, they will not receive email messages from the agency. If an employee declines to provide information to be included in the *Fresh Facts* newsletter, their information is not included in the newsletter.
4.5	What are the procedures that allow individuals to gain access to their information?	The messages and *Fresh Facts* newsletters are sent out via email and stored on the intranet. Employees can access the newsletters by clicking the Fresh Facts button on the FHFA intranet home page.
4.6	What are the procedures for correcting inaccurate or erroneous information?	Once a message is sent, any inaccuracies or incorrect information cannot be addressed in that message and that message cannot be altered. To avoid misinforming FHFA employees, contractors, and the public, the incorrect message can be corrected and resent via the system, but that will not cause the deletion of the previously mistaken message.

Section 5.0 Sharing and Disclosure

The following questions define the content, scope, and authority for information sharing.

#	Question	Response
5.1	Is information shared with internal office(s) or division (s)? • If yes, please identify the FHFA office(s) or division(s) and describe the information shared and for what purpose. • If no, please state "N/A" in the response section.	Yes, all messages and newsletters sent through GovDelivery are shared with all FHFA offices and divisions.
5.2	Is information shared with external (outside FHFA) agencies, organizations, contractors, or other entities? For purposes of this Section, external organization(s) include Federal, state, and local government, and the private sector. • If yes, please identify the information shared, and for what purpose. • If no, skip to Section 6.	Yes, messages are sent via the system to external stakeholders and the media, albeit infrequently. However, no PII is shared in these messages.

5.3	Is the sharing of PII outside the agency compatible with the stated purpose of the original information collection? • If yes and a SORN applies, identify the applicable routine uses in the SORN listed in Question 4.1. • If no and/or a SORN does not apply, identify the legal authority that permits the sharing outside FHFA.	PII is not shared outside of the agency.

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	Will FHFA Office of Inspector General (OIG) or non-FHFA personnel (e.g., contractor personnel, regulated entity personnel) have access to the System/Collection and information contained therein? • If yes, how will they gain access to the System/Collection? • If no, how will the agency control access to and use of that information? • Are there procedures or criteria documented in writing? If so, please describe.	Yes, the vendor, Granicus/GovDelivery, has the ability to access FHFA's system for training and troubleshooting purposes.
6.2	Are there any conflicts of interest with respect to the System/Collection or information? If so, identify the conflicts of interest and describe how they are addressed.	No.
6.3	Describe the type and frequency of training that is provided to users that is specifically or generally relevant to the System/Collection.	All FHFA employees are required to undergo Security, Privacy, and Records and Information Management (RIM) training at new employee onboarding training and annually thereafter. In addition, all FHFA users with elevated privileges receive specialized security training, and role-based privacy awareness training for those individuals whose work duties and responsibilities involve the collection, use, storage, access, or maintenance of PII. OCAC has a training guide and meets quarterly with its GovDelivery contractor for training on new features. Additionally, OCAC's Standard Operating Procedure on Agency-Wide Email Distribution, available internally at https://intranet.fhfa.gov/downloader.ashx?objectid=2984200, is accessible to FHFA employees and provides information about this system and how it functions.

6.4	Describe the technical/administrative safeguards in place to protect the data.	GovDelivery is authorized under the Federal Risk and Authorization Management Program (FedRAMP). GovDelivery received its initial FedRAMP Authorization on 04/08/2016. It is in the continuous monitoring phase of the FedRAMP program and FHFA reviews the status of ongoing assessments at least annually. FHFA has developed Customer Controls that describe the Agency's implementation of controls that are the responsibility of FHFA as the Customer Agency, and not the responsibility of the vendor. This includes the implementation of single sign-on authentication, procedures for securely managing access to the system, assigning permissions based on the concept of least privilege, generating and reviewing audit logs, etc.

Section 7.0 Risk

The following questions describe the risk to the information within the System or Collection.

#	Question	Response
7.1	Given the amount and type of information collected, what are the risks to an individual's privacy associated with collection of the data? Explain in detail how the loss or compromise of the information will/can affect an individual's privacy and describe how these risks are mitigated.	The data collected is limited to a person's name, email, photograph, and any information submitted for *Fresh Facts* articles. No other identifiable information is collected so the risk caused by loss or compromised data is low. The risks are mitigated by ensuring that the information is only shared with the intended audiences per the administrators who are using the system.
7.2	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	The data collected only applies to a person's name, email, photograph, or information submitted for *Fresh Facts* articles. No other identifiable information is collected. Only administrators have access to the archived information.
7.3	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	All externally shared information is intended for public consumption and dissemination and therefore, there is no risk associated with external sharing of data.