FARM CREDIT ADMINISTRATION
PRIVACY IMPACT ASSESSMENT (PIA)

SYSTEM, PROGRAM, OR PROJECT NAME: GovDelivery Communications Cloud

SYSTEM TYPE: Information Technology System or Capability

PURPOSE: The GovDelivery Communications Cloud system is a FedRAMP authorized Software as a Service (SaaS) solution, which provides for efficient communication of timely information to the public. FCA uses the system to handle email subscription management and to deliver opt-in email to interested parties. Visitors to FCA's website, www.fca.gov, may choose to subscribe to receive email correspondence based on individual, self-selected, needs and interests.

AUTHORITY: 12 U.S.C. 2243, 2252, and the Federal Information Security Management Act (FISMA), Pub. L. No. 107-347

INFORMATION OVERVIEW:

Covered Person(s)	Included
Farm Credit Institution Employees	☑
Farm Credit Institution Customers	☐
FCA Employee(s), Contractors, Interns	☑
Employees of other federal agencies	☐
Members of the Public	☑

Personally Identifiable Information (PII) Element(s)	Included
Full Name	☐
Date of Birth	☐
Place of Birth	☐
Social Security number (SSN)	☐
Employment Status, History or Information	☐
Mother's Maiden Name	☐
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☐
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☐
Home Address	☐
Phone Number(s) (non-work)	☐
Email Address (non-work)	☑
Employee Identification Number (EIN)	☐
Financial Information	☐
Driver's License/State Identification Number	☐
Vehicle Identifiers (e.g., license plates)	☐
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☐
Education Records	☐
Criminal Information	☐
Military Status and/or Records	☐
Investigative Report or Database	☐
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐
Photographic Identifiers (e.g., image, x-ray, video)	☐
Other (Specify): Subscription preferences; account password (if created by user).	☑

LIFECYCLE NARRATIVE:

The GovDelivery Communications Cloud system is a FedRAMP authorized SaaS solution. The system provides several features to support the efficient communication of timely information to the public. It provides a comprehensive digital communications management solution tailored to public sector requirements. It is designed to facilitate and increase citizen engagement with public government messaging.

FCA uses GovDelivery to disseminate official Farm Credit Administration information to subscribers of an email list. To accomplish this, users provide an email address, subscription preferences (frequency and generalized content topics) and, if they so choose, a password to use in managing their account. GovDelivery may also be used to disseminate information about i) FCA events; or ii) information that may be of interest to the press. Such information may include PII, such as names, photographs and contact information of FCA staff, however, such information is not stored in the GovDelivery solution and is otherwise publicly available.

In general, information collection is voluntary. Information in the system is primarily collected directly from individuals (subscribers). In some cases, information is collected from Farm Credit System (FCS) institution representatives on behalf of their employees – emails submitted in this case are business email addresses and not personal email addresses. In other cases, FCA includes public officials of FCS institutions. Subscribers are sent a confirmation email to validate their intent to sign up for emails and confirm their subscription preferences. Additionally, users may amend their information or unsubscribe at any time by logging into their account and updating their preferences or choosing "unsubscribe."

When information is collected directly from individuals, notice is provided of the collection and use of provided information in the form of a Privacy Act statement, which references the applicable System of Records Notice (FCA-13 – Correspondence Files - FCA). These individuals have opportunities to change or update information that is erroneous, out of date, or no longer relevant, either by directly updating their account or by requesting access to or amendment of their information in accordance with the Privacy Act and the FCA's Privacy Act regulations, as outlined in 12 CFR Part 603. In addition to the Privacy Act Statement, a web privacy policy is also provided. Additionally, FCA has published this PIA and, where applicable, relies on a SORN to provide notice to impacted individuals.

Finally, information in the system may be shared internally to facilitate the distribution of communications and information or the management of such distribution lists, and externally in accordance with the Routine Uses identified in the applicable SORN, FCA-13. Any external sharing of information is within scope of the Agency's authorities and regulations and facilitates a specific FCA business function. Users can learn more about how FCA uses the information internally by reading the Agency's web privacy policy. Additionally, GovDelivery, which provides the underlying service to FCA, does not share information with third-parties, as outlined in their privacy policy, available at https://granicus.com/privacy-policy/.

COMPLIANCE WITH APPLICABLE STATUTES, REGULATIONS, AND REQUIREMENTS:

For each, indicate as applicable and provide a link or a brief description of compliance. If not applicable, indicate with N/A.

The Privacy Act of 1974 (As Amended)	
System of Records Notice(s)	FCA's use of GovDelivery is covered by the Privacy Act System of Records: FCA-13 – Correspondence Files – FCA, available here.
Computer Matching and Privacy Protection Act of 1980	
Notice of Computer Matching Agreement(s)	N/A –FCA does not have any computer matching agreements that pertain to this system.
The Paperwork Reduction Act of 1995	
OMB Control Number(s) or related Form(s)	N/A –FCA does not have any OMB Control Numbers of forms associated with this system.
The Federal Records Act of 1950 (As Amended)	
Record(s) Control Schedule Name(s) and Number(s)	Records are maintained in accordance with FCA's Comprehensive Records Schedule and NARA's General Records Schedule (GRS) 6.4: Public Affairs Records, item 020. Specifically, such items are considered temporary and are to be destroyed when 90 days old, with longer retention authorized as necessary for business use.
Other	
N/A	N/A

ADMINISTRATIVE AND TECHNOLOGICAL CONTROLS:

☑	All applicable controls for protecting PII as defined in NIST Special Publication (SP) 800-53, Revision 4, Appendix J and NIST SP 800-122 have been implemented and are functioning as intended, have compensating controls in place to mitigate residual risk, or have an approved Plan of Action and Milestones (POA&M).
☑	The system has been reviewed for and assigned a categorization level in accordance with NIST FIPS Publication 199 and NIST Special Publication 800-60, and the SAOP has approved the categorization. Federal Information Processing Standards (FIPS) 199 Security Impact Category: Low* *Note: FedRAMP has authorized the solution as Moderate, but for FCA's use, the system is authorized as Low.
☑	A security assessment has been conducted for the system and it has been determined that there are no additional privacy risks.
☑	The information system has been secured in accordance with Federal Information Security Modernization Act (FISMA) requirements. Most Recent Assessment & Authorization Type: Authorization to Use (ATU) and Date: May 27, 2020 ☐ This is a new system and Assessment & Authorization Date is pending.
☑	A comprehensive listing of data elements included in the system has been provided to the Privacy Officer, reviewed and approved, and included in the Agency-wide PII Inventory.
☐	System users are subject to or have signed a confidentiality or non-disclosure agreement as applicable.
☑	System users are subject to background checks or investigations.* *FCA Administrators undergo background investigations as part of their employment with the Agency; GovDelivery staff are subject to background checks or investigations in accordance with FedRAMP requirements.
☑	System access is limited to authorized personnel with a bona fide need-to-know in support of their duties.
☑	Notice is provided in the form of a Privacy Act Statement, Privacy Notice, Privacy Policy or similar, as applicable.
☐	Contract(s) or agreement(s) (MOUs, MOAs, ISAs, etc.) establish ownership rights over data, including PII.
☐	Acceptance of liability and responsibilities for exposure of PII is clearly defined in agreement(s) or contract(s).
☑	Access to and use of PII is monitored, tracked, or recorded.
☑	Training on PII, confidentiality, and information security policies and practices is provided to system users or those with access to information.

ADMINISTRATIVE AND TECHNOLOGICAL CONTROLS NARRATIVE

GovDelivery is a self-contained SaaS offering owned and operated by Granicus Company (GovDelivery LLC and Granicus Inc.), which has been authorized by the FedRAMP Joint Authorization Board (JAB) for use by federal agencies. There are currently 400 federal agencies using GovDelivery, including the U.S. Department of Treasury, the Federal Trade Commission, the Securities and Exchange Commission, the Department of Justice, and the Federal Reserve. Under the FedRAMP framework, GovDelivery is subject to an independent security review of the provider's policies, products, and infrastructure – the outcome of this review is made available to federal agencies considering the solution for use.

FCA reviewed the documentation and other supplied materials provided through the FedRAMP package and determined that the security controls in place are sufficient to protect FCA information categorized as low. While the system was authorized by the JAB at a Moderate level, FCA has categorized information stored in the system (email addresses, subscriber preferences and, if created, a password) as "low," in terms of sensitivity. The system was granted an Authorization to Use (ATU) by the FCA Chief Information Officer (CIO). GovDelivery secures information in the system by a variety of means, including, but not limited to:

- Physical security controls at the data center where the solution is hosted;
- Use of firewalls, intrusion detection prevention (IDS/IPS) systems, anti-virus and other software and capabilities for detection of malware and other malicious threats;
- Use of Transport Layer Security (TLS) connections and multi-factor authentication;
- Access controls and least privilege; and
- Application, network, server, and database activity logs, with resulting logs made available to FCA upon request.

In addition to the controls provided by the service provider, FCA is responsible for a series of controls that address how information in the system is processed, such as data handling in accordance with the sensitivity of data in the system; managing user access and permissions (who can view or change specific information in the system); and records retention.

Users are limited to four types:

Subscribers – end users who access the GovDelivery site via links on FCA's website, fca.gov, or via system-generated emails. These users can access their own data (email addresses, subscription preferences, and, if created, passwords), update their data, or delete their accounts.

FCA Administrators – these are FCA employees within the Office of Congressional and Public Affairs and the Office of Information Technology (OIT). There are different types of administrator roles with varying degrees of permissions and system access, for example – the ability to add or send new content to subscribers versus the ability to add a new administrator to the system or grant system permissions. FCA employees will have access to the system only as needed and on a least-privilege basis. FCA has designated an individual to serve as the primary Client Administrator over the entire system. In this role, the Client Administrator is authorized to approve other administrators within the system. Account administrative privileges are restricted to the primary Client Administrator and an Office of Information Technology (OIT) point of contact. Accounts and permissions are reviewed on an annual basis. FCA users leverage usernames and passwords with a second factor of authentication to access the system, and all users must have FCA accounts and government-issued personal identity verification (PIV) cards, or acceptable alternatives, to access FCA's GovDelivery system.

GovDelivery Administrators, and GovDelivery Technical Staff – These individuals are identified by GovDelivery and assigned roles based on their job functions. They are given only the permissions needed to perform their work – for example, to assist FCA staff with implementation support or set up a new Client Administrator in the system.

FCA Administrators receive notification whenever a major system change occurs (such as adding a new administrator or changing related permissions) or when a communication is sent out to the subscriber list (Administrators receive a copy). These "alerts" help keep the FCA Administrators aware of any potential misuse of the system.

Formalized, documented procedures exist for use of the GovDelivery system. These procedures include the steps necessary to create and remove accounts, grant permissions, provide system training, and conduct annual audits of user accounts.

All FCA users receive annual IT security and privacy awareness training and are responsible for reviewing and attesting to the requirements outlined in FCA's PPM 902 and 906, which outline user responsibilities for use of FCA IT resources. Additionally, OIT provides staff in OCPA responsible for use of GovDelivery with a briefing on their responsibilities in using the system, including confidentiality considerations as they relate to PII.

PRIVACY RISK ANALYSIS

What follows is a general overview of the primary risks associated with FCA's use of GovDelivery. These risks and their mitigations are described in detail below:

Overall Risk:

FCA's use of GovDelivery presents an overall low privacy risk.

FCA evaluated the data included in its use of GovDelivery and determined that it is of low risk. In accordance with the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-122, "the confidentiality of PII should be protected based on its impact level," noting that a "breach of the confidentiality of PII at the low impact level would not cause harm greater than inconvenience, such as changing a telephone number." In the event of a loss of confidentiality, the harm to impacted individuals would be relatively minor – such as SPAM or otherwise unsolicited email – and result in a minor inconvenience. Further, additional controls, such as the ability to apply a password, email confirmation for subscribers, and the ability of users to directly amend or correct their information through the system, reduce the overall risk presented. Despite the low risk, FCA and the service provider have implemented controls to reduce the risk of unauthorized access to or use of PII maintained by the system.

Users are provided opportunities for notice and consent, and may access, correct, update, and delete their accounts at any time. When an individual unsubscribes, the individual's subscription is permanently deleted from the GovDelivery system.

DOCUMENT CONTROL:

Approval

WESLEY FRAVEL Digitally signed by WESLEY FRAVEL Date: 2020.06.29 16:09:38 -04'00' Wesley Fravel, FCA Privacy Officer	ELSIE SHAFFER Digitally signed by ELSIE SHAFFER Date: 2020.07.07 20:46:00 -04'00' Jeannie Shaffer, Chief Information Security Officer (CISO) and Associate Director, Governance Division
YAGHMOURE Digitally signed by YAGHMOURE Date: 2020.07.08 14:34:54 -04'00' Emily Yaghmour, Deputy Director, Office of Congressional and Public Affairs	GOLLEYJ Digitally signed by GOLLEYJ Date: 2020.07.09 07:46:28 -04'00' Jerry Golley, Chief Information Officer (CIO) and Senior Agency Official for Privacy

Change Control and Approval History

Version	Date	Change Summary
V 1.0	6/29/2020	Initial Version
	[DATE]	Choose an item.
	[DATE]	Choose an item.