FARM CREDIT ADMINISTRATION
PRIVACY IMPACT ASSESSMENT (PIA)

SYSTEM, PROGRAM, OR PROJECT NAME: Use of Third-Party Social Media for Official FCA Communications

SYSTEM TYPE: Third-Party Website or Social Media Application

PURPOSE: The Farm Credit Administration uses social media as a strategic communication tool to facilitate both internal and external communication. We have developed this PIA in accordance with OMB guidance on the use of third-party websites or applications that make personally identifiable information (PII) available to the public.

AUTHORITY: 12 U.S.C. 2243, 2252

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)	☐
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)	☐
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): Usernames, handles, profiles, and similar content posted and made available by users on social media platforms.	☒

LIFECYCLE NARRATIVE:

- FCA uses social media as a strategic communication tool to expand our reach and increase our visibility to a broader, more diverse audience.

Through the social media websites and applications covered by this PIA, we do not directly solicit, collect, maintain, or disseminate sensitive personally identifiable information (PII) from individuals who interact with it. This PIA covers our use of the following social media third-party services:

- FCA Official Twitter – @FCAgov (https://twitter.com/fcagov)
- FCA Official Facebook – Farm Credit Administration (https://www.facebook.com/fcagov)
- FCA Official YouTube – FCA (https://www.youtube.com/@fca9660)
- FCA Official LinkedIn – Farm Credit Administration (https://www.linkedin.com/company/farm-credit-administration/)
- FCA Official Instagram — Farm Credit Administration (https://www.instagram.com/farmcreditgov/)

Although FCA does not solicit, collect, maintain, or disseminate PII from visitors to our third-party social media sites, it is possible for individuals to voluntarily make such information available to us. Such information may become available when a user provides, submits, communicates, links, posts, or associates information with an official FCA account (e.g., by liking a post, following the agency's account, responding to a post, or commenting on content we generate). We will not otherwise collect, maintain, or disseminate personal information made available on any of our official social media accounts.

Typical examples of the types of PII that may become available to us include names of individuals and businesses, images from photos or videos, screen names, and email addresses. In addition, many third-party social media websites or applications request PII at the time of registration. The process will vary across third-party social media websites or applications, and often users can provide more than is required for registration. For example, users can provide their interests, birthdays, religious and political views, names of family members, relationship status, education, occupations and employment, photographs, contact information, and hometowns. If the privacy settings on the third-party social media website or application are not restricted, this information may be publicly available.

We do not collect or use Information provided to third-party social media websites or applications during registration. Information that individuals voluntarily submit as part of the registration process is not FCA property, and we will not solicit this information.

To the extent that our social media activity or public response constitutes the creation of a record under the Federal Records Act, we may maintain and archive this interaction according to records retention requirements. If a user submits PII in a request or an inquiry through our website, we may use the PII provided by the user to fulfill the specific request as outlined in the posted web privacy policy. However, we do not otherwise collect, maintain, or disseminate PII from individuals who interact with any of our social media websites or applications.

We do not share PII that is made available through our social media accounts with any individual or entity inside or outside the agency.

When interacting with FCA or others on a third-party website or application, PII that users share or disclose may become available to other users or any individuals with access to the website. To mitigate the risks of disclosure of sensitive PII, the agency has disabled comments to the extent possible on its social media sites and may choose to delete or hide comments or other user interactions when a user's sensitive information is included.

Only approved members of the Office of Congressional and Public Affairs have access to manage official agency social media websites and applications.

Generally, FCA does not collect, maintain, or disseminate PII from individuals who interact with authorized agency accounts. Therefore, PII cannot be retrieved with a personal identifier in a way that would constitute a system of records as defined by the Privacy Act.

Because FCA does not otherwise collect, maintain, or disseminate PII from individuals who interact with any of its social media websites or applications that are covered by this PIA, and information cannot be retrieved with a personal identifier, there is no requirement for a Privacy Act System of Records Notice.

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)	N/A – FCA does not collect, maintain, or disseminate PII from individuals who interact with any of its social media websites or applications, nor is information retrieved by personal identifier.
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 orforms associated with this system.
The Federal Records Act of 1950 (As Amended)	
Record(s) Control Schedule Name(s) and Number(s)	FCA uses social media websites and applications as platforms for communicating its messages to as many people as possible or to target specific audiences. To the extent that FCA's social media activity or public response constitutes the creation of a record under the Federal Records Act, the agency may maintain and archive such interaction according to records retention requirements. In the absence of an FCA-specific schedule, the agency will preserve all records generated by social media permanently until a schedule is approved by the National Archives and Records Administration (NARA).
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: N/A
☒	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: N/A ☐ 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 agencywide PII Inventory.
☐	System users are subject to or have signed a confidentiality or nondisclosure 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

FCA uses third-party social media for internal and external communications. The agency does not directly solicit, collect, or maintain PII through its use of social media, nor does the agency claim ownership of any data collected or solicited by the service providers who own the social media services. FCA does not consider the third-party social media applications and websites it uses to be an agency information system and has not conducted specific assessments of the security controls for these solutions. That said, the agency has implemented internal administrative controls on its use of these tools and, in some cases, has leveraged existing privacy and security features these tools provide to reduce the overall risk presented in their use.

By policy, the agency does not engage directly with individuals via social media. Additionally, to reduce the risk of disclosure of sensitive PII, the agency has disabled comments on its accounts (where possible) and may choose to delete or hide comments or other user interactions when a user's sensitive information is included.

All FCA social media pages include an official FCA seal to indicate their authenticity. In addition, each includes a direct link to the agency's homepage (fca.gov), which has a link to FCA's privacy program.

Formalized, documented policies and procedures exist for use of the agency's social media accounts. Among other things, these procedures cover account creation, security, records management, and approvals for posts. Only approved staff members in the Office of Congressional and Public Affairs have access to manage official agency social media websites and applications. Account credentials are secured from unauthorized access or use.

All FCA users receive annual IT security and privacy awareness training and are responsible for reviewing and attesting to the agency's Rules of Behavior, which outline user responsibilities for use of FCA IT resources.

PRIVACY RISK ANALYSIS

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

Overall Risk:

FCA's social media activities present an overall low privacy risk. FCA has identified the following privacy-related risks:

Disclosure of PII by users: When users interact on a social media website (e.g., by posting comments), PII that they share or disclose will ordinarily become available to other users or anyone else with access to the site. To mitigate the risks of disclosure of sensitive PII, the agency may choose to delete or hide, to the extent possible, comments or other user interactions when a user's sensitive information is included.

***Third-party advertising and tracking*:** A third-party website operator may display advertising or other special communications on behalf of other businesses, organizations, or itself when a user interacts with FCA on the social media application. If the user clicks on the advertisement or reads the communication to learn about the advertised product or service, the user's PII may be shared by the website operator with the advertiser. The user's actions may also initiate tracking technology (e.g., cookies, web bugs, or beacons), enabling the website operator or advertiser to create or develop a history or profile of the user's activities. The tracking data can be used to target specific types of advertisements to the user (i.e., behavioral advertising), or it can be used or shared for other marketing or nonmarketing purposes. Users can avoid or minimize these risks by regularly deleting cookies through their browser settings, by not

clicking on advertisements, and by not visiting advertisers' sites. Users may also opt out of some tracking technologies altogether.

Individuals falsely claiming to be FCA official pages: An individual with malicious intent may set up a third-party social media website and claim it to be an official FCA social media presence. To reduce this likelihood, all agency third-party social media websites have been appropriately branded. This branding gives the public confidence that this is an official FCA social media presence and they can trust the information on it.

Spam, unsolicited communications, spyware, and other threats: Users may also receive spam or other unsolicited or fraudulent communications because of their interactions with FCA on social media. To avoid harm, users should be wary of responding to such communications, particularly if they solicit the users' personal information, which can be used for fraudulent or other undesirable purposes. Users should also avoid accepting or viewing unknown or unsolicited links, applications, or other content that may be sent or forwarded in such communications. These unsolicited links and applications can contain unwanted tracking technology as well as computer viruses or other malicious payloads that can pose a variety of risks to the user.

DOCUMENT CONTROL:

Approval

/s/ Wesley Fravel, FCA Privacy Officer	/s/ Jeannie Shaffer, Chief Information Security Officer (CISO) and Associate Director, Governance Division
/s/ Emily Yaghmour, Deputy Director, Office of Congressional and Public Affairs	/s/ Jerry Golley, Chief Information Officer (CIO) and Senior Agency Official for Privacy

Change Control and Approval History

Version	Date	Change Summary
V 1.0	5/31/2018	Initial Version
V 2.0	8/8/2023	Revised for new agency template.
	[DATE]	Choose an item.