FARM CREDIT ADMINISTRATION
PRIVACY IMPACT ASSESSMENT

SYSTEM, PROGRAM, OR PROJECT NAME:

Use of Third-Party Social Media for Official FCA OIG Communications

SYSTEM TYPE

Third-Party Website or Social Media Application

PURPOSE

The Farm Credit Administration Office of Inspector General uses social media as a strategic communication tool to facilitate 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

The Inspector General Act of 1978, as amended, 5 U.S.C. §§ 401–424.

INFORMATION OVERVIEW

Covered Persons	Included
Farm Credit institution employees	☐
Farm Credit institution customers	☐
FCA employees, 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 record numbers, medical notes, or X-rays)	☐
Home address	☐
Phone number(s) (nonwork)	☐
Email address (nonwork)	☒
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.	☒

LIFE CYCLE NARRATIVE

FCA OIG uses social media as a strategic communication tool to promote public awareness of its mission and work products.

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

- X
- Facebook
- LinkedIn

Although the OIG does not solicit, collect, maintain, or disseminate PII from visitors to its third-party social media sites, it is possible for individuals to voluntarily make such information available to the OIG. Such information may become available when a user provides, submits, communicates, links, posts, or associates information with an official FCA OIG account (e.g., by liking a post, following the office's account, responding to a post, or commenting on content the OIG generates). The OIG 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.

The OIG does 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 OIG property, and the OIG will not solicit this information.

The OIG does not use official OIG social media accounts in the conduct of audits, inspections, evaluations, investigations, or other reviews, except to promote awareness of announced projects and finally issued reports. To the extent that information is collected from social media sites for investigative purposes, official OIG social media accounts are not used; the use of such information collected is addressed in the privacy impact assessment concerning the OIG's Complaints and Investigations System.

To the extent that the OIG's social media activity or public response thereto constitute a record under the Federal Records Act, the OIG will 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 FCA web privacy policy. However, the OIG does not otherwise collect, maintain, or disseminate PII from individuals who interact with any of our social media websites or applications.

The OIG does not share PII that is made available through our social media accounts with any individual or entity inside or outside FCA.

When interacting with the OIG 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 OIG 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. To further mitigate such risk, the OIG provides information on its social media accounts profiles regarding official avenues to submit complaints and information to the OIG.

Only personnel approved by the Inspector General have access to manage official OIG social media websites and applications.

Generally, the OIG 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.

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 — the OIG 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 – the OIG does not have any OMB Control Numbers or forms associated with this system.
The Federal Records Act of 1950 (As Amended)	
Record(s) control schedule name(s) and number(s)	To the extent that FCA's social media activity or public response thereto constitute the creation of a record under the Federal Records Act, the agency may maintain and archive such interaction according to records retention requirements. Applicable schedules may include National Archives and Records Administration (NARA) General Records Schedule 6.4, Public Affairs Records; DAA-0103-2018-0001, Records of the Office of Inspector General; and DAA-0103-2023-0001, Records of the Office of Inspector General.
Other	
N/A	N/A

ADMINISTRATIVE AND TECHNOLOGICAL CONTROLS

☐	All applicable controls for protecting PII as defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5 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.
☐	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 requirements. Most recent assessment and authorization type: Authorization to Use (ATU) and Date: N/A ☐ This is a new system, and the assessment and 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 confidentiality or nondisclosure agreements as applicable.
☒	System users are subject to background checks or investigations. * *OIG administrators undergo background investigations as part of their employment with the agency.
☒	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) (e.g. memorandums of understanding, memorandums of agreement, and information security agreements) establish ownership rights over data, including PII.
☒	Acceptance of liability and responsibilities for exposure of PII are clearly defined in agreement(s) or contract(s).
☒	Access to and use of PII are monitored, tracked, and 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 OIG uses third-party social media for external communications. The OIG does not directly solicit, collect, or maintain PII through its use of social media, nor does the OIG claim ownership of any data collected or solicited by the service providers who own the social media services. The OIG does not consider the third-party social media applications and websites it uses to be an OIG information system and has not conducted specific assessments of the security controls for these solutions. That said, the OIG 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 OIG does not engage directly with individuals via social media. Additionally, to reduce the risk of disclosure of sensitive PII, the OIG disables comments on its posts (where possible) and may choose to delete or hide comments or other user interactions when a user's sensitive information is included.

All FCA OIG social media pages include an official FCA OIG logo to indicate their authenticity. In addition, each includes a direct link to the FCA OIG's homepage (https://www.fca.gov/about/inspector-general), which has a link to FCA's privacy program. The OIG homepage also includes links to each of the social media pages.

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

Like all FCA users, OIG staff 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 OIG's use of third-party social media. These risks and their mitigations are described in detail below:

***Overall Risk**:*

FCA OIG's social media activities present an overall low privacy risk. The OIG 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 OIG 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 the OIG 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 OIG official pages: An individual with malicious intent may set up a third-party social media website and claim it to be an official FCA OIG social media presence. To reduce this likelihood, all OIG third-party social media websites have been appropriately branded. This branding gives the public confidence that this is an official FCA OIG social media presence, and they can trust the information on it. To further instill such confidence, the OIG provides links to its official social media accounts on the OIG's website and, where possible, will pursue account verification for each of its official social media accounts.

Spam, unsolicited communications, spyware, and other threats: Users may also receive spam or other unsolicited or fraudulent communications because of their interactions with FCA OIG 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/_____ Wesley Fravel, CISO and associate director, information protection division
_____/s/_____ Stephen H Ravas, inspector general	_____/s/_____ Jerry Versace, CIO and SAOP

Change Control and Approval History

Version	Date	Change Summary
V 1.0	10/8/2026	Initial Version