Farm Credit Administration
Office of Information Technology

PRIVACY IMPACT ASSESSMENT (PIA)

System Name: Use of Third-Party Social Media for Official FCA Communications

Issued by: Jerald Golley, CIO and Senior Agency Official for Privacy

Version 1
Approved: May 31, 2018

Document History

Version No.	Date	Author	Revision Description
1.0	May 31, 2018	FCA	Initial Release

References

- PPM 205 - Policy for Official Use of Social Media and Implementing Procedures, 8/23/2016
- OMB Memorandum M-10-06, Open Government Directive, 12/8/2009
- OMB Memorandum M-10-23, Guidance for Agency use of Third-Party Websites and Applications, 6/25/2010
- 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/channel/UCMLBjEdJAom6CaT3xRWV6oQ)
- FCA Official LinkedIn – Farm Credit Administration (https://www.linkedin.com/company/farm-credit-administration/)

Introduction

The Farm Credit Administration (FCA or Agency) recognizes that social media facilitates communication both internally and externally for the purpose of conducting official business.

In accordance with OMB Memorandum M-10-23, an "adapted" Privacy Impact Assessment (PIA) is required whenever an agency's use of a third-party website or application makes personally identifiable information (PII) available to the agency. In general, each adapted PIA should be posted on the agency's official website and should include:

1. the specific purpose of the agency's use of the third-party website or application;
2. any PII that is likely to become available to the Agency through public use of the third-party website or application;
3. the Agency's intended or expected use of PII;
4. with whom the Agency will share PII;
5. whether and how the agency will maintain PII, and for how long;
6. how the Agency will secure PII that it uses or maintains;
7. what other privacy risks exist and how the Agency will mitigate those risks; and
8. whether the agency's activities will create or modify a "system of records" under the Privacy Act.

Scope

The following Privacy Impact Assessment (PIA) covers FCA's use of the following Social Media Third-Party Services ("social media"):

- 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/channel/UCMLBjEdJAom6CaT3xRWV6oQ)
- FCA Official LinkedIn – Farm Credit Administration (https://www.linkedin.com/company/farm-credit-administration/

Impact Assessment

1. Purpose of FCA's Use of Social Media

FCA uses social media as a strategic communication tool to facilitate both internal and external communication. The goal is for FCA to use social media as an effective way to expand its reach and increase its visibility to a broader, more diverse audience. The benefits of social media include the following:

1. Improving the Agency's reach to diverse audiences;
2. Furthering the delivery of consistent, timely, repetitive, and tailored/targeted messages; and
3. Facilitating engagement and transparency

Specific procedures related to FCA's use of social media are available in PPM 205 – Policy for Official Use of Social Media and Implementing Procedures.

Through the social media websites and applications covered by this PIA, FCA does not solicit, collect, maintain, or disseminate sensitive personally identifiable information (PII) from individuals who interact with it.

2. Information Likely to Be Available to the Agency Through Social Media

Although FCA does not solicit, collect, maintain, or disseminate PII from visitors to these third-party social media applications, it is possible for individuals to voluntarily make such information available to the Agency. Such information may become available when a user provides, submits, communicates, links, posts, or associates information with official FCA accounts (e.g., through "liking," "following," responding, or commenting on content generated by the FCA). The Agency will not otherwise collect, maintain, or disseminate personal information made available on official FCA social media accounts.

Typical examples of the types of PII that may become available to agencies include names of individuals and businesses, images from photos or videos, screen names, email addresses, etc. 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 such information as his or her interests, birthday, religious and political views, family members and relationship status, education, occupation and employment, photographs, contact information, and hometown. If the privacy settings on the third-party social media website or application are not restricted, such information may be made available to the Agency.

Information provided to third-party social media websites or applications during registration is not collected or used by FCA. Information that individuals voluntarily submit as part of the registration process is not the property of FCA and the Agency will not solicit this information.

PII that is voluntarily provided by an individual may be used by the Agency to respond to inquiries, answer questions, or fulfill a request submitted by the individual.

3. Intended or expected use of PII

FCA uses social media websites and applications as platforms for communicating its message 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. If a user submits PII in a request or an inquiry to an agency through the agency's website, the agency may use the PII provided by the user to fulfill the specific request. However, the Agency does not otherwise collect, maintain, or disseminate PII from individuals who interact with any FCA social media website or application.

FCA may use a person's screen name, email address, or other information provided by the user to respond to specific comments or questions directed to or about Agency activities, or to fulfill a request. In such situations, only the minimum required information that is needed to appropriately respond is used.

4. Sharing or disclosing PII

FCA does not transmit or share PII that is made available through its social media presences internally or with outside entities.

5. Maintenance and retention of PII

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. If a user submits PII in a request or an inquiry to an agency through the agency's website, the agency may use the PII provided by the user to fulfill the specific request. FCA does not otherwise collect, maintain, or disseminate PII from individuals who interact with any of its websites or applications that are covered by this PIA. Other PII, such as user registration information, is maintained by the third-party website or application, and is not accessible by FCA.

6. Securing PII

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. In order to mitigate the risks of disclosure of sensitive PII, to the extent possible, the agency may choose to delete or hide comments or other user interactions when a user's sensitive information is included. This will be done in accordance with the posted FCA comment moderation policy (see PPM 205, Guideline 3(h)).

Only approved members of the FCA Social Media Council and Office of Congressional and Public Affairs have access to manage official Agency social media websites and applications (see PPM205, Guidelines 1 and 2).

7. Identifying and Mitigating Privacy Risks

FCA has identified the following privacy-related risks:

- *Disclosure of PII by users*: When interacting on a social media website (e.g., posting comments), PII that users share or disclose will ordinarily become available to other users or anyone else with access to the site.

  In order to mitigate the risks of disclosure of sensitive PII, to the extent possible, the agency may choose to delete or hide comments or other user interactions when a user's sensitive information is included. This will be done in accordance with the posted FCA comment moderation policy (see PPM 205, Guideline 3(h)).

- *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 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," "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 non-marketing purposes. Users can avoid or minimize these risks by regularly deleting "cookies" through their browser settings, not clicking on advertisements or not visiting advertisers' sites. Users may also opt-out of some tracking technologies all together.

- *Individuals falsely claiming to be FCA Official pages*: A malicious individual may set up a third-party social media website and claim it to be an official FCA social media presence. To negate these false sites, all Agency third-party social media websites have been appropriately branded. This branding allows the public to know that this is an official FCA social media presence, and that they can trust the information that is on it.

- *Spam, unsolicited communications, spyware, and other threats*: Users may also receive spam or other unsolicited or fraudulent communications as a result of their interactions with the FCA social media presence. To avoid harm, users should be wary of responding to such communications, particularly those that may solicit the user's 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.

8. Creating or modifying a system of records

Generally, FCA does not collect, maintain, or disseminate PII from individuals who interact with authorized agency accounts. Therefore, PII is not, nor can it be, retrieved by a personal identifier of United States citizens and/or lawfully admitted permanent resident aliens.

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. If a user submits PII in a request or an inquiry to an agency through the agency's website, the agency may use the PII provided by the user to fulfill the specific request. 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 by a personal identifier there is no requirement for a Privacy Act System of Records Notice.

Issuing Unit:	**OCPA**
PPM Category:	**Public Affairs**
Document Number:	**205**
Date of Publication:	**8/23/2016**
Title:	**Policy for Official Use of Social Media**
Worklife:	**No**

POLICY

The Farm Credit Administration (FCA or Agency) recognizes that social media facilitates communication both internally and externally for the purpose of conducting official business. It is FCA's policy to (1) create, maintain, and monitor all official social media applications, channels, content, and profiles in accordance with its mission; and (2) consider security, privacy, and transparency.

FCA uses social media as a strategic communication tool to facilitate both internal and external communication. FCA social media channels and applications must be related to FCA's mission. The goal is for FCA to use social media as an effective way to expand its reach and increase its visibility to a broader, more diverse audience. The benefits of social media include the following:

4. Improving the Agency's reach to diverse audiences
5. Furthering the delivery of consistent, timely, repetitive, and tailored/targeted messages
6. Facilitating engagement and transparency

This policy applies to all FCA offices, as well as to all FCA employees and contractors who are engaged in the official use of social media. In the event of any conflict between this policy and any other FCA policy, directive, or regulation, this policy will govern and supersede any previous issuance or directive with regard to social media.

REFERENCES

- The Rehabilitation Act of 1973, 29 U.S.C. §794(a) [Section 508 Compliance]
- Office of Management and Budget (OMB) Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010)
- OMB Memorandum M-13-10, *Antideficiency Act Implications of Certain Online Terms of Service Agreements* (April 4, 2013)
- The Privacy Act of 1974, 5 U.S.C. §552a
- FCA PPM 902, Computer Security Program
- FCA PPM 902B, FCA Internet, E-Mail, and Network Acceptable Use Policy
- FCA PPM 903, Records Management
- Negotiated Terms of Service Agreements
- U.S. Digital Registry

DELEGATIONS

The Assistant Director, Office of Congressional and Public Affairs (OCPA), is delegated the responsibility to develop and recommend procedures and controls necessary to implement this policy. The Chief Operating Officer (COO) is authorized to approve implementing procedures and controls.

REPORTING REQUIRED

The Assistant Director of OCPA will evaluate and report on this policy to the COO as requested.

Approved: /s/ Date: 08/23/2016

Kenneth A. Spearman

Board Chairman and Chief Executive Officer

Farm Credit Administration

IMPLEMENTING PROCEDURES

INTRODUCTION AND PURPOSE

These procedures govern FCA's official use of social media. In the past several years, the use of Facebook, Twitter, LinkedIn, YouTube, and other social media tools to disseminate information has grown significantly and continues to trend upward. Social media is a group of online tools and services that encourage interaction and engagement among the individuals who use these tools. Social media services are participatory and include user-generated content.

Social media activities include posting content on the Internet, commenting on content that others have created or posted, and downloading and interacting with content that others have created. Social media can include, but is not limited to, Web and mobile phone applications, blogs, photo- and video-sharing sites, micro-blogging and social networking sites, and wikis.

GUIDELINES FOR OFFICIAL USE OF SOCIAL MEDIA

1. **Official Postings to FCA-Sponsored Social Media Channels**

   The Office of Congressional and Public Affairs (OCPA), in conjunction with the Social Media Council (Council), will maintain and monitor FCA social media profiles. The Council will access and contribute content in accordance with these procedures and the security standards of the Office of Information Technology (OIT). The content of all posts must be formally approved through these procedures before public release.

   All content posted by FCA in FCA-sponsored social media channels and applications must be Section 508 compliant unless the Chief Information Officer grants an exception.

2. **Managing and Posting on Official FCA Social Media Channels**

   Council staff who maintain and monitor FCA social media profiles must commit time and resources to establish a profile or channel, moderate comments from the public, maintain security standards, and ensure Section 508 compliance.

3. Specific Requirements for Creating and Managing Official Social Media Profiles, Channels, or Applications

The FCA Social Media Council, which includes representatives from various FCA offices, will develop guidelines that address the process, best practices, and technical specification for social media. OCPA will approve the guidelines and add them to these procedures. The Council will follow these guidelines in all social media activities.

a. **Profile Creation and Disclaimers**. Only the Council may create an official profile. The Council must brand all official profiles in social media channels with the FCA name and/or logo. All official profiles must include a disclaimer based on Office of Management and Budget policy and the negotiated Terms of Service. The disclaimer should read as follows:

> Comments and images posted by the public do not necessarily represent the views of FCA. If you are looking for official FCA information, please go to www.fca.gov.

When applicable, all profiles must include this posted comment policy.

b. **Terms of Service**. Prior to using a social media channel, the Council must ensure that the channel has a negotiated Terms of Services agreement in place with the General Services Administration (GSA) and FCA.

c. **Privacy Impact Assessment**. Each new social media site or application must be included in the privacy impact assessment conducted by OIT. Each new social media site or application must include a privacy statement and a posted link to FCA's privacy policy.

d. **Clearance**. Any use of a social media channel, creation of a new profile, or development of a social media application must be approved by OCPA in coordination with OIT. New social media profiles must also be reviewed by the FCA Social Media Council prior to launch.

The Council must carefully consider the nature of posted content and messages. Content that is likely to draw widespread media attention, reflects a change in policy, or addresses a controversial topic must be cleared through the Chief Operating Officer.

e. **Registering Profiles**. The Council will maintain a directory of all official social media profiles. The Council must register profiles with USA.gov, as required by OMB.

f. **Security**. All participation in social media must comply with information security and privacy standards published by OIT, OMB, and GSA. It must also comply with the Privacy Act and other applicable requirements.

   Passwords for an official account must be unique to that account; the creator of each page must maintain a password that is distinct from his or her agency password. Passwords must be changed on all social media channels every 180 days for security purposes.

g. **Guidance and Best Practices**. All participation in social media will follow the guidance, standards, and best practices described in this document.

h. **Content Monitoring and Moderation**. A Council member must moderate comments and approve or remove them based on a posted comment policy. All social media profiles require regular management; the frequency depends on the type of site and type of content. Frequency of maintenance should be posted as part of the comment policy.

i. **Records Management**. A federal record is determined by its content and not by the medium in which it is created, received, or transmitted. The Federal Records Act (44 U.S.C. 3301) defines federal records as any material that is created or received in the course of government business, regardless of its form or characteristics, and worthy of preservation. Social media content that meets this definition must be managed according to applicable law and regulations. As with email and text messaging, if social media applications are used to conduct Agency business, employees are responsible for capturing the "record" content and maintaining it for the appropriate retention period in an official FCA record-keeping system.

   Responsible Council members must establish controls over FCA social media sites to ensure federal records are being captured and to

   1. select a designee(s) who is responsible for official records created, received, and transmitted;
   2. ensure designee(s) monitors content to ensure that it is downloaded and stored in a way that prevents modification of records and allows access for required retention periods;
   3. ensure designee(s) has knowledge of where original records reside; and

4. ensure designee(s), with the assistance of the Records Officer, determines how social media records will be downloaded from social media sites for temporary or permanent retention.

The originating Council member(s) will contact the FCA Records Officer for assistance in determining record status and for additional management assistance.

j. **Section 508 Compliance**. All content posted by FCA in social media channels and applications must be Section 508 compliant unless an exception is granted by the Chief Information Officer. Complying with Section 508 includes, but is not limited to, providing captioning and audio description of videos, using appropriate headings and color, and providing alternate text and descriptions in the captions of photos and other images. The FCA Section 508 Coordinator must approve section 508 compliance of FCA's social media applications.

RESPONSIBILITIES

1. **FCA Chief Information Officer**
   a. Provides technical and electronic resources for hosting, maintaining, and administering FCA social media channels and applications, both internally and externally, and provides expertise in security.

2. **FCA Privacy Act Officer**
   a. Provides expertise in privacy.

3. **FCA Director for OCPA**
   a. Chairs the FCA Social Media Council.
   b. Recommends additional policies, if required, for social media-related issues.

4. **FCA Assistant Director for OCPA**
   a. Reviews and approves requests to establish FCA-sponsored public, external social media, as applicable.
   b. Ensures clearance of all posted content.
   c. Ensures all social media activities comply with this social media policy.
   d. Maintains and makes available a list of FCA-sponsored public, external social media channels and applications.
   e. Provides oversight and management of social media channels and applications operated by FCA.

5. **FCA Records Officer**
   a. Provides expertise in records documentation.
   b. Provides records control schedules.
   c. Provides other assistance for maintaining federal records.

6. **FCA Social Media Council**
   a. Reviews and approves standards, guidelines, and best practices related to FCA's social media use.
   b. Reviews new FCA social media profiles prior to launch and provides feedback and recommendations.
   c. Develops and maintains usage guidelines, posting guidelines, and other guidelines needed for FCA social media use.
   d. Provides oversight and management of FCA's primary social media channels and applications, to include moderation of comments.

7. **FCA Section 508 Coordinator**
   a. Provides Section 508 compliance of social media technologies.
   b. Reviews and approves developed social media applications.

WHERE TO GET ADDITIONAL INFORMATION

This issuance is intended to provide specific information on the official use of social media at FCA. For more information, contact the Assistant Director of OCPA.

Approved: /s/ Date: 08/18/2016

William J. Hoffman

Chief Operating Officer