FARM CREDIT ADMINISTRATION PRIVACY IMPACT ASSESSMENT

SYSTEM, PROGRAM, OR PROJECT NAME

Office of Inspector General (OIG) Tips and Complaints Web Intake Form

SYSTEM TYPE

Information Technology System or Capability

PURPOSE

The OIG Tips and Complaints Web Intake Form is used to capture investigative tips and complaints in support of the OIG's oversight mission. The form is hosted on the FCA's website www.fca.gov.

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): Other supplemental information deemed necessary and submitted by the complainant (in free text fields) such as those outlined in the narrative section of this assessment.	☒

LIFE CYCLE NARRATIVE

The Farm Credit Administration (FCA or "Agency") Office of Inspector General (OIG) is responsible for providing independent and objective oversight of FCA programs and operations. The OIG carries out this responsibility as authorized by and in accordance with the Inspector General Act of 1978, as amended, in part by conducting investigations of allegations of misconduct relating to the programs and operations of FCA. Investigations may address administrative, civil, and criminal violations of laws and regulations by any agency employee, contractor or consultant, or any person or entity involved in alleged wrongdoing relating to the FCA's programs and operations. The OIG receives tips and complaints about fraud, waste, or abuse related to FCA programs and operations from internal and external sources in-person and via email, telephone, and physical mail. Investigations may also be initiated as a result of information identified through other OIG activities.

In support of these efforts, the FCA OIG has developed an electronic, web-based intake form that allows individuals to submit tips or complaints via the FCA's website, www.fca.gov. Once submitted, the information is automatically transferred to a secure, internal database that serves as a repository for this information, which is made available to OIG staff for tracking and resolution via a custom application. Collectively, these capabilities are herein referred to as the OIG Tips and Complaints Web Intake Form. PII collected and processed by the OIG Tips and Complaints Web Intake Form varies by complaint or tip type but generally includes the following:

- Name (first and last), preferred email address, preferred phone number, organization, and mailing address of the submitter.
- Name (first and last), email address, phone number, organization, and mailing address of suspected wrongdoers.
- Name (first and last), email address, phone number, organization, and mailing address of other persons whom the submitter believes may be able to provide the OIG with information about the alleged wrongdoing.
- Association with the Farm Credit Administration.
- Self-description (i.e. FCA employees, FCA applicants, FCS employees or borrowers, employees of another Federal, State, or Local agency, etc.)
- Nature of the complaint or tip, including additional details,
- Whether the submission is related to another submission and details of the previous submission (if yes)

Where a tip or complaint serves as the basis for further review, those tips or complaints and associated documentation, as well as any resulting investigatory material, is managed in a dedicated site in the FCA's Microsoft SharePoint environment. That site, the OIG Complaints and Investigations system, is further discussed in a separate PIA. While the OIG Tips and Complaints Web Intake Form discussed in this PIA may feed, indirectly, information contained in the OIG Complaints and Investigations system, no direct connection exists between the two systems.

In addition to the data types outlined above, information in documents submitted as part of supporting documentation for a complaint or tip may contain PII about the individuals who are the subject of a complaint or tip, as well as information about individuals who have knowledge of or information pertaining to allegations of fraud, waste, and abuse as it relates to FCA programs and operations. Because of its law enforcement purpose, the documents may contain a broad range of PII elements including medical, biometric, financial, legal, employment, photographic, educational, and contact information about FCA employees, contractors, and others related to investigations. At present, these documents are submitted via email directly to an access-controlled OIG email inbox. Supplementing

documentation is not stored in the same database or made accessible through the associated internal interface; to the extent such documentation is submitted to the OIG, it is stored in the above-referenced OIG Complaints and Investigations system in the FCA's Microsoft SharePoint environment. Examples of common PII include but are not limited to:

- Names (first, last, middle)
- Information related to the complaint or investigation including details of any alleged fraud, waste, or abuse.
- Contact information, such as mailing address, phone number, and email address (home and work)
- Identifying numbers such as employee ID numbers, Social Security numbers, tax identification numbers, driver's license numbers, and similar
- Employment information, including title, position, and compensation.
- Information about the relationship between a complainant and the subject of a complaint, or a witness and a subject of investigation
- Information about existing actions being taken against the person or previous complaints or investigations.

The information collected is limited to that which the complainant chooses to share and which the OIG requires to investigate and (as necessary) conduct IG investigations. All information collection is voluntary, and submitters may choose to submit their tip or complaint anonymously or with in a way that allows for limited disclosure. Users who do not wish to submit information via the OIG Tips and Complaints Web Intake Form may still provide the FCA OIG with tips and complaints via alternative methods including email, phone, or physically (in person or by postal mail) as outlined at https://www.fca.gov/about/how-to-report-fraud-waste-and-abuse.

The OIG Tips and Complaints Web Intake Form is filled out by individuals who wish to file a complaint with the FCA OIG or otherwise alert (via tip) the OIG to potential fraud, waste, abuse, or criminal activity. This includes members of the public as well as internal FCA employees and contractors. To this end, information is collected from, but not limited to: current and former FCA employees, contractors and consultants, as well as current and former employees of other federal, state, and local agencies, employees of FCA-regulated institutions, and other persons and entities with knowledge of or information pertaining to allegations of fraud, waste, and abuse as it relates to FCA programs and operations, or with a relationship with FCA or the FCA OIG. In general, the information is collected from persons other than the subject of a complaint or tip. Because of the nature of information collected and its use, opportunities for notice and consent are limited. FCA has published this privacy impact assessment (PIA) and the applicable SORN, as well as a Privacy Act statement on the web form to mitigate risks related to notice and consent.

All collected information is subject to evaluation by OIG staff and verified against information collected from other records sources. As noted earlier, data collected may form the basis of, or add to, an investigation managed in the OIG Complaints and Investigations system. To that end, extracts of the data may be shared with other Agencies and law enforcement organizations to support ongoing investigations through a manual process and not an automatic system to system connection. The system does not support direct sharing or connection with other internal or external systems and no information sharing or similar agreements are in place.

Upon submission of a complaint or tip, information is temporarily held in a secured location within the FCA website environment pending transfer to the internal database that houses the information. Transfer happens through an automated, regularly scheduled process. Upon transfer, the information is wiped from the website. After OIG staff review a complaint or tip, they may choose to "archive" or "delete" a complaint or tip, based on internal business processes. In general, delete is reserved for those complaints deemed to be SPAM or unrelated to the FCA or the OIG's authorities. By archiving a complaint or tip, a copy of the record is saved for reference and Federal recordkeeping requirements in accordance with the applicable schedule(s).

Individuals who are the subject of a complaint or investigation may have limited opportunities to access, change, or update information included in the system in accordance with the Privacy Act and FCA's Privacy Act regulations, as outlined in 12 CFR part 603.

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 Office of Inspector General Complaints and Investigations System is covered by the Privacy Act system of records: FCA-7 – Inspector General Investigative Files – FCA, available at 85 FR 613550.
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 — 5 U.S.C. § 406(k) exempts Offices of Inspectors General from the requirements of the Paperwork Reduction Act, during the conduct of an audit, investigation, inspection, evaluation, or other review.
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 Records Schedule DAA-0103-2018-0001, available at: https://www.archives.gov/files/records-mgmt/rcs/schedules/independent-agencies/rg-0103/daa-0103-2018-0001_sf115.pdf.
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 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. ***NOTE:*** *FCA is in the process of transitioning all systems, including subsystems to 800-53, Revision 5.*
☒	The system has been reviewed for and assigned a categorization level in accordance with NIST Federal Information Processing Standards (FIPS) Publication 199 and NIST SP 800-60, and the senior agency official for privacy has approved the categorization. FIPS 199 Security Impact Category: Moderate
☒	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 Operate (ATO) and Date: 2/14/2023 ☐ 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. * *FCA employees undergo background checks.
☒	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

As described above, the OIG Tips and Complaints Web Intake Form consists of a public facing web form on FCA's website www.fca.gov and an internal database which delivers submitted information to an internal custom application. Access to the web form is available to anyone who visits fca.gov.

The internal database and custom application through which internal users access the submitted complaints and tips is part of the Agency's larger General Support System (GSS). Access to the system is limited to OIG employees and FCA Office of Information Technology (OIT) administrators and is managed as a single-sign-on experience, available to FCA employees only on FCA-issued laptops and connected to the FCA network. The FCA GSS is further discussed in a separate PIA.

FCA's GSS is categorized as a moderate system, and FCA's chief information officer (CIO) has granted the system an ATU. The agency secures information in the system using a variety of means, including the following:

- Physical security controls of FCA facilities and data centers that house GSS components
- Use of firewalls, intrusion detection and prevention systems and antivirus and other software and capabilities for detection of malware and other malicious threats
- Use of transport layer security connections and multifactor authentication
- Use of total disk encryption and other encryption methods for securing sensitive data, including PII
- Access controls and use of the principle of least privilege
- Application, network, server, and database activity logs, which are reviewed upon detection of abnormalities or upon request by the CIO or Chief Information Security Officer (CISO).

There are two types of users within the internal custom application which supports the OIG Tips and Complaints Web Intake Form:

- *Authorized OIG users of the Tips and Complaints Web Intake Form:* These are employees within OIG a need to know in support of their duties related to facilitating and documenting the conduct of oversight activities relating to programs and operations of the FCA, and/or reporting on the results of such activities.
- *Administrators (Office of Information Technology or "OIT" employees):* These are FCA staff responsible for managing the Agency's GSS environment, including its internal databases and custom applications. Administrators only access the database or application when requested directly by the Office of Inspector General to troubleshoot issues, modify existing capabilities or develop new capabilities.

Capabilities within the internal interface are limited to reading, printing, archiving, and deleting entries only. No editing of entries is permitted.

Annual access and permission reviews of FCA systems, including those on the GSS are carried out by OIT staff in coordination with representatives from the office of the designated system owner. There are also built-in auditing capabilities to monitor and track certain user activities within the internal interface. These capabilities mirror those native to the underlying database.

Formalized, documented policies and procedures exist for routing of, access to, use and disclosure of complaint and tip records. Additionally, a formal agreement exists between the IG and the FCA Chief Information Officer (CIO) providing that the CIO will ensure that only authorized personnel have access to OIG information as described above.

Finally, all FCA users receive annual IT security and privacy awareness training and are responsible for reviewing and attesting to the requirements outlined in FCA IT security and personal use policies and the Agency's Rules of Behavior (RoB).

PRIVACY RISK ANALYSIS

What follows is an overview of the primary risks associated with the OIG Tips and Complaints Web Intake Form and a description of corresponding mitigations put in place by the agency for each.

Data minimization: Because of its law enforcement purpose, the OIG Tips and Complaints Web Intake Form may collect a broad range of PII elements including medical, biometric, financial, legal, employment, photographic, educational, and contact information about FCA employees, contractors, and others related to tips or complaints or as the basis of a potential investigation. Information requested is limited to that which is required to evaluate complaints and tips received and determine if further investigative activities are warranted. Information that is beyond the scope of requirements for a potential investigation, or beyond the issues revealed in the investigation is not requested. All collected information is subject to evaluation by OIG staff for utility. Additionally, all information collection is voluntary and at the discretion of the submitter. Required fields are limited to name and a method of contact for those individuals who choose not to submit their complaint or tip anonymously. To further mitigate the risk associated with collecting large amounts of sensitive PII, the agency developed a centrally managed, access limited, and secure custom application to allow members of the OIG staff to review submissions, including any included documentation, reducing the risk that sensitive information could be unknowingly or mistakenly shared with individuals who are not authorized or otherwise do not have a need-to-know the information. Finally, the agency employs the appropriate technical, physical, and administrative controls to ensure the PII it does collect and maintain is secured from unauthorized access, use, disclosure, or destruction.

Data confidentiality, including access or use by unauthorized users: There is a risk that PII collected through the OIG Tips and Complaints Web Intake Form could be leaked or exposed, or that persons without a clearly defined need to know could gain access to and use of sensitive PII.

To reduce the risks of data loss, leaks, and unauthorized or unnecessary access and use, FCA uses a variety of technical and administrative controls to limit access to data it stores and processes on its network and in the OIG Tips and Complaints Web Intake Form and associated custom application, as outlined in the Administrative and Technological Controls Narrative section of this PIA.

Transparency: Because of its law enforcement purpose, the OIG Tips and Complaints Web Intake Form affords limited opportunities for notice to and consent by individuals whose PII may be collected. Information may not be collected directly from individuals; rather, PII is provided by an individual submitting a complaint or tip or acquired through submitted supporting documentation. Because information in the system is subject to the Privacy Act, notice of the collection of PII through the web form is provided by the applicable SORN and the associated Privacy Act Statement. FCA also has published this PIA to provide additional notice of the collection and use of PII in the system.

Overall risk: FCA recognizes the risk inherent in collecting and processing sensitive PII, both as individual data elements (such as SSNs) and contextually (as it relates to the subject of the complaint or tip, or a resulting investigation). Therefore, the agency developed a system which reduces the overall risks associated with collecting, using, and maintaining this information. The agency put controls in place to highly limit access to sensitive PII and the ability to edit, modify, or delete documents which contain complaint (and associated investigation) information by FCA OIG staff. Finally, the agency took steps to publish public notices — a SORN and this PIA — as well as a Privacy Act statement on the form itself, to be transparent about the collection and use of PII as it relates to the OIG's investigative process.

DOCUMENT CONTROL

Approval

/s/ Wesley Fravel, FCA Privacy Officer	/s/ Jeannie Shaffer, CISO

/s/ Wendy Laguarda, Inspector General	/s/ Jerry Golley, CIO and SAOP

Change Control and Approval History

Version	Date	Change Summary
V 1.0	1/16/2024	Initial Version