FARM CREDIT ADMINISTRATION
PRIVACY IMPACT ASSESSMENT

SYSTEM, PROGRAM, OR PROJECT NAME

Office of Inspector General (OIG) Complaints and Investigations System

SYSTEM TYPE

Information Technology System or Capability

PURPOSE

The OIG Complaints and Investigations System is used to document the conduct and outcome of investigations, tips and complaints received, and actions taken, and to maintain other records related to the OIG's activities.

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	☒

Personally Identifiable Information (PII) Element(s)	Included
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 by the complaint, witnesses, or OIG staff in support of the investigation or as part of the complaint, such as relationships between two parties, etc.	☒

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 involving 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, an electronic web-based intake form, telephone, and physical mail. Investigations may also be initiated as a result of information identified through other OIG activities.

The OIG manages complaints and tips received, as well as any resulting investigations, in a dedicated site in the FCA's Microsoft SharePoint environment. Microsoft SharePoint (SharePoint) is a commercial off-the-shelf web-based application that integrates with Microsoft Office to provide enhanced communication and collaboration features. SharePoint is an application that falls within a larger information system: FCA's IT Infrastructure System. Through SharePoint, OIG staff can more easily share documents, collaboratively edit documents, and create document libraries. SharePoint also offers other administrative management features, such as workflows – pre-programmed applications that streamline and automate business processes, such as document approval or signature. FCA has set up a variety of SharePoint sites customized for individual Agency offices and teams and for business processes undertaken by those offices and teams.

The OIG SharePoint site, herein referred to as the OIG Complaints and Investigations system, is one such site. The system is made up of subsites, each consisting of a set of standardized document libraries and folder types containing a variety of document and file types related to a specific complaint or investigation. Documents may be generated within SharePoint via workflows and collaboration or obtained from outside of SharePoint and loaded into a particular library or folder. This system contains documents relating to:

- Investigative activities
- Internal staff memoranda
- Copies of subpoenas issued, affidavits, witnesses' statements, transcripts and recordings of testimony taken, and accompanying exhibits
- Documents and records obtained from governmental or non-governmental sources, or copies thereof
- Interview notes, investigative notes, staff working papers, draft materials, and other investigative documents or records
- Investigative plans, progress reports, and closing reports
- Other documents and information relating to the investigation of alleged or suspected criminal, civil, or administrative violations or similar wrongdoing relating to FCA programs and operations

A variety of internal forms are also available within the system. These forms are filled out by OIG staff as part of the complaints and investigation management process. Finally, some folders or documents may have workflows associated with them such as document approval or signature.

Information in documents included in the system includes PII about the individuals who are the subject of a complaint or investigation, 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 system 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. 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, and similar used to confirm identities of individuals or to facilitate certain law enforcement requests
- Employment information, including title, position, and employer
- Information about the relationship between a complainant and the subject of a complaint, or a witness and a subject of an investigation
- Information about existing actions being taken against the person or previous complaints or investigations
- Any other supplemental information deemed necessary by OIG staff in support of the investigation or as part of the complaint.

The system may also contain information collected through discovery and stored for case management and legal research functions.

Information in the OIG Complaints and Investigations System is collected from a variety of sources, including, 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. Some information may be collected directly from persons who are the subject of a complaint or investigation, however, most information is generally collected from persons other than the subject of the complaint or investigation. All information included in the system is input directly by OIG staff only. Because of the nature of records in the system, opportunities for notice and consent are limited. FCA has published this privacy impact assessment (PIA) and the applicable SORN to mitigate the risk related to notice and consent.

The information collected is limited to that which is required to evaluate complaints received and conduct IG investigations, and to refer any potential violations that are revealed throughout the course of reviewing a complaint or investigating, as necessary. Information that is beyond the scope of a complaint or investigation completed, or beyond the issues revealed in the complaint or investigation is not requested.

All collected information is subject to evaluation by OIG staff and verified against information collected from other records sources. Extracts of the data may be shared with other Agencies and law enforcement organizations to support ongoing investigations and to facilitate external qualitative assessment reviews of the OIG by those organizations. In both cases, data sharing is 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.

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. Additionally, the Inspector General Act of 1978, as amended, 5 U.S.C. app. § 6(j) provides that computerized comparisons performed by an Inspector General, or by an agency in coordination with an Inspector General, when conducting an audit, investigation, inspection, evaluation, or other review are not to be considered a matching program.
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.
☒	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 Use (ATU) and Date: 8/27/2020 ☐ 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 Complaints and Investigations System consists of a dedicated SharePoint site with subsites made up of standardized folders, templates, and workflows. The SharePoint site is part of the Agency's larger SharePoint environment, with access to the system limited to OIG employees. SharePoint access is managed as a single-sign-on experience, available to FCA employees only on FCA-issued laptops and connected to the FCA network. The SharePoint environment and the associated network and access management solution are part of the Agency's General Support System (GSS).

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 OIG Complaints and Investigations System:

- *Authorized OIG users of the Complaints and Investigations System:* These are employees within with OIG a need to know in support of their duties related to facilitating and documenting the conduct of investigative 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 and SharePoint environment. Administrators only access the site when requested directly by the Office of Inspector General to troubleshoot issues, modify existing capabilities or develop new capabilities. Certain members of OIG staff have elevated permissions within the SharePoint environment which allow them to perform certain maintenance functions, reducing the overall amount of access necessary by OIT employees.

Annual access and permission reviews of OIG Complaints and Investigations System are carried out by OIT staff in coordination with representatives from OIG. There are also built-in audit logs to monitor and track reads (who accessed a document), writes (who created a new document or modified an existing document), and deletes (who removed a document or documents or a folder). These logs are checked regularly to ensure that the system is accessed appropriately.

Formalized, documented policies and procedures exist for routing of, access to, use and disclosure of investigative 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.

PRIVACY RISK ANALYSIS

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

Data confidentiality, including access or use by unauthorized users: The primary risk associated with the OIG Complaints and Investigations system is the possibility that sensitive PII 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 Complaints and Investigations system as outlined in the Administrative and Technological Controls Narrative section of this PIA. By centrally managing documents related to a particular investigation or complaint in a central, access managed location with auditing and versioning capabilities, the Agency reduces the risk that sensitive information in associated documentation could be unknowingly or mistakenly shared with individuals who are not authorized or otherwise do not have a need-to-know the information.

Transparency: Because of its law enforcement purpose, the OIG Complaints and Investigation system and the investigative process, in general, afford 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 existing records or external record sources. Because information in the system is subject to the Privacy Act, notice of the collection of PII through the OIG investigative process is provided by the applicable SORN. FCA also has published this PIA to provide additional notice of the collection and use of PII in the system.

Data minimization: Because of its law enforcement purpose, the OIG Complaints and Investigations system contains 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. Information requested is limited to that which is required to evaluate complaints received and conduct IG investigations, and to refer any potential violations that are revealed throughout the course of the investigation. Information that is beyond the scope of requirements for the investigation, or beyond the issues revealed in the investigation is not requested. All collected information is subject to evaluation by OIG staff for utility. To mitigate the risk associated with collecting large amounts of sensitive PII, the agency developed a centrally managed, access limited, secure repository for housing documents related to a particular investigation or complaint reducing the risk that sensitive information in associated documentation could be unknowingly or mistakenly shared with individuals who are not authorized or otherwise do not have a need-to-know the information. Further, the agency employs the appropriate technical, physical, and administrative controls to ensure the PII it does collect and maintain is secured.

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 investigation or the violation). Therefore, the agency developed a system which reduces the the overall risks associated with collecting 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 investigation and complaint information by FCA staff. Finally, the agency took steps to publish two public notices — a SORN and this PIA — 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	6/28/2022	Initial Version
V 1.1	1/31/2024	Update to authority references and Paperwork Reduction Act to align with amended Inspector General Act; Updates to reflect how information is collected, including web-based form and removal of references to facsimile.