Privacy Impact Assessment (PIA)

Farm Production and Conservation (FPAC)

Foreign Programs System (FPS)

Revised: June 2021

Template Version: FPAC-PIA-2013-08-19

Document Information

System Owner Contact Information	
Name	Sieg, Angela
Contact Number	816-926-1568
E-mail Address	Angela.Sieg@usda.gov

Document Revision History		
Date MM/DD/YYYY	Author Name & Organization	What was changed?
03/04/2014	Charlene Niffen – ISO	Initial creation
10/14/2014	Matthew Knechtel – ISO	Initial consolidated PIA
05/02/2018	Darren Smith – ISO	Portfolio realignment
06/09/2021	Gordon Moore – FPS	CY21 update

Document Review				
Reviewer	Title	Date	Update: Y/N	If systemic, please provide comments
Jacques Tournoy	A&A Analyst	3/19/21	Y	Updated doc for CY21 renewal

Table of Contents

Purpose of Document

USDA DM 3515-002 states: “Agencies are responsible for initiating the PIA in the early stages of the development of a system and to ensure that the PIA is completed as part of the required System Life Cycle (SLC) reviews…” and “New systems, systems under development, or systems undergoing major modifications are required to complete a PIA.”

This document is being completed in accordance with NIST SP 800-37 Rev 1 which states, “The security plan also contains as supporting appendices or as references to appropriate sources, other risk and security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, incident response plan, and continuous monitoring strategy.”

Abstract

Name of the component and system: Foreign Programs System (FPS)

Brief description of the system and its function: The Foreign Programs System (FPS) provides automated systems for program administration and financial management of CCC’s Export Credit Guarantee programs and the Public Law 480 Title I & Title III programs. Using the online GSM applications, FAS and FPAC users can process and track agreements, deliveries, fees, foreign bank limits, subsidies, payments, commodities, assignments, defaults, claims, and collections owed to CCC. The Automated Public Law 480 Umbrella System (APLUS) provides an automated method to enter, update, and extract data for current and planned budgets; original, amended and rescheduled agreements; purchase authorizations and sales, which includes letters of commitments and vessel approvals; disbursements for commodities and ocean transportation; and collections of repayments from foreign governments.

Why the PIA is being conducted: To support federal law, regulations and policies.

System Information

System Information	
Agency:	Farm Production and Conservation (FPAC)
System Name (Acronym):	Foreign Programs System (FPS)
System Type:	☒ Major Application ☐ General Support System ☐ Non-major Application
System Categorization (per FIPS 199):	☐ High ☒ Moderate ☐ Low
Who owns this system? (Name, agency, contact information)	Angela Sieg FPAC-BC/ISD/ISSDOB/FSS U.S. Department of Agriculture Farm Production and Conservation – Business Center 6501 Beacon Drive Kansas City, MO 64133 816-926-1568 angela.sieg@kcc.usda.gov
Who is the security contact for this system? (Name, agency, contact information)	Brian Davies Information Systems Security Program Manager (ISSPM) USDA/ FPAC-ISD-IAB-CS 1400 Independence Avenue SW Washington, D.C. 20250 (202) 720-2419 Brian.Davies@usda.gov
Who completed this document? (Name, agency, contact information)	Jacques Tournoy, A&A Analyst U.S. Department of Agriculture Farm Production and Conservation – Business Center 6501 Beacon Drive Kansas City, MO 64133 816-651-1416 Jacques.Tournoy@usda.gov

Overview

- **System Name:** Foreign Programs System (FPS)

- **System Description:** The Foreign Programs System (FPS) provides automated systems for program administration and financial management of CCC's Export Credit Guarantee programs and the Public Law 480 Title. Using the online GSM applications, FAS and FPAC users can process and track agreements, deliveries, fees, foreign bank limits, subsidies, payments, commodities, assignments, defaults, claims, and collections owed to CCC. The Automated Public Law 480 Umbrella System (APLUS) provides an automated method to enter, update, and extract data for current and planned budgets; original, amended and rescheduled agreements; purchase authorizations and sales, which includes letters of commitments and vessel approvals; disbursements for commodities and ocean transportation; and collections of repayments from foreign governments. Externally, GSM sends information on a quarterly basis to the U.S Department of Treasury. The information does not contain PII, it is budget related information dealing with subsidy. The reports produced for FSA (now FPAC-BC) deal with accounting, fees, subsidy, and application activity. There is no PII involved. APLUS generates reports for the State Department, Congress, and embassies. There is no PII in the reports generated by APLUS.

  The applications of which FPS is comprised were previously ATO'd under General Sales Manager Export Credit Guarantee System (GSM) and Automated Public-Law-480 Title I Umbrella System (APLUS). Characteristics of the GSM require it to be included in this Privacy Impact Assessment (PIV) but the APLUS system will be excluded.

Applications	Overview
GSM	System Purpose: The General Sales Manager Export Credit Guarantee System (GSM) tracks agreements between the US exporter, the US financial institution, the foreign banks, and the foreign importers, to sell, export, buy, finance, and pay for US commodities exported to countries participating in the Commodity Credit Corporation Export Credit Guarantee programs. GSM monitors CCC obligations, maintains accounting records, and produces reports for USDA Farm Service Agency (FSA) and the Foreign Agricultural Service (FAS). • General System Description: GSM feeds information to the CORE general ledger system. It allows external users (US Banks and Exporters) to access the on-line application via the Internet to enter and review their own program information. GSM produces files nightly for uploading to the GSM Data Mart for creation of EPM11 canned reports and running of ad hoc reports/queries by end users for posting to the Internet. In addition, the system produces financial and program system reports for internal users via the Intranet and for the Treasury Department via FSA and

	Commerce Department via FAS. The application’s mission is to provide reporting of financial and GSM-102 program data to the FPAC Financial Management Division (FMD) and to provide application operational support for FAS. • Typical Transaction: GSM monitors CCC obligations, maintains accounting records, and produces reports for USDA Farm Service Agency (FSA) and the Foreign Agricultural Service (FAS) • Information Sharing: N/A • Module & Component Description: GSM – Internal - Web application for Announcements, Agreements, Deliveries, and Payment Schedules functionality. • Legal Authority to Operate: The Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule or technology being developed.

1.1 What information is collected, used, disseminated or maintained in the system?

Applications	Information is collected, used, disseminated or maintained in the system.
GSM	Point of contact names, email addresses, and phone numbers for exporters, US financial institutions, importers, and foreign banks. Tax identification number and payment bank information for exporters and US financial institutions. Names and business email addresses for USDA employees and contractors who are users of the GSM system

1.2 What are the sources of the information in the system?

Applications	Sources of information in the system.
GSM	Exporters, US Financial Institutions, Importers and Foreign Banks that participate in the Program.

1.3 Why is the information being collected, used, disseminated or maintained?

Applications	Why information being collected, used, disseminated or maintained.
GSM	The information collected is required to provide export credit guarantees for exporters and US financial institutions participating in Commodity Credit Corporation export guarantee programs. These programs can require the payment of claims and the pro-rata disbursement of recoveries to these participating organizations.

1.4 How is the information collected?

Applications	How information collected.
GSM	Data is collected from exporters and US and foreign financial institutions. These entities can enter and review only their specific program information through the public interface of the GSM application.

1.5 How will the information be checked for accuracy?

Applications	How information is checked for accuracy.
GSM	When data was initially entered in the applications it was validated for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and then again when any required updates are made.

1.6 What specific legal authorities, arrangements and/or agreements defined the collection of information?

Applications	Legal authority to collect information.
GSM	Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigate.

Applications	Privacy risks and how mitigated.
GSM	The privacy risks are moderate. The minimum amount of personally identifiable information is collected to satisfy the purpose of this system. The risks are mitigated using various control mechanisms. See below: • All users must be uniquely identified and authenticated prior to accessing the application. • Access to data is restricted.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

Applications	Uses of information.
GSM	Using the online GSM applications, FAS and FPAC users can process and track agreements, deliveries, fees, foreign bank limits, subsidies, payments, commodities, assignments, defaults, claims, and collections owed to CCC. The data is used for recording and monitoring CCC obligations, accounting records and reports for USDA (FAS &FSA), Treasury, and Commerce departments. External users can review their program information. Nightly files are used by the GSM data warehouse team and its users to create (as of COB) ad hoc EPM11 queries/reports, and for the GSM data warehouse system to produce EPM11 canned reports that are posted to the intranet for use by FAS and FSA. Reports are for internal use only by Government employees and contractors; however, the reports generated from the system are submitted to auditors, Department of Treasury, Department of State, etc.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Applications	Tools used to analyze data and what type of data produced.
GSM	No additional “tools” (other than the application and database itself) are used to analyze the data.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Applications	Why and how commercial or publicly available data is used.
GSM	The system does not use commercial or public data. DUNS number, reporting to USA Spending. Excluded party list, verify that listed parties do not do business in GSM

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Applications	Controls in place to ensure information is handled in accordance with the above described uses.
GSM	Access to the system and data are determined by business need and individual roles. Controls are in place to provide reasonable assurance that data integrity and confidentiality are maintained during processing. Controls in place to ensure the correct handling of information include the following: • End users are correctly identified and authenticated according USDA and

	FPAC) security policies for access managements, authentication and identification controls, 2) Audit logging is used to ensure data integrity.
	•

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

Applications	Time information is retained?
GSM	The information is retained indefinitely (permanent records).

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Applications	Retention period approved by component records officer and National Archives and Records Administration (NARA)?
GSM	Yes, in accordance with USDA Directive DR 3080-001: Appendix A: Scheduling Records.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Applications	Risks associated with the length of time data is retained and how those risks are mitigated.
GSM	During this period, the stored information may be at risk for viewing by unauthorized parties, data loss or destruction and non-availability. Access to computerized files are protected by access control software, physical access controls and if warranted, password protected. SORN USDA/FPAC-2 States: Program documents are destroyed within 6 years after end of participation. However, FPAC is under a records freeze. According to Records Management DR3080-001 Disposition of Inactive Records: Records and other documents that are no longer sufficiently active to warrant retention in office space shall be removed as rapidly as possible by: (a) transfer to a Federal Records Center, or (b) transfer to a records retention facility meeting the requirements of 36 CFR Chapter 12, Subchapter B Records

	Management, Subpart K, 1228.224 through 1228.244, or (c) if authorized, by disposal. (See Appendix B – Records Disposition Procedures.)

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Applications	Internal organization(s) in which information is shared, what information is shared and for what purpose?
GSM	N/A

4.2 How is the information transmitted or disclosed?

Applications	Information transmittal / disclosure.
GSM	N/A

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Applications	Privacy risks associated with the sharing and how they were mitigated.
GSM	N/A

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Applications	External organization(s) is the information shared, what information is shared, and for what purpose?
GSM	No application information is being shared outside of the USDA environment.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Applications	External PII sharing compatibility and SORN coverage, or legal mechanisms by which system is allowed to share PII.
GSM	N/A

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Applications	Externally shared information and security measures.
GSM	N/A

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Applications	External sharing privacy risks and mitigation.
GSM	N/A

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Applications	Individual notice prior to collection of PII information.
GSM	Yes

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Applications	Individual's right to decline to provide PII information?
GSM	Yes. FPAC Privacy Policy states that "Submitting information is strictly voluntary."

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Applications	Individual's right to consent to uses of PII and how exercised.
GSM	Yes, in accordance with FPAC Privacy policy and the individual's written consent.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Applications	Notice to individuals and unawareness risk mitigation.
GSM	The risk is considered moderate. Notification is automatically provided in the system of records notice (Federal Register publication): SORN: USDA/FPAC–2 - Farm Records File (Automated) and USDA/FPAC-14 - Applicant/Borrower.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Applications	Individuals access to PII procedures.
GSM	As published in SORN USDA/FPAC-2 and SORN USDA/FPAC-14: "An individual may obtain information about a record in the system which pertains to such individual by submitting a written request to the above listed System Manager. The envelope and letter should be marked ``Privacy Act Request." A request for information should contain: Name, address, ZIP code, name of the system of records, year of records in question, and any other pertinent information to help identify the file."

7.2 What are the procedures for correcting inaccurate or erroneous information?

Applications	Correction of erroneous information procedures.
GSM	As published in SORN USDA/FPAC-2 and SORN USDA/FPAC-14: "Individuals desiring to contest or amend information maintained in the system should direct their request to the above listed System Manager, and should include the reason for contesting it and the proposed amendment to the information with supporting information to show how the record is inaccurate. A request for contesting records should contain: Name, address, ZIP code, name of the system of records, year of records in question, and any other pertinent information to help identify the file."

7.3 How are individuals notified of the procedures for correcting their information?

Applications	How individuals notified of correction procedures.
GSM	Formal redress is provided via the FPAC Privacy Act Operations Handbook.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Applications	Alternatives available to individual if no redress.
GSM	N/A

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Applications	Privacy risks associated with redress and risk mitigation.
GSM	The risk associated with redress is considered low, as the public does not have

	access to the system or the data. While the public cannot access the system to update or change their personal information, they may update their information using from AD 2530 and submit to the appropriate FPAC official. The FPAC official will in turn update the system based on the information provided. There is work going on for Customer Self Service which will be public facing. SCIMS is no longer the source of entry since Business Partner was implemented in December 2014.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

Applications	Access procedures and documentation.
GSM	FSA-13-A is used to request user access to USDA and FPAC information technology systems including specifying authorization for accessing the system. (Refer to Notice IRM-440) In addition, access to FPAC web applications is gained via an on-line registration process similar to using the FSA-13- A form. For system specific detailed access see SSP.

8.2 Will Department contractors have access to the system?

Applications	Contractor access.
GSM	Department contractors do have access to the System.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Applications	User privacy training.
GSM	Once hired, privacy training and security awareness training is completed prior to gaining access to a workstation. The privacy training addresses user's responsibilities to protect privacy data and how to protect it.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Applications	Certification & Accreditation.
GSM	, but the most recent was completed 6//18/2018

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Applications	Auditing measures and technical safeguards.
GSM	Most GSM database tables maintain history of all updates with identifier of who or what updated the data. Any logging and auditing of access, transactions or output is left to the OCIO-ITS, and eAuthentication Application.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Applications	Privacy risks identified and risk mitigation.
GSM	The main risk associated with privacy is the exposure to unauthorized access to privacy information. This risk is considered moderate. Mitigating controls are in place to ensure privacy risks are minimal. Mitigated controls are mapped back to SSP in CSAM. Annual access reviews are done to ensure controls are mitigated.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

Applications	Project / System type.
GSM	Major Application

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

Applications	Technology privacy risks.
GSM	No

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Applications	SO and/or ISSPM review of Web guidance.
GSM	Yes, no 3rd party website (hosting) or 3rd party application is being used.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

Applications	Purpose of 3rd-party websites and/or applications?
GSM	N/A

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

Applications	PII availability through 3rd-party websites and/or applications.
GSM	N/A

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

Applications	Use of PII available through 3rd party websites and/or applications.
GSM	N/A

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

Applications	Maintenance and security of PII available through 3rd party websites and/or applications.
GSM	N/A

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

Applications	Periodic purging of PII available through 3rd party websites and/or applications.

GSM	N/A

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

Applications	Access to PII available through 3rd party websites and/or applications.
GSM	N/A

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

Applications	Internal / external sharing of PII available through 3rd party websites and/or applications.
GSM	N/A

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

Applications	SORN requirements for sharing of PII available through 3rd party websites and/or applications.
GSM	N/A

10.10 Does the system use web measurement and customization technology?

Applications	Web measurement and customization technology.
GSM	N/A

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

Applications	User rights for web measurement and customization technology.
GSM	N/A

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

Applications	3rd party websites and/or applications privacy risks and mitigation.
GSM	N/A

Appendix A. Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the Foreign Programs System (FPS)

ANGELA SIEG

Digitally signed by ANGELA SIEG
Date: 2021.06.11 10:52:18 -05'00'

Angela Sieg
FPAC/FPS Information System Owner

Date

BRIAN DAVIES

Digitally signed by BRIAN DAVIES
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=BRIAN DAVIES, 0.9.2342.19200300.100.1.1=12001000000604
Date: 2021.06.11 15:23:59 -04'00'

Brian Davies
Information Systems Security Program Manager

Date

Amber K. Ross

Digitally signed by AMBER ROSS
Date: 2021.06.14 10:21:19 -05'00'

Amber Ross
FPAC Privacy Officer

Date