Federal Supply Services-19 (FSS-19)

Privacy Impact Assessment (PIA)

April 30, 2021

POINT *of* CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Instructions for GSA employees and contractors:

This template is designed to help GSA employees and contractors comply with the E-Government Act of 2002, Section 208. GSA conducts privacy impact assessments (PIAs) for electronic information systems and collections in accordance with CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. The template is designed to align with GSA business processes and can cover all of the systems, applications, or projects logically necessary to conduct that business.

The document is designed to guide GSA Program Managers, System Owners, System Managers, and Developers as they assess potential privacy risks during the early stages of development and throughout the system, application, or project's life cycle.

The completed PIA shows how GSA builds privacy protections into technology from the start. Completed PIAs are available to the public at gsa.gov/pia.

Each section of the template begins with a statement of GSA's commitment to the Fair Information Practice Principles (FIPPs), a set of eight precepts that are codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. Please note the instructions, signatory page, and document revision history table will be removed prior to posting the final PIA to GSA's website. **Please send any completed PIAs or questions to gsa.privacyact@gsa.gov.**

Stakeholders

Name of Information System Security Manager (ISSM):

- Richard Banach. Email:richard.banach@gsa.gov

Name of Program Manager/System Owner:

- Mark Zenon. Email:mark.zenon@gsa.gov

Signature Page

Signed:

DocuSigned by:
Richard Banach
21B998D30FCE4B6...

Information System Security Manager (ISSM)

DocuSigned by:
Mark Zenon
AEF52C607EA9404...

Program Manager/System Owner

DocuSigned by:
Richard Speidel
171D5411183F40A...

Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third-party services and robotics process automation (RPA)	2.0
6/26/2018	New question added to Section 1 regarding Information Collection Requests	2.1
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
11/5/2018	Removed Richard's email address	2.3
11/28/2018	Added stakeholders to streamline signature process and specified that completed PIAs should be sent to gsa.privacyact@gsa.gov	2.4
4/15/2019	Updated text to include collection, maintenance or dissemination of PII in accordance with e-Gov Act (44 U.S.C. § 208)	2.5
9/18/2019	Streamlined question set	3.0
2/20/2020	Removed email field from signature page	3.1

05/05/2020	Initial content for FSS-19 by Shobitha Nandi	V1.0
04/12/2021	Updates based on Privacy Office comments	V1.1

Table of contents

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan (SSP) for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technical, and managerial perspective?

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

Document purpose

This document contains important details about GSA IT FISMA System ***Federal Supply Services (FSS-19)***. To accomplish its mission GSA IT must, during COMET program (CIO Modernization Enterprise Transformation), collect personally identifiable information (PII) about the people who use such products and services. PII is any information [1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.[2]

A. System, Application, or Project Name:

FISMA Application Name: Federal Supply Services (FSS-19)
Sub Application handling PII and PCI

Sub System Name/Module	PII data elements	PCI DSS data
FSS 19 PR module	TIN or SSN	NA
Pegasus Connect	NA	CC#
OCMS	TIN or SSN, Full Name, Address and Phone Number	NA
EDI Gateway	NA	CC#

B. System, application, or project includes information about:

Sub System Name/Module	PII Category of People	PCI DSS Category of People
FSS 19 PR module	Vendor	NA
Pegasus Connect	NA	Vendor
OCMS	Vendor	
EDI Gateway	NA	Vendor

C. For the categories listed above, how many records are there for each?

As of May 2020

Sub System Name/Module	PII Records count	PCI DSS Records count
FSS 19 PR module	~4.2M	
Pegasus Connect	NA	
OCMS	~421	
EDI Gateway	NA	

D. System, application, or project includes these data elements:

Sub System Name/Module	PII data elements	PCI DSS data
FSS 19 PR module	TIN, SSN	
Pegasus Connect		CC#
OCMS	TIN, Full Name, Address, Phone Number, Contractor Data	
EDI Gateway		CC#

Overview

Application	Description
FSS-19 PR Module	
Purpose	FSS-19 is a collection of mainframe Work Flow Language (WFL) scripts that run on the Clearpath Unisys mainframe for the principal data processing of the FSS-19 System. Many of these modules work with other FSS-19 sub-applications to provide the data interaction functionality for user interfaces (such as FSS On-line, eFSSOnline, etc.) FSS-19 Modules are implemented via the WFL scripts. The FSS-19 PR (Procurement) module automatically processes orders from the OP module (Purchase Orders) and sends all Federal Acquisition Service (FAS) Awards data to Federal Procurement Data System (FPDS). Also provides support to maintain Contract Writing System, maintain Industrial Funding Fee (IFF) Sales Records, and generate Multiple Award Schedule (MAS) and IFF Management Reports.

Description of PII	FSS-19 processes sensitive data including Financial information and PII. As FSS-19 processes TIN for payees and payees can be individuals, some SSN information would be included, which is PII (in the PR module for use by OCMS). Financial information can include vendor financial account information and agency payment, budget, and AR data in the PR, OP, PM, and Finance modules. Other sensitive information includes contract data, proprietary vendor information, and contract performance data in the PR module.
Handling of PII (Collection, Use & Destruction)	FSS-19 PR module uses the DMS II database on the Unisys plus mainframe hosted in the Clearpath data center. It relies on the Clearpath Hosting Center for many inherited or hybrid security controls. Covered under **SORN ID GSA/GOVT-9** for SAM (System Awards Management).

Application	**Description**
On-Line Contract Management System (OCMS)	
Purpose	A web-based, internal facing application used by the Contracting Officer (CO) community to primarily manage post contract-award administration and compliance reporting through main software functions: Contract Management, Subcontracting, Off-Ramping, Complaint Investigation (CI), Industrial Funding Fee (IFF) Claims, Risk-Based Assessment and Contractor Report Card (RBA), Action Items (AI), Pre-Award Assessment Report (PAR), Supply Report Card (SRC). OCMS also has scheduled jobs that send Sales/Payment/Subcontracting Reminders and Delinquency Notifications via the GSA Email servers based on defined business rules.
Description of PII	OCMS includes sensitive information including Financial information, proprietary vendor information, and PII. OCMS includes TIN for payees and payees can be individuals, some SSN information would be included. Other PII would include Full Name, Work Address (which is likely the same as Home Address for some small business vendors), email address, Other sensitive information includes contract data, complaint information and "Report Card" (which could affect a vendor's reputation if released), and contract performance investigation data.
Handling of PII(Collection, Use & Destruction)	OCMS is deployed in the Clearpath data center and relies on the Clearpath Hosting Center for many inherited or hybrid security controls. The FSS-19 Database used by OCMS encrypts the TIN field with AES-256

Application	Description
EDI Gateway	
Purpose	The Federal Acquisition Streamlining Act (FASA) of 1994 requires the Government to evolve its acquisition process from one driven by paper to an expedited process based on electronic commerce/electronic data interchange (EC/EDI). EDI improves business processes (e.g., procurement, finance, logistics) into a fully electronic environment by automating vendor/GSA electronic communication
Description of PII	EDI Gateway processes Financial information and PII. This includes credit card numbers. Other sensitive information includes proprietary vendor information.
Handling of PII(Collection, Use & Destruction)	EDI Gateway is located in the EIO data center and relies on the EIO Hosting Center for many inherited or hybrid security controls The EDI Gateway performs a number of essential functions to ensure that all inbound and outbound EC/EDI/cXML/FAX transactions are processed, mapped, translated, archived, and forwarded to their correct destinations in a timely fashion. EDI Gateway uses Gentran Integration Suite (GIS), which is a product that allows trading partners (e.g. vendors) to transmit data via various protocols, such as SFTP, SCOPY, HTTP, HTTPS, AS2 and XML via GIS to allow Government buyers (GSA and client agencies) to conduct business with federal vendors

Application	Description
Pegasys Connect (PC)	
Purpose	Pegasys Connect (PC) is a financial component of GSA’s Billing and Accounts Receivable (BAAR) solution. Pegasys Connect provides transformation and validation of various financial transactions between Pegasys (GSA) and Pegasys (USDA).
Description of PII	Pegasys Connect processes Sensitive data, including Financial information and PII. PC contains agency Credit Card numbers, which are financial information and PII. Other Financial information includes agency Accounts Receivable information.
Handling of PII(Collection, Use & Destruction)	The Pegasys Connect (PC) software that is part of FSS-19 consists of 2 components supported by an extensive framework and Application Programming Interface (API) responsible for the provision of core financial services. These components are Pegasys Connect (PC), which is a collection of batch facilities operating on the GSA Unisys Mainframe to process and delivery financial transaction information

	to the United States Department of Agriculture's (USDA's) financial system and Pegasys Connect Rejection and Invalid Transaction Handling (PC R&ITH) which allows authorized GSA users to correct the transactions that were returned by USDA Pegasys. PC handles the resubmission of corrected transactions, as part of handling Billing and Inventory transactions for General Supplies and Services (GS&S) and Billing transactions for Telecom/Information Technology Category (ITC). PC R&ITH Online functionality is available via an internal Web Interface with no external users. PC R&ITH has been developed using Java/JBoss/Spring framework and uses PC DMSII database with DMSQL as the middle tier. Pegasys is located in the ClearPath data center and relies on the ClearPath Hosting Center for many inherited or hybrid security controls.

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?

1. The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.
2. Agreements with external agencies are listed in the following table:

FSS-19 Subsystem/Module	***External Agency***	**Agreement Type (ISA, MOU/PBA)**
FSS19	DLA	PBA
EC/EDI Gateway	DLA - GEX	PBA
FSS19	FEDLOG - outgoing.	MOU
FSS19	USPS - incoming to GSA	ISA
Pegasys Connect	USDA	ISA

FSS19	USCG	ISA

1.2 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information?

Sub System Name/Module	Is PII information searchable
FSS 19 PR module	Records are retrievable by searching against information in the record, including, but not limited to, the person's or entity's name, SSN and TIN. Searching for vendor records by TIN is limited to Federal Government users. Covered under **SORN ID** **GSA/GOVT-9** for SAM (System Awards Management). This system collects entity legal business name/sole proprietor's entity email address, entity telephone number, entity Taxpayer Identification Number (TIN), and entity address. In the case of a sole proprietor, tax laws allow them to use their Social Security Number (SSN) as their TIN if they do not have a separate Employer Identification Number (EIN)
OCMS	Covered under **SORN ID** **GSA/GOVT-9** for SAM (System Awards Management). This system collects entity legal business name/sole proprietor's entity email address, entity telephone number, entity Taxpayer Identification Number (TIN), and entity address. In the case of a sole proprietor, tax laws allow them to use their Social Security Number (SSN) as their TIN if they do not have a separate Employer Identification Number (EIN)

1.3 Has an Information Collection Request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

Not applicable. Information is collected by the sam.gov system and relies on that system for any approvals.

1.4 Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

There is no records retention schedule specifically for FSS-19. FSS-19 will follow the records schedules for enterprise IT systems outlined in GRS 03.1/020 and GRS 03.2/010

GRS 03.1/020 Information Technology Operations and Maintenance DAA-GRS-2013-0005-0004. Information technology operations and maintenance records. Information Technology Operations and Maintenance records relate to the activities associated with the operations and maintenance of the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Includes the activities associated with IT equipment, IT systems, and storage media, IT system performance testing, asset and configuration management, change management, and maintenance on network infrastructure.

Temporary. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.

GRS 03.2/010 Systems and Data Security Records. DAA-GRS-2013-0006-0001 Systems and data security records.
These are records related to maintaining the security of information technology (IT) systems and data. Records outline official procedures for securing and maintaining IT infrastructure and relate to the specific systems for which they were written. This series also includes to analysis of security policies, processes, and guidelines, as well as system risk management and vulnerability analyses.

Temporary. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls though out the life of the system.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects, maintains, uses or disseminates as well as how it protects and shares it. It provides straightforward ways for individuals to learn how GSA handles PII.

2.1 Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

Sub System Name/Module	**Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.**
FSS 19 PR module	NA. The collection of PII is collected outside of the application via application programming interface. The vendor is notified via the registration site sam.gov
OCMS	NA. The collection of PII is handled outside of the application via application programming interface. The vendor is notified via the registration site sam.gov

SECTION 3.0 DATA MINIMIZATION

GSA limits PII collection only to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Why is the collection and use of the PII necessary to the system, application, or project?

The FSS-19 set of applications, supports government wide contracts with commercial companies that provide access to millions of commercial products and services at fair and reasonable prices to the government. The application makes buying easy and efficient with the use of modern technology to connect government buyers and industry. The collection of PII is critical to the mission for vendor identification, notification and payment collection purposes. For more details see Overview section.

3.2 Will the system, application, or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

Sub System Name/Module	Will the system, application, or project create or aggregate new data about the individual? If so, how will this data be maintained and used?
FSS 19 PR module	NA. No new data is aggregated
OCMS	NA. No new data is aggregated

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?

Sub System Name/Module	Will the system, application, or project create or aggregate new data about the individual? If so, how will this data be maintained and used?
FSS 19 PR module	NA. No new data is consolidated
OCMS	NA. No new data is consolidated

3.4 Will the system monitor the public, GSA employees, or contractors?

Not Applicable. The system does not monitor the public, GSA Employees, or contractors in any capacity.

3.5 What kinds of report(s) can be produced on individuals?

Not Applicable. The system does not produce any reports on vendors.

3.6 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

Not Applicable. The system does not produce any reports on vendors.

SECTION 4.0 LIMITS ON USING AND SHARING INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?

Individuals and or businesses register to do business with the Government. FSS-19 contains records including the entity legal business name, entity email address, entity telephone number, entity Taxpayer Identification Number (TIN), and entity address. In the case of a sole proprietor, tax laws allow them to use their Social Security Number (SSN) as their TIN if they do not have a separate Employer Identification Number (EIN).
See GSA SORN SAM **GSA/GOVT-9**

4.2 Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations? If so, how will GSA share the information?

Yes. Data is shared with other federal agencies.

FSS-19 Subsystem/Module	***External Agency***	**Agreement Type (ISA, MOU/PBA)**
FSS19	DLA	PBA
FSS19	FEDLOG - outgoing.	MOU
FSS19	USPS - incoming to GSA	ISA
FSS19	OMS	Unknown
FSS19	USCG	ISA

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

The information **is not** collected directly from individuals. The information is collected through the GSA SAM (System for Awards Management)

4.4 Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA? If so, who and how? Is a formal agreement(s) in place?

For internal breach or suspected breach of PII, the process outlined in the applications IRP is executed. For breaches with external agencies, the process outlined in the MOA, ISA or MOU is executed.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?

Accuracy and completeness of vendor information collected is handled by the registration module in sam.gov. Entity-entered TINs are validated by the IRS to ensure the TIN and Taxpayer Name provided matches the TIN and name control on file with the IRS. For completeness system validation rules ensuring required fields are populated correctly are in place. A record cannot be completed without all mandatory fields being completed.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application, or project? What is the authorization process to gain access?

The FSS 19 access controls are summarized in the table below.

Application	Role	Internal or External	Sensitivity Level	Authorized Privileges and Functions Performed
FSS-19	FSSUser	Internal	Moderate	Access to FSS-19 Database as a user. Access to Mainframe equates to default access to all databases with read access. FSSUser has only read access to FSS-19 databases.
(Pegasys Connect) R&ITH	Administrator	Internal	Moderate	Authorized Privileges: (Privilege) Approves requests to provide view or update functions for Application Users. Administrators are GSA Branch Chiefs and GSA Project Managers Functions Performed: There are only two functions: 1) to approve requests for application users and 2) on a need basis run or schedule Pegasys reference load.
(Pegasys Connect) R&ITH	Application User	Internal	Moderate	Authorized Privileges: (Non Privilege Role). Once a user is authenticated and gets access to the application, Application User performs different business functions that are internal and specific to application business needs. Users are Global Supply and Services and Telecom. Functions Performed: User can view, correct and resubmit rejected transaction records.

OCMS	Application User	Internal	Moderate	Authorized Privileges: (Non-Privilege). Once a user is authenticated and gets access to the application, Application User performs different business functions that are internal and specific to application business needs. GSA Contracting Officers, Office of Acquisition Management, GSA Project Manager gets Application User Accounts. Functions Performed: Users primarily manage post contract-award administration and compliance reporting such as create subcontracting plans and reports, perform complaint investigations, create Claims Reports, perform and create Risk based assessment, perform Pre-Award Assessments and create specific Action Items.
EDI Gateway	EDI User Administrator	Internal	Moderate	Authorized Privileges: (Privilege) Grants access to other EDI User Administrators Functions Performed: Performs essential functions to ensure that all inbound and outbound EC/EDI/cXML/FAX transactions are processed, mapped, translated, archived, and forwarded to their correct destinations in a timely fashion.
EDI Gateway	Fax User Administrator	Internal	Moderate	Authorized Privileges: (Privilege) Create other Fax User Administrators and perform business functions. Functions Performed: Fax Administrator can start services, check logs and monitor health.

6.2 Has GSA completed a System Security Plan (SSP) for the information system(s) or application?

Yes – FSS-19 was granted ATO July 12 2019.

6.3 How will the system or application be secured from a physical, technical, and managerial perspective?

The Eagan environment that houses the FSS-19 system has technical and physical security protections required for a FISMA Moderate system. The environment technical and physical and controls are detailed in the ClearPath SSP.

The Technical controls that are documented in the FSS-19 SSP:

- Identification and Authentication
- Access Controls
- Event auditing
- Encryption at rest and transport
- Vulnerability Scanning and Remediation

The FSS-19 FISMA system has Managerial controls that are documented in the FSS-19 SSP and on the FSS-19 Google Team Drive.

- Security Training
- User access request procedures
- Annual user recertification
- Audit Review, Analysis, and Reporting
- Security Assessments
- Incident Reporting and Incident Response Plan

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

The FSS 19's System Owner and Information System Security Officer are responsible for oversight and management of the Application's security and privacy controls. All authorized users are responsible for immediately reporting any suspected loss, compromise, unauthorized access or disclosure of data from the system in accordance with the GSA rules of behavior and IT Security policies.

The FSS 19 Incident Response Plan outlines the steps and procedures to execute in the event any PII was lost, stolen or inappropriately accessed.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2 What procedures allow individuals to access their information?

Sub System Name/Module	PII Category of People	Description
FSS 19 PR module	Vendor	The FSS 19 sub system is an internal application and does not offer such functionality(opt-in or opt-out) to the individuals
OCMS	Vendor	The OCMS sub system is an internal web application and does not offer such functionality(opt-in or opt-out) to the individuals

7.3 Can individuals amend information about themselves? If so, how?

Sub System Name/Module	PII Category of People	Description
FSS 19 PR module	Vendor	The vendor cannot modify their information. The FSS 19 sub system is an internal application and does not offer amend functionality
OCMS	Vendor	The vendor cannot modify their information. The OCMS sub system is an internal web application and does not offer amend functionality

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.

Individual (employees and contractors) with access to PII under the FSS-19 program have to complete the following training.

- “IT Security Awareness and Privacy Training 101” training within 30 days of employment.
- “IT Security Awareness and Privacy 101” training annually.
- Specialized Privacy Training 201 for managers/supervisors who work with PII as part of their duties.

GSA IT produces a report to identify individuals who have not taken the training and ensure the training is completed by everyone.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system owner ensure that the information is used only according to the stated practices in this PIA?

The System Owner reviews and approves the responses documented against the controls related to PII in the Application's System Security Plan (SSP).

The controls that align to the stated practices in this PIA and map the NIST PII controls are outlined under Chapter 13 of the FSS 19 System Security plan.

1. Access Control
2. Audit and Accountability
3. Identification and Authentication
4. Media Protection; Planning
5. Risk Assessment
6. System and Communications Protection;

In addition the System Owner also ensures that controls in the SSP are validated by a third party who will audit the technical and policy safeguards, which include the PIA, ensure that information is used appropriately.

FSS-19 completed an external financial audit conducted by third party KPMG in Sep 2019.

[1] OMB Memorandum Preparing for and Responding to the Breach of Personally Identifiable Information (OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.