Privacy Impact Assessment

Financial Reporting Improvements and Optimization (FRIO)

- Version: 1.0
- Date: November 13, 2019
- Prepared for: SDA OCIO TPA&E

United States Department of Agriculture

Privacy Impact Assessment for the

Financial Reporting Improvements and Optimization (FRIO)

November 13, 2019

Contact Point
Martina Sims
Financial Reporting Improvements and Optimization (FRIO)
(202) 720-3614

Reviewing Official
Arianne Perkins
Emmanuel Olufotebi
Privacy Office
United States Department of Agriculture

Revision History

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
0.1	09/18/2019	Robin Wagner	Document Creation
1.0	11/13/2019	Robin Wagner	ATO

Abstract

This Privacy Impact Assessment is being conducted since FRIO was identified during the Privacy Threshold Assessment as using Personally Identifiable Information (PII).

Financial Reporting Improvements and Optimization (FRIO) eliminates all the manual data manipulation and download efforts by obtaining and organizing data from the source system for easy management and reporting. In the FRIO application, roles and permissions are set so users can selectively access application features and data. In addition, FRIO helps to reduce manual errors and provide reliable and efficient reporting.

FRIO is a centralized reporting and data management application for the financial data of Food Safety and Inspections Services (FSIS) branch of the United States Department of Agriculture (USDA). FRIO supports budget allocation, forecasting, what-if analysis, and execution monitoring for all FSIS program areas. The system also features a multitude of administrative features, like user management, organization management, and meta data management.

FRIO is not used by the public or non-Federal entity.

Overview

FRIO is a centralized reporting and data management application for the financial data of Food Safety and Inspections Services (FSIS) branch of the United States Department of Agriculture (USDA). FRIO supports budget allocation, forecasting, what-if analysis, and execution monitoring for all FSIS program areas. The system also features a multitude of administrative features, like user management, organization management, and meta data management.

FRIO is an application that runs on the Platform as a Service (PaaS) Digital Infrastructure Services Center (DISC) Enterprise Cloud Platform (ECP) System housed in the DISC facility located in Kansas City, MO. The PaaS DISC/ECP System is a General Support System (GSS) that hosts multiple applications. The GSS was designed specifically to offer hosting services to DISC customers to enable them to take advantage of cloud computing. PaaS and DISC/ECP system enables DISC customers to take advantage of virtualization of their computing environments. FRIO is, therefore, protected by the physical and environmental controls that are attributed to this DISC facility.

- FRIO is not available to the general public; it is only available to those with access to the PaaS and DISC/ECP and with an e-Authentication (e-Auth) username and password.
- FRIO is not located in a harsh environment that would be detrimental to the hardware or to the system's performance and availability.
- There are 9 roles in FRIO. The key role is the Administrator. The functionality they are responsible for include:
- FRIO is a new application, and as such, this is the initial ATO process.

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?

The following data is collected, used, disseminated or maintained in the system:

- FMMI Alloc. Execution data: which contains financial execution records for FSIS with the fields - Business Area, Fiscal Year, Sgl Account, Fund, Fund Description, Fm Budget Period, Functional Area, Functional Area Name, Funded Program, Funded Program Description, Fund Center, Fund Center Description, Commitment Item, Orig .Auth, Undist. Appro., Undist Appor, Budg. Auth., Commitments, Obligations, Expenditures, Disbursement, Total Cmts. Oblg., Availauth.

- FMMI Payroll data: which contains financial payroll records for FSIS with fields – Business area Key, L01 Fund Key (Not Compounded), Fund Name, Budget Period Key, Functional Area Key, Functional Area Medium Name, L01 Funded Program Key (Not Compounded), Funded Program Long Name, L01 Fund Center Key (Not Compounded), Funds Center Name, PACS Type Emp Key, PACS Pay Plan Key, PACS Grade Key, L01 Commitment item Key (Not Compounded), Commitment Item Name, PACA Pp Cd Key, L01 Fiscal year Key (Not Compounded), Posting period Key, Amount PACS, Pay hours PACS.

- User Entered Data: Fiscal Year Allocations, OPM Data, Resource Management data, various BOC Hierarchies, Organization Hierarchies and other manually entered data.

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

Following are the sources of information in the system:

- FMMI system: Although, FRIO does not directly interact with FMMI to load the source data, 'FRIO reads CSV files (FMMI Alloc. Execution data and FMMI Payroll Data mentioned in 1) from the FMMI SFTP server and imports the data into the database. This process is scheduled to run nightly. The nightly loader is configured as an OpenShift cronjob, which creates pods according to the cron schedule and spins them down when there are no more files to load. The Program/Business area has scheduled an automated load from the source file system - FMMI into the SFTP server that runs nightly as well and drops the source files in to the folder before the FRIO nightly loader runs.

- User Entered Data: This data is all data that is manually entered/configured in the system by users themselves.

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

The information being collected, used, disseminated, or maintained is used to generate various financial reports for the users based on their needs/requirements.

1.4 How is the information collected?

The information is collected in the following ways:

- FMMI system: Although, FRIO does not directly interact with FMMI to load the source data, 'FRIO reads CSV files (FMMI Alloc. Execution data and FMMI Payroll Data mentioned in 1) from the FMMI SFTP server and imports the data into the database. This process is scheduled to run nightly. The nightly loader is configured as an OpenShift cronjob, which creates pods according to the cron schedule and spins them down when there are no more files to load. The Program/Business area has scheduled an automated load from the source file system - FMMI into the SFTP server that runs nightly as well and drops the source files in to the folder before the FRIO nightly loader runs.

- User Entered Data: This data is all data that is manually entered/configured in the system by users themselves.

1.5 How will the information be checked for accuracy?

Information is checked for accuracy, by validation of business rules, functional/technical requirements through testing procedures established by Harmonia. Harmonia conducts its own Quality Assurance Testing to make sure accuracy of information/data, which is compared against the business rules that have been shared and signed off by the business team. Accuracy of information is also validated and verified by end users during User Acceptance and IV&V testing before each release.

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

The authorities for USDA to collect, maintain, use and disseminate information through this system are: 5 U.S.C.301 (government organization and employees); Title 5 USC 552a (Records Maintained on Individuals (Privacy Act)); Title 41 CFR 201-6.1 (Federal Information Resources Management Regulation); 44 U.S.C.3101 (Records Management); OMB Circular No. A-108 (Responsibilities for the Maintenance of Records About Individuals by Federal Agencies); OMB Circular No. A-130 (Management of Federal Information Resources, Appendix 1, Federal Agency Responsibilities for Maintaining Records About Individuals); and Authorization to Operate (ATO), dated 22-07-14.

In addition, USDA is generally authorized to collect information to support its mission under: Title 7, Chapter 55-2205 (7 U.S.C 2204) (which authorizes the Secretary of Agriculture to collect information and employ any sampling or other statistical method deemed appropriate); 21 U.S.C. 679c(a)(1)-(3) (which expressly authorizes the Secretary to give high priority to enhancing the ability of FSIS to conduct its mission); the Federal

Meat Inspection Act (FMIA) (21 U.S.C. 601, et seq.), the Poultry Product Inspection Act (PPIA) (21 U.S.C., et seq.), the Egg Products Inspection Act (EPIA) (21 U.S.C. 1031, et seq.), and the Humane Methods of Livestock Slaughter Act of 1978 (7 U.S.C. 1901-1906).

1.7 Privacy Impact Analysis:

Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated. As FRIO reports display financial data pertaining to different Programs and Divisions under FSIS, users had to be restricted to only view/edit data based on their hierarchy and organization (Program/Division). Additionally, users had to be restricted based on the functions they perform in each agency. Thus, two levels of permission were established in FRIO:

1. Data Level Permission – (Program Level User or Division Level User) This permission controls which Program/Division's data the user can view/edit. This permission is attached to the user.
2. Page Level Permission – Report pages to which the role may have access. This permission is attached to a role, which may be assigned to a user.

Additionally, only users whose FRIO registration request is approved may access FRIO. This is facilitated through E-Auth authentication using LincPass. A registration request has to be approved by a FRIO Administrator for a user to gain access to FRIO. The registration request itself has two sets of permissions mentioned above – Organization Request (grants data level permission) & Role Request (grants page level permission). FRIO Administrator has the mandate to authorize or reject requests.

There is no PII in the source data for FRIO.

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.

The information being collected, used, disseminated, or maintained is used to generate various financial reports for the users based on their needs/requirements

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

FRIO is a customized solution built for FSIS that integrates various commercial off-the-shelf software and custom code:

Business Function Served	Tool Employed
Storing and retrieving data (Database)	PostgreSQL 9.6
Reporting and Analytics	JQuery DataTables (https://datatables.net), Python
User Interface	Python Programming with Django 1.11 framework, HTML 5, CSS 3 and Java Script 6

PostgreSQL 9.6: The data storage and retrieval for FRIO is handled by a PostgreSQL database. The database holds source flat files, processed data from FMMI, user inputs, user class information, and audit tables, and hosts the FRIO staging area. The complete list of data management activities and data specifications are documented in the FRIO Data Management Plan.

JQuery DataTables: JQuery DataTables is a framework that allows easy display of tabular data. FRIO's API and Web interfaces will pass data to the javascript and DataTables will display it.

The users can export the financial reports generated in FRIO in Excel and PDF.

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

FRIO does not use any commercial or publicly available data.

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.

The controls detailed in Section 1.7 address these risk issues specifically.

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?

Currently, all the information is retained in FRIO database indefinitely.

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

No, but FSIS has an overarching data retention policy that has been approved by NARA. Please see FSIS Directive 2620.1, *Records Management Program*.

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

The length of time data is retained does not affect the type or level of risk. The controls outlined in Section 1.7 provide ongoing privacy protection to the data.

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?

The information is shared internally between the following Programs and Divisions as of 11/07/2019:

1. Programs:
    1) AGENCY COST - GRANTS TO STATES
    2) AGENCY RELOCATION
    3) AGENCY SERVICES
    4) CIVIL RIGHTS DIVISION
    5) EEO SETTLEMENTS
    6) FEME DISASTER (ODIFP)
    7) FSIS AGENCY LEVEL
    8) GREENBOOK, WORKING CAPITAL & CENTRAL CHARGES
    9) INTERNAL AFFAIRS
    10) INTERNATIONAL COORDINATION
    11) OFFICE OF THE ADMINISTRATOR
    12) OFFICE OF THE CHIEF FINANCIAL OFFICER
    13) OFFICE OF THE CHIEF INFORMATION OFFICER - AGENCY IT & NO-YEAR
    14) OFFICE OF THE CHIEF INFORMATION OFFICER - OPERATING
    15) OFFICE OF EMPLOYEE EXPERIENCE AND DEVELOPMENT
    16) OFO (FIELD)
    17) OFFICE OF FIELD OPERATIONS (HEADQUARTERS)
    18) OFFICE OF INVESTIGATION, ENFORCEMENT AND AUDITS
    19) OFFICE OF MANAGEMENT
    20) OFFICE OF PUBLIC AFFAIRS AND CONSUMER EDUCATION
    21) OFFICE OF PLANNING AND ANALYSIS AND RISK MANAGEMENT
    22) OFFICE OF PUBLIC HEALTH SCIENCES
    23) OFFICE OF POLICY & PROGRAM DEV

24) SPECIAL PROJECTS
25) STUDENT PROGRAM

2. Divisions:
    1) Agency Cost - GTS - Main
    2) Agency Services
    3) Agency Settlements
    4) CRS
    5) FEME Disaster (ODIFP) - Main
    6) FIT - Special Projects
    7) FSIS Agency Level
    8) GB / WCF / CC
    9) IA
    10) Import Field Offices
    11) OA - OAA
    12) OCFO - ALFAD
    13) OCFO - BD
    14) OCFO - FOD
    15) OCFO - FSC
    16) OCFO - Main
    17) OCIO - Agency IT & NY - Main
    18) OCIO - BSC
    19) OCIO - CEC
    20) OCIO - GQAD
    21) OCIO - IOD
    22) OCIO - ISC
    23) OCIO - OCTO
    24) OCIO - Operating - Main
    25) OCIO - PGC
    26) OCIO - PMD
    27) OEED - CFL
    28) OEED - EERS
    29) OEED - Main

30) OEED - OEDB
31) OEED - TMB
32) OEED - TOB
33) OEED - TTDLS
34) OFO - Alameda District
35) OFO - Albany District - Closed
36) OFO - Atlanta District
37) OFO - Beltsville District - Closed
38) OFO - Chicago District
39) OFO - Dallas District
40) OFO - Denver District
41) OFO - Des Moines District
42) OFO (Field)
43) OFO - Import Inspection Division (Closed)
44) OFO - Jackson District
45) OFO - Lawrence District - Closed
46) OFO - Madison District - Closed
47) OFO - Minneapolis District - Closed
48) OFO - OAA
49) OFO - Philadelphia District
50) OFO - Raleigh District
51) OFO - REGOPS
52) OFO - RMPS
53) OFO - RMS
54) OFO - Springdale District
55) OFO - Strategic Planning
56) OIC
57) OIEA - ARMD
58) OIEA - CID
59) OIEA - ELD
60) OIEA - EOB
61) OIEA - FSAB

62) OIEA - HAB
63) OIEA - IAB
64) OIEA - LEPB
65) OIEA - Main
66) OIEA - MCAD
67) OIEA - MCG
68) OIEA - NRO
69) OIEA - RMAAB
70) OIEA - SRO
71) OIEA - SWRO
72) OIEA - WRO
73) OM - HR
74) OM - HRM
75) OM - HRO
76) OM - LERD
77) OM - Main
78) OM - OAS
79) OPACE - CPAO
80) OPACE - ECIM
81) OPACE - FOIA
82) OPACE - FSES
83) OPACE - Main
84) OPACE - WDC
85) OPARM - DAS
86) OPARM - IDAS
87) OPARM - Main
88) OPARM - RMICS
89) OPARM - SPES
90) OPHS - AES
91) OPHS - EALS
92) OPHS - EL
93) OPHS - EL CHEM

94) OPHS - EL MB
95) OPHS - EL PATH
96) OPHS - FERN
97) OPHS - LQAS
98) OPHS - Main
99) OPHS - ML
100) OPHS - ML CHEM
101) OPHS - ML MB
102) OPHS-NACMF
103) OPHS - RAAS
104) OPHS - RPMS
105) OPHS - SS
106) OPHS - WL
107) OPHS - WL CHEM
108) OPHS - WL MB
109) OPPD - IEPDS
110) OPPD - IES
111) OPPD - LPDD
112) OPPD - Main
113) OPPD - PAS
114) OPPD - PDD
115) OPPD - PID
116) OPPD - RMD
117) Regulatory Operations
118) Relocation
119) Resource Management and Financial Planning Staff
120) Strategic Planning and Operations Management Staff
121) Student Program

The following data is collected, used, disseminated or maintained in the system:

- FMMI Alloc. Execution data: which contains financial execution records for FSIS with the fields - Business Area, Fiscal Year, Sgl Account, Fund, Fund Description, Fm Budget Period, Functional Area, Functional Area Name, Funded Program, Funded Program Description, Fund Center, Fund Center Description, Commitment Item, Orig .Auth,

Undist. Appro., Undist Appor, Budg. Auth., Commitments, Obligations, Expenditures, Disbursement, Total Cmts. Oblg., Availauth.

- FMMI Payroll data: which contains financial payroll records for FSIS with fields – Business area Key, L01 Fund Key (Not Compounded), Fund Name, Budget Period Key, Functional Area Key, Functional Area Medium Name, L01 Funded Program Key (Not Compounded), Funded Program Long Name, L01 Fund Center Key (Not Compounded), Funds Center Name, PACS Type Emp Key, PACS Pay Plan Key, PACS Grade Key, L01 Commitment item Key (Not Compounded), Commitment Item Name, PACA Pp Cd Key, L01 Fiscal year Key (Not Compounded), Posting period Key, Amount PACS, Pay hours PACS.

- User Entered Data: Fiscal Year Allocations, OPM Data, Resource Management data, various BOC Hierarchies, Organization Hierarchies and other manually entered data.

The information being collected, used, disseminated, or maintained is used to generate various financial reports for the users based on their needs/requirements.

4.2 How is the information transmitted or disclosed?

As FRIO reports display financial data pertaining to different Programs and Divisions under FSIS, users had to be restricted to only view/edit data based on their hierarchy and organization (Program/Division). Additionally, users had to be restricted based on the functions they perform in each agency. Thus, two levels of permission were established in FRIO:

1. Data Level Permission – (Program Level User or Division Level User) This permission controls which Program/Division's data the user can view/edit. This permission is attached to the user
2. Page Level Permission – Report pages to which the role may have access. This permission is attached to a role, which may be assigned to a user.

Information is transmitted or disclosed through different financial reports in FRIO to users based on the above permissions assigned to them.

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.

Refer to section 1.7.

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?

Information is not shared with organizations external to the USDA.

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.

FRIO does not share PII outside of the Department.

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

Should FRIO information need to be shared externally, departmental guidelines for providing information to such organizations will be followed. This includes the redacting of PII, unless the information is required under law.

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

As long as employee PII data is transmitted externally, there is the risk that it may be disclosed to unauthorized individuals.

Under normal operating circumstances, employee PII is not shared externally. Such information would only be provided if required by law. Standard FSIS or USDA guidelines for protecting the information would be followed.

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 Does this system require a SORN and if so, please provide SORN name and URL.

FRIO does not require a SORN.

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

Yes. Notice is provided to the individual prior to collection of any information, in accordance with USDA Memorandum Minimum Safeguards for Protecting Personally Identifiable Information (PII) for all Source System users. The user is told prior to system access that entering their name is a requirement of working on the system; therefore, the user is notified.

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

Yes. However, because collection of the information is a requirement to access FRIO, if they decline, they cannot work on the FRIO system.

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

The individual is made aware of their right to consent to particular uses of the information; however, because collection of the information is a requirement to access FRIO, if they decline the particular use of their information, they cannot work on the FRIO system.

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

The user is told prior to system access that entering their name is a requirement of working on the system; therefore, the user is notified.

As users enter the data themselves or see the data in the system, there is no lack of awareness, and thus, no risk.

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?

Individuals who have reason to believe that this system might have records pertaining to them should write to the FSIS FOIA office.

FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 2166, 1400 Independence Avenue, SW Washington, DC 20250-3700 - Phone: (202) 720-2109 - Fax (202) 690-3023 – E-mail: fsis.foia@usda.gov.

For more information about how to make a FOIA request, please see:

http://www.fsis.usda.gov/wps/portal/footer/policies-and-links/freedom-of-information-act/foia-requests

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

This information is provided to the individual when presented with the two notices identified in Section 7.3 below, and should contact the system owner.

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

Before providing information, the individual is presented with a Privacy Act Notice and an explanation of the Notice, on both the USDA Memorandum Minimum Safeguards for Protecting Personally Identifiable Information (PII).

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

N/A. Formal redress is provided. See 7.2 above.

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

The risk is that a user might share personal contact data of another user with someone who does not have authority to have that information. FRIO users are routinely provided privacy reminders and take part in annual security awareness training to mitigate that risk.

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?

Only users whose FRIO registration request is approved may access FRIO. This is facilitated through E-Auth authentication using LincPass. A registration request has to be approved by a FRIO Administrator for a user to gain access to FRIO. The registration request itself has two sets of permissions mentioned in 1.7 – Organization Request (grants data level permission) & Role Request (grants page level permission). FRIO Administrator has the mandate to authorize or reject requests.

8.2 Will Department contractors have access to the system?

Yes. Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel experts in such matters.

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

Users are required to undergo Computer Security Awareness Training annually as a condition of continued access to the FSIS systems.

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

No. This is the initial Authority to Operate (ATO) for FRIO.

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

The system is designed to limit incorrect data in the system and to limit access to data overall. The system also includes management, operational, technical controls, and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors. See section 1.7 for more information on controls.

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?

No serious privacy risks could be identified. It is not possible to retrieve records using PII. The scope of the information collected is small. All of the FRIO staff has received training on the importance of safeguarding PII. Privacy risks are mitigated through annual training.
Overall, the privacy risk in this system is low. FRIO has further mitigated the risks by granting access only to authorized personnel. Further, all USDA employees have undergone a background investigation and contractor access is governed by contracts identifying rules of behavior for USDA and FSIS systems and security.

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?

FRIO is a major application.

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

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"?

Yes. Both M-10-22 and M-10-23 have been reviewed by the SO and ISSPM.

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

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

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?

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

If so, is it done automatically?

N/A - Third party websites are not being used.

If so, is it done on a recurring basis?

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

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?

N/A - Third party websites are not being used.

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)?

N/A - Third party websites are not being used.

10.10 Does the system use web measurement and customization technology?

No.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

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?

N/A.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

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.

N/A - Third party websites are not being used.

Responsible Officials

Martina Simms
System Owner
1400 Independence Ave SW Rm 2151-S
Washington, DC 20250

Elamin Osman
Chief Information Security Officer
1400 Independence Ave., SW
Washington, DC 20250

Bajinder Paul, PMP
Chief Information Officer
1400 Independence Ave., SW
Washington, DC 20250

Arianne Perkins
Emmanuel Olufotebi
Privacy Office
Room 1142, South Building
Washington, DC 20250

Approval Signatures

Agreed: MARTINA SIMMS Digitally signed by MARTINA SIMMS Date: 2019.11.13 15:58:24 -05'00'

_____ _____

Martina Simms — Date

System Owner

Agreed: _____ _____

Elamin Osman — Date

Chief Information Security Officer

Agreed: _____ _____

Bajinder Paul — Date

Chief Information Officer

Agreed: _____ _____

Emmanuel Olufotebi — Date

Privacy Officer