Privacy Impact Assessment

for

NRE FS e-Collections Retail System (NRE FS ERS)

Policy, E-Government and Fair Information Practices

Version: 1.0

Date: February 4, 2022

Prepared for: USDA FS CIO

Contact Point

Anstienette Sharpe

System Owner

USDA NRE Forest Service

703-605-5199

Reviewing Official

Cynthia Towers

Privacy Officer

USDA NRE Forest Service

386-301-4060

Abstract

The Privacy Impact Assessment (PIA) addresses the USDA Natural Resources and Environment (NRE), Forest Service (FS), e-Collections Retail System (ERS) (NRE FS ERS). The primary objective of NRE FS ERS is to reduce the collection of currency and paper checks at FS Over-the-Counter (OTC) locations by providing and encouraging electronic payment alternatives. The PIA is being conducted because name, address, signature, and financial data on the paper check will be collected in NRE FS ERS.

Overview

NRE FS ERS is a Major Application owned by the United States (US) Forest Service (FS). The mission of this system is to automate Over the Counter (OTC) sales transactions performed throughout the FS, reduce the collection of currency and paper checks, and encourage electronic payment alternatives. The system accepts as input basic sales transaction information including price, product identifiers, and payment information. Payment from a customer can take the form of cash, paper check, or credit cards. Credit card and paper check processing occurs in near real-time if there is an active internet connection. Information from the credit card transactions is sent at the time of payment to Worldpay for payment authorization. Paper check transactions, including check images, are sent nightly via batch process to the US Treasury required Over-the-Counter Channel (OTCnet) system.

When a customer pays with a credit card, assuming that the system is online (i.e., connected to the FS network), a request for credit card authorization is sent to Worldpay. If the card is valid, the bank will return an authorization code approving the transaction. If the card is not valid, no code will be returned, and the payment will be rejected in NRE FS ERS. If the customer does not have another valid form of payment, the transaction is cancelled.

ERS connects to the following:

FS End User Computing Environment (FS EUCE) General Support System (GSS) where NRE FS ERS point of sale (POS) components reside.

Forest Service Computer Base – Network (FSCB NW): GSS that serves as a transmission medium for NRE FS ERS POS components to NRE FS ERS Microsoft D365 Commerce in Microsoft Azure Cloud datacenter.

USDA Financial Management Modernization Initiative (FMMI): FMMI is the Department's financial system of record and all NRE FS ERS collection-related transactions are recorded in FMMI. A Memorandum of Understanding (MOU) between the USDA and FS is in place to address the information sharing between NRE FS ERS and FMMI. There is no direct connection

between NRE FS ERS and FMMI. Data file transfer using Secure File Transfer Protocol (SFTP) is submitted and retrieved from the FMMI designated file location.

USDA Authentication System: The ERS D365 Retail Headquarters users are authenticated using USDA Enterprise Active Directory (EAD) federation and ERS Settlement and Reporting (ERS-SR) module users are authenticated to the application, which is hosted in MS Azure Commercial Cloud, using e-Authentication (eAuth). Both authentication mechanisms comprise the programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals, bind those identities to credentials that may serve as a proxy for the individual in access transactions, and leverage the credentials to provide authorized access to an agency's resources. A separate MOU between USDA and FS regarding the use of the Department-mandated authentication system is in place.

Department of the Treasury's Collection Information Repository (CIR): CIR is the system used by the Treasury to show transactions that have been cleared and deposited. NRE FS ERS utilizes information from CIR to settle deposits with collections.

Two Department of the Treasury-specific banks: Federal Reserve Bank of Cleveland (FRBC) and Comerica Bank. The Department of the Treasury has mandated that the FS use FRBC and Comerica Bank to process paper checks and credit card transactions, respectively. A MOU outlining the agreement between the FS and the Department of the Treasury is already in place.

Azure Dynamics 365 Commercial is a Software as a Service (SaaS) offering from Microsoft that is hosted in Azure Commercial Cloud.

All FS-specific customizations needed to implement check batch processing, check settlement, credit card settlement, cash deposit management, FRBC integration, Pay.gov integrations, Collections Information Repository (CIR) integration, and Financial Management Modernization Initiative (FMMI) file import/export are implemented by Network Specialty Group, Inc. (NSG) outside of the Microsoft Dynamics 365 Retail product. The information from the individual sales transaction is sent at the time of processing to the ERS Retail Channel Database (DB) and subsequently to ERS Retail Headquarters. These transactions are then transmitted to the ERS-SR application. The Reconciliation and Settlement module submits electronic check transactions to OTCnet and performs settlement activities for each transaction and prepares an account posting file that will be transmitted to FMMI.

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 Identification

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

NRE FS ERS collects payments in the form of cash, check and/or credit card from public users (customers) who purchase products and/or services from the FS. Most of the time, a paper check has customer information printed on the check including name, address, bank account information, and signature. NRE FS ERS stores check images temporarily to submit them with additional sales transaction information to OTCnet for further processing. For credit cards, the FS Collection Officer confirms the name on the credit card by viewing a valid government ID while accepting payment. Credit card data is securely transmitted to the Treasury-designated bank/processor (Worldpay) for authorization. Upon successful payment authorization, partial card number, authorization code, and card expiration date are stored in NRE FS ERS.

1.2 Source

What is the source(s) of the information in the system?

The sources of the data is from payments made by customers using cash, credit cards, and/or paper checks. No customer information is requested as part of payment using cash, credit card, and/or paper check except when customers make payments using checks which may have printed Personally Identifiable Information (PII) (name, address, bank routing and account number). Paper check images with bank routing and account numbers are stored in NRE FS ERS temporarily and submitted to a Treasury designated system for further payment processing.

1.3 Justification

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

NRE FS ERS collects and disseminates PII information to process payments received from customers in the form of credit card and paper check. In case of payments made using cash, no PII is collected or stored.

NRE FS ERS POS terminals with a Europay, MasterCard, and Visa (EMV) device process credit card transactions directly with Worldpay and provide only the obfuscated credit card numbers with the first five digits and last four digits as well as the payment authorization code and credit card expiration date to ERS, which is stored in NRE FS ERS for follow-on settlement activities.

Customer name, address, bank routing and account number, and signature on the paper checks are present on the check if a customer is making payment for goods and services using a paper check. ERS stores Magnetic Ink Character Recognition (MICR) code, routing and account number, check number, and check image so that it can be transmitted to the financial institution selected by the Department of the Treasury for processing via an encrypted channel. An electronic image of the check is stored in NRE FS ERS and is accessible by authorized users only and cannot be modified. All information is used to collect payments owed to the Government.

1.4 Collection

How is the information collected?

Credit cards are inserted in the EMV device by the customer to make payments and are removed once the payment is authorized. Credit card information and the payment amount is sent directly to the Treasury-selected credit card processor for authorization. Obfuscated credit card numbers are collected from the electronic data stored on the magnetic strip found on the back of the credit card or within the electronic chip on the front of the card. Partial card information is stored in NRE FS ERS (data which is not PII).

Paper checks may be provided to FS Collection Officers and/or submitted in the fee tubes at various collection points throughout the FS. These checks are scanned using the RDM scanner to collect and store images of the front and back of the check as well as the check MICR information into NRE FS ERS for further processing.

The agreement between the FS and Department of the Treasury outlines the data processing requirements for Federal agencies using Treasury's credit card and electronic check processing services.

1.5 Validation

How will the information be checked for accuracy?

Once a sales transaction is created, it will not be modified. Only status flags associated with the transaction are updated. Treasury mandated financial

institutions perform all required validity checks on the collected information contained on the credit card or check images.

1.6 Authority

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

The following documents are used to define the basis for collection of information:

e-Government Act of 2002: Improves the management and promotion of electronic government services.

Check Clearing for the 21st Century Act of 2003: Authorizes the use of paper check scanners to convert paper checks to electronic substitutes.

Collections and Cash Modernization Initiative: Reorganizes collection systems and processes to save money and reduce operational risk. Improves reporting to provide agencies and other Treasury systems with detailed collections information in a standard format through centralized means. Improves accuracy of information provided to agencies and meets Government-Wide Accounting requirements of the Computer Security Act of 1987.

Pay.gov Agency Participation Agreement: Outlines the Treasury Department's Financial Management Services (FMS) credit and debit card acquiring services. This agreement outlines the entities that perform card transactions on behalf of the agency.

Strategic Cash Management Agreement between USDA and the Treasury Department's Financial Management Service: Outlines the Treasury's cash management practices performed on behalf of the USDA.

1.7 Risk Mitigation

Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The FS Chief Financial Officer (CFO), System Owner, Program Manager, Information System Security Manager, Information Security Office, and contractors share responsibility for ensuring proper use of system data. User access to data will be limited to roles established for NRE FS ERS. Access to paper checks collected from customers will be limited to Collection Officers (cashiers, store managers) in the field. Once checks are scanned into NRE FS ERS, the data available through the application can only be accessed by users

after authentication to limited system users on an as-needed basis. Upon successful authentication, users can access only those functions as defined by their role.

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 Usage

Describe all the uses of information.

Routine uses are defined as disclosures where information is consistently shared whether internally or externally. Below are routine uses applicable to NRE FS ERS:

ERS shares credit card information with Treasury-designated processor (Worldpay) for payment received by credit card. Check information, including check image, bank routing and customer bank account number is shared with Treasury designated system OTCnet.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside FS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

Sharing data with the Department of the Treasury or another federal agency conducting financial assessment and payments.

Sharing information with the Department of Justice (including United States Attorney Offices) or another federal agency conducting litigation or in proceedings.

Sharing information with a congressional office in response to an individual's request.

Sharing information with the National Archives and Records Administration (NARA) or other federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

Sharing information with an agency, organization, or individual for the purpose of performing an audit or oversight operations.

Sharing information with an agency, organization, or individual for the purpose of performing an audit or oversight operations as authorized by law, but only such information that is necessary and relevant to such audit or oversight function.

Sharing information with appropriate agencies, entities, and persons when the FS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised. The FS will determine that as a result of:

Suspected or confirmed compromise, risk of harm to economic or property interests, Identity theft or fraud, harm to the security or integrity, of the system or to other systems or programs (whether maintained by the Department or another agency or entity), and harm to the individuals that rely upon the compromised information.

The disclosure made to such agencies, entities, and persons would be reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Sharing information with contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for FS when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to FS officers and employees.

Sharing information with the news media and the public, in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, or when disclosure is necessary to preserve confidence in the integrity of FS or is necessary to demonstrate the accountability of FS's officers, employees, or individuals covered by the system, except to the extent to which is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

2.2 Analysis and Production

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

There are no external tools used to analyze the data. NRE FS ERS provides reporting for financial data, however no personal information is part of this reporting.

2.3 Commercial/Public Use

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

NRE FS ERS does not use commercial or publicly available data.

2.4 Risk Mitigation

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

NRE FS ERS stores paper check images to process payments received from customers. Data is maintained in the information technology application which is managed by the NRE FS ERS project team. It is configured and maintained in accordance with policies and procedures established by the National Institute of Standards and Technology (NIST) standards and guidance (NIST SP 800-53 rev 4). NRE FS ERS meets all twelve requirements for Payment Card Industry Data Security Standard (PCI DSS) compliance.

Section 3.0 Retention

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

3.1 Time Period

How long is information retained?

NRE FS ERS sales and payment settlement data is retained for 6 years. However, the digital check images will not be retained for more than 18 months.

3.2 Approval

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

The retention period of 6 years based on NARA file code “6530 – Billings and collections,” has been selected for this system. NARA representative (William Meadows) was consulted for concurrence with the retention period and file code selected to facilitate the scheduling of the system. Concurrence was received from Mr. Meadows January 19, 2022.

3.3 Risk Mitigation

Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The primary risk associated with records retention within NRE FS ERS is that check information incorrectly retained could be stolen and used to access the financial records of the purchasers. This risk is mitigated by controlling access to the system. Access to the application is role based. The user’s access is restricted based on job function within the agency. A profile based on the user’s ID within the system determines what data the user can view. It is the responsibility of the user’s manager and the NRE FS ERS Security Administrator to ensure that the proper written authorization for access to the financial management system is completed and signed. In addition, it is also the responsibility of the NRE FS ERS Security Administrator to ensure that the right profile is attached to the user. Information within the system is also encrypted to prevent the misuse or abuse of the data captured.

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 Identification and Purpose

With which organization(s) outside of the Forest Service, but still within the Department of Agriculture is the information shared? What information is shared and for what purpose?

USDA FMMI: FMMI is the Department's financial system of record and all NRE FS ERS collection-related transactions are recorded in FMMI. A MOU between USDA and FS is in place to address the connection between ERS and FMMI.

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

Information collected at the registers (sales transaction information) as well as associated payment information is transmitted securely to the NRE FS ERS D365 Commerce Module at the time of the transaction via the FS Network. NRE FS ERS also transmits information to FMMI via a nightly batch file upload. The FMMI file contains job codes and amounts to be posted. No PII information is included in this file.

4.3 Risk Mitigation

Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The primary privacy risk associated with internal information sharing is the inadvertent or malicious release of customer information, either at the operational or application level. These risks are mitigated by restricting the type of information stored within the system and by utilizing role-based security to further minimize the amount of information available for viewing. The least privilege principal was used when establishing user roles so that the least amount of functionality required to use the system is assigned to each role.

Internal operational risks include the inadvertent sharing of information between applications. The Application Computing Environment in which the application resides, has controls in place to protect the unintended transfer of information between discrete applications sharing servers or databases.

Operational risks are mitigated through identification, authentication, and the security in place throughout the Microsoft Azure cloud hosting environment which is also certified by FedRamp.

Risks to privacy are mitigated by granting access only to authorized persons. All employees of the Department of Agriculture have undergone a thorough background investigation. Access to facilities is typically controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort.

Paper checks containing personal information are stored temporarily in secured file cabinets or in restricted areas, access to which is limited to authorized personnel until they are destroyed.

When a transaction must contain a signature in writing in order to be legally enforceable, due care is taken to ensure that documentation provides a record that is not subject to imperfect memory or competing claims as to what parties to the transactions intended.

The methods used to obtain, send, disclose, and store information comply with applicable laws, such as those governing privacy, confidentiality, recordkeeping, and accessibility to persons with disabilities.

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 Identification and Purpose

With which external organization(s), outside of both the Forest Service and the Department of Agriculture, is the information shared? What information is shared, and for what purpose?

NRE FS ERS connects to the following:

Encrypted credit card information is sent at the time of the transaction to the Treasury's designated financial institutions (Comerica Bank to process credit card transactions via Worldpay) using secure transmission protocols.

Encrypted paper check information is sent from ERS-SR module during a nightly process to the Treasury's designated financial institution (Federal Reserve Bank of Cleveland to process paper checks via OTCnet) using secure transmission protocols.

Department of the Treasury's CIR System: CIR is the system used by the Treasury to show transactions that have been cleared and deposited. NRE FS ERS users use information from CIR to settle deposits with collections and sales. The connection to CIR occurs via a secure transmission using protocols mandated by the Treasury. The banks send information to CIR for consolidation and reporting. Only select members of the ERS project team have access to the CIR reports.

Department of the Treasury's Pay.gov System: Pay.gov is the system used by the Treasury to collect credit card and electronic check payments for FS goods and services. NRE FS ERS uses information collected from Pay.gov to settle deposits with collections and sales.

Microsoft Azure Cloud Services: NRE FS ERS D365 Commerce SaaS and ERS-SR module are hosted at FedRamp certified Microsoft Azure Commercial Cloud.

5.2 Compatibility

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, provide SORN name and hyperlink URL to text.
If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

NRE FS ERS stores and transmits check images with potential PII to Treasury systems for the purpose of processing the payments. NRE FS ERS does not modify or use this for any other purpose and is not considered as the system of record. Similarly, credit card information is transmitted to Treasury systems for the purpose of processing the payments. NRE FS ERS stores partial card data (non PII) for the purpose of settlement activities.

5.3 Delivery and Security Measures

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

The information is transmitted using the secure transmission protocols required by the Treasury for any agency connecting to their mandated financial partners (Federal Reserve Bank of Cleveland and Comerica Bank). In addition, NRE FS ERS relies on the FS Application Cloud Environment (FS ACE) GSS and the FS Chief Information Officer (CIO) procedures for secure telecommunications and transfer protocols to be in place. These connections are limited to the egress Internet Protocol (IP) addresses as established by the US Forest Service and the US Treasury Interconnection Security Agreements (ISA).

5.4 Risk Mitigation

Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

PII data on credit cards is transmitted to the Treasury-designated credit card processor (Worldpay), data transmission is encrypted using treasury mandated protocols immediately upon collection of PII data in the EMV device directly to Worldpay and only partial (non-PII) data is transmitted back to NRE FS ERS Modern Point of Sale (MPOS) module (POS Terminal software). EMV device is considered a peripheral device to NRE FS ERS MPOS. If system is offline, data is held in the EMV device until proper communication channels are established. Data is not retrievable by users from the EMV device. A MOU is established between the FS and the Treasury for data managed by the Treasury-designated payment processor.

PII data on check images are transmitted to the Treasury-designated electronic check processor (FRBC) via OTCnet, data transmission is encrypted using Treasury-mandated protocols in a nightly batch process from

NRE FS ERS to OTCnet. A MOU is established between the FS and theTreasury for data managed by the Treasury-designated payment processor.

Section 6.0 System of Records Notice (SORN)

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 Requirement and Identification

Does this system require a SORN?
If so, please provide SORN name and hyperlink URL to text.
If a SORN is not required, answer "No" to this question, and "N/A" for questions 6.2 through 6.5.

NRE FS ERS is not a system of record, since neither the check images nor the credit card information is managed by the FS. Since the application is not a system of record, no SORN is required.

6.2 Individual Notification

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

FS policy adheres to Treasury regulations and guidance for individual notification. Each location prominently displays signage that explains what information may be collected and how that information will be used. Following are the details of the signage.

Notice to Customers Making Payment by Check

When you provide a check as payment, you authorize us either to use information from your check to make a one-time electronic fund transfer from your account or to process the payment as a check transaction. When we use information from your check to make an electronic fund transfer, funds may be withdrawn from your account as soon as the same day we receive your payment, and you will not receive your check back from your financial institution. For inquiries, please call 1-877-372-7248 Option #1.

Privacy Act – A Privacy Act Statement required by 5 U.S.C. § 552a (e) (3) stating our authority for soliciting and collecting the information from your check, and explaining the purposes and routine uses which will be made of your check information, is available from our internet site at www.fs.fed.us/billpay or call toll free at 1-877-372-7248 Option #1 to obtain a

copy by mail. Furnishing the check information is voluntary, but a decision not to do so may require you to make payment by some other method.

6.3 Right to Decline

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

Individuals have the option of declining to provide information by using cash rather than check or electronic payment methods. For cash payment, no PII is collected from customers.

6.4 Right of Consent

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

Individuals do not have the right to dictate the use of the information collected. Credit card and check payments are processed and maintained according to the prescribed guidelines at the Treasury-designated banks that process and maintain the information.

6.5 Risk Mitigation

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

Individuals are notified via signage displayed (mandated and provided by Treasury) as specified in section 6.2.

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.

NRE FS ERS stores check images with potential PII temporarily when an individual makes payment using a paper check. No other PII is stored and/or maintained in NRE FS ERS for individual access, redress and/or correction. NRE FS ERS is not considered a system of record for the information stored.

7.1 Access

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

Not applicable

7.2 Correction

What are the procedures for correcting inaccurate or erroneous information?

Not Applicable

7.3 Notification

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

Not Applicable

7.4 Redress Alternatives

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

Not Applicable

7.5 Risk Mitigation

Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

All redress actions are performed outside the ERS, if required.

Section 8.0 Technical Access and Security

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

8.1 Procedures

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

The FS CFO, System Owner, Program Manager, Information Systems Security Program Manager (ISSPM), Information System Security Officer (ISSO), and contractors share responsibility for ensuring proper use of system data. User access to data will be limited to roles established in NRE FSERS. Access to data will be limited to Collection Officers (cashiers, store managers), Budget Officers, and ASC Supervisors. The data available through the application can only be accessed by users after authentication. Upon successful authentication, users can access only those functions defined by their role.

System roles have been established to control the level of access by a user. Users requesting access to NRE FS ERS must sign and submit the FS 6500-214 form signed by their supervisor to request access to any FS Financial Management System. The users must have a current FS Active Directory account and must have completed FS-mandated security awareness training. In addition, users requesting access to NRE FS ERS must have an active USDA Active Directory and e-Authentication account.

8.2 Contractor Access

Will Department contractors have access to the system?

No, Department (USDA) contractors will not have access. Access is limited to current FS personnel and NRE FS ERS project team only. NRE FS ERS project team includes FS contractors (Network Specialty Group, Inc.).

8.3 Privacy Training

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

Annual Security Awareness Training and Rules of Behavior Training are mandatory for all employees who have FS accounts. If this training is not completed by the required deadline, the accounts are disabled until such time

when proof is supplied that the training has been completed. Onboarding and periodic refresher training on the proper handling of cash, credit cards and checks. Because checks are maintained physically, training is provided for the proper protection and disposition of the checks collected and scanned during the purchase

8.4 System Authority to Operate

Has Assessment & Authorization been completed for the system(s) supporting the program? If so, answer "Yes" and provide ATO expiration date(s).

Yes, November 23, 2023

8.5 Audit and Technical Safeguards

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

The ISSO and System Owner review/analyze audit logs on a periodic and as-needed basis for reasons such as: suspected activity violations, suspicious activity investigation, indications of inappropriate or unusual activity, and for the reporting of findings to appropriate officials to take necessary actions. NRE FS ERS will utilize a Dynamics portal for auditable events to support operations and security teams monitoring of the day-to-day activity, response to emergent threats, and after-the-fact forensics.

8.6 Risk Mitigation

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?

Risks identified are broken down into three modules: NRE FS ERS MPOS, NRE FS ERS Microsoft D365 Retail and ERS-SR. The MPOS components (credit card readers and check scanners) process PII information as part of the payment processing required of a POS system. NRE FS ERS Microsoft D365 Retail and ERS-SR modules store scanned check images for further payment processing. Only obfuscated credit card information is stored in NRE FS ERS Microsoft D365 Retail and ERS-SR modules for further settlement activities and it is not PII.

When payments are collected at point-of-sale sites, PII data associated with paper checks is visible to the payment processing individuals. PII information on the paper check is visible to collection officers. Data is transmitted to MS

Dynamics Headquarters immediately and it is not retrievable by component users once the payment transaction is successfully completed. If the system is offline, data is held until proper communication channels are established.

NRE FS ERS uses separation of duties and multi-layered levels of security to mitigate privacy risk for transferring information to other individuals and/or external organizations.

Checks might be visible to nearby persons who do not have a need to know this data. FS Collection Officers perform check scanning activities behind the counter to prevent nearby persons from viewing check information. Once checks are scanned, they are secured in accordance with FS physical security policy and procedures.

Physical checks may not be controlled properly after scanning. Physical paper checks are secured temporarily and destroyed in accordance with FS financial management policy and procedures.

Existing access controls prevent unauthorized access and/or modification of data, and in some instances, data is no longer available for modification based on process (it is locked). Roles are tested to ensure that they can only get to the data to which they are intended to have access.

Check images that will show PII are stored for further processing in NRE FS ERS cloud components. Data is securely transmitted from MPOS to NRE FS ERS in a cloud environment and the data is encrypted at rest. Only a limited number of roles can have access to these check images on an as-needed basis to resolve system issues for further processing and settlement activities. Roles are tested to ensure that they can only get to the data to which they are intended to have access.

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 Description

What type of project is the program or system?

NRE FS ERS is a major application used to process FS over-the-counter payment for goods and services offered. This system has three components, (1) MPOS which will be deployed throughout the FS field offices and recreation areas (2) Microsoft D365 Retail which is hosted on Microsoft Azure Commercial Cloud and manages configurations of MPOS centrally (3) ERS-SR module (Custom Development) which is hosted on the Microsoft Azure Commercial Cloud data center.

9.2 Privacy Concerns

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

NRE FS ERS POS components, cash drawers, credit card readers, and check scanners are used as part of the payment collection process. NRE FS ERS accepts as input, basic sales transaction information including price, product identifiers, and customer payment information. Payment from a customer can take the form of cash, paper check, or credit card.

Credit card processing occurs in near real-time, if there is an active internet connection. Information from the credit card transactions is sent at the time of payment to Worldpay for payment authorization. Paper check transactions, including check images, are sent nightly via batch mode to the US Treasury (OTCnet).

When a customer pays with a credit card, assuming that the system is online (i.e. connected to the FS network), a request for credit card authorization is sent to Worldpay. If the card is valid and sufficient funds are available, the bank will return an authorization code approving the transaction. If the card is not valid, no code will be returned, and the payment will be rejected in NRE FS ERS.

In the case where the system is operating in off-line mode (i.e., the connectivity to the network is not operational), the EMV devices will store the transaction and provide a provisional approval/disapproval. Once network

connectivity is restored, the transactions will be automatically submitted for processing to WorldPay/Comerica by the EMV device.

Check Payments – When a customer pays with a check, an image of the scanned check is stored with the transaction. These images are sent securely to the Federal Reserve Bank of Cleveland every night for processing.

The security controls in place, both physically and internal to the FS ACE GSS, networks, and Azure Commercial Cloud services, mitigate or eliminate any privacy concerns. This GSS works in tandem with other GSS and the cloud services vendor to support the security of the FS data.

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 Review

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, the System Owner and ISSPM have reviewed OMB M-10-22 and M-10-23.

10.2 Purpose

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

Third party websites and/or applications are not used for NRE FS ERS.

10.3 PII Availability

What Personally Identifiable Information (PII) will become available through the agency's use of 3rd party websites and/or applications.

Third party websites and/or applications are not used for NRE FS ERS.

10.4 PII Usage

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

Third party websites and/or applications are not used for NRE FS ERS.

10.5 PII Maintenance and Security

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

Third party websites and/or applications are not used for NRE FS ERS.

10.6 PII Purging

Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically? If so, is it done automatically? If so, is it done on a recurring basis?

Third party websites and/or applications are not used for NRE FS ERS.

10.7 PII Access

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

Third party websites and/or applications are not used for NRE FS ERS.

10.8 PII Sharing

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?

Third party websites and/or applications are not used for NRE FS ERS.

10.9 SORN Requirement

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)?

Third party websites and/or applications are not used for NRE FS ERS.

10.10 Web Measurement and Customization

Does the system use web measurement and customization technology? If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

Third party websites and/or applications are not used for NRE FS ERS.

10.11 Web Measurement and Customization Opt-In/Opt-Out

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

System users are not allowed to engage in decisions on the use of web measurements or customization technology because third party websites and/or applications are not used for NRE FS ERS.

10.12 Risk Mitigation

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.

Third party websites and/or applications are not used for NRE FS ERS.

Responsible Official

ANSTIENETTE SHARPE
Digitally signed by ANSTIENETTE SHARPE
Date: 2022.02.25 10:13:21 -05'00'

Anstienette Sharpe
System Owner (SO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture

Approval Signature

CYNTHIA TOWERS
Digitally signed by CYNTHIA TOWERS
Date: 2022.03.01 13:07:28 -06'00'

Cynthia Towers
Privacy Officer (PO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture

CYNTHIA TOWERS
Digitally signed by CYNTHIA TOWERS
Date: 2022.03.01 13:07:50 -06'00'

Laura Hill
Assistant Chief Information Security Officer (ACISO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture