U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

OFFICE OF THE CHIEF PRIVACY OFFICER

The completion of USDA Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that security and privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, USDA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement**,** PIAs will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Guidance on how to complete the following PIA Questionnaire is available here.

Privacy Impact Assessment for the USDA IT System/Project:

NRE FS eCollections Retail System (NRE FS ERS)

Office of the Chief Financial Officer

USDA Forest Service

Date PIA submitted for review:

2/26/2024

Mission Area System/Program Contacts:

	Name	E-mail	Phone Number
Mission Area Privacy Officer	Cynthia Ebersohn	cynthia.ebersohn@usda.gov	386-301-4060
Information System Security Officer	Joshua Holer	joshua.holer@usda.gov	719-225-6454
System Owner	Anstienette Sharpe	anstienette.sharpe@usda.gov	703-217-4720

Abstract

The abstract provides the simplest explanation for the "what does the system do?" and will be published online to accompany the PIA link.

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

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA.

The NRE FS e-Collections Retail System (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.

NRE FS ERS is hosted on the Microsoft Azure Commercial Cloud Service. The Forest Service Chief Financial Officer (CFO), in coordination with the Chief Information Office (CIO), is aligning its applications to comply with the 2019 Federal Cloud Computing Strategy — Cloud Smart — to achieve additional savings, security, and faster services. Leveraging risk management framework inheritance concepts and best practices, while utilizing FedRAMP-compliant cloud services, the FS has the opportunity to implement leading solutions to better serve the agency's mission, drive improved citizen services, and increase cyber security.

This is a hybrid system with payment collection components at the point of sale, which exchanges data with the Azure Cloud Dynamics 365 Commerce Software as a Service (SaaS) and the FS Reconciliation and Settlement Application (Custom Development) hosted on the Azure FedRAMP-compliant Platform as a Service (PaaS). This relationship supports the management of stores, prices, and provides a front-facing point-of-sale system to consolidate all sales transactions, settle payments with banks, transfer settled data to the USDA's Financial Management Modernization Initiative (FMMI), and reconcile deposits and debits between the Department of the Treasury and FMMI.

ERS connects to the following:

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

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: This 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 Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

1.1. What legal authorities and/or agreements permit the collection of information by the project or system?

Public Law 108–100: 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.

1.2 Has Authorization and Accreditation (A&A) been completed for the system?

Yes

1.3. What System of Records Notice(s) (SORN(s)) apply to the information?

N/A; NRE FS ERS does not retrieve information using a personal identifier.

1.4. Is the collection of information covered by the Paperwork Reduction Act?

No

Section 2.0 Characterization of the Information

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

2.1. What information is collected, used, disseminated, or maintained in the system/program?

PII is defined 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. Mark all applicable PII and data elements in the table.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

Identifying Numbers			
□	Social Security number	□	Truncated or Partial Social Security number
□	Driver's License Number	□	License Plate Number
□	Registration Number	□	File/Case ID Number
□	Student ID Number	□	Federal Student Aid Number
□	Passport number	□	Alien Registration Number
□	DOD ID Number	□	DOD Benefits Number
□	Employee Identification Number	□	Professional License Number
□	Taxpayer Identification Number	□	Business Taxpayer Identification Number (sole proprietor)
□	Credit/Debit Card Number	□	Business Credit Card Number (sole proprietor)
□	Vehicle Identification Number	□	Business Vehicle Identification Number (sole proprietor)

☒	Personal Bank Account Number	☒	Business Bank Account Number (sole proprietor)
□	Personal Device Identifiers or Serial Numbers	□	Business device identifiers or serial numbers (sole proprietor)
☒	Personal Mobile Number	□	Business Mobile Number (sole proprietor)
□	Health Plan Beneficiary Number		

Biographical Information

☒	Name (including nicknames)	□	Gender	☒	Business Mailing Address (sole proprietor)
□	Date of Birth (MM/DD/YY)	□	Ethnicity	□	Business Phone or Fax Number (sole proprietor)
□	Country of Birth	□	City or County of Birth	□	Group/Organization Membership
□	Citizenship	□	Immigration Status	□	Religion/Religious Preference
☒	Home Address	☒	Zip Code	☒	Home Phone or Fax Number
□	Spouse Information	□	Sexual Orientation	□	Children Information
□	Marital Status	□	Military Service Information	□	Mother's Maiden Name
□	Race	□	Nationality	□	Global Positioning System (GPS)/Location Data
□	Personal e-mail address	□	Business e-mail address	□	Personal Financial Information (including loan information)
□	Employment Information	□	Alias (username/screenname)	□	Business Financial Information (including loan information)
□	Education Information	□	Resume or curriculum vitae	□	Professional/personal references

Biometrics/Distinguishing Features/Characteristics

□	Fingerprints	□	Palm prints	□	Vascular scans
□	Retina/Iris Scans	□	Dental Profile	□	Scars, marks, tattoos
□	Hair Color	□	Eye Color	□	Height
□	Video recording	□	Photos	□	Voice/ Audio Recording
□	DNA Sample or Profile	□	Signatures	□	Weight

Medical/Emergency Information

□	Medical/Health Information	□	Mental Health Information	□	Disability Information
□	Workers' Compensation Information	□	Patient ID Number	□	Emergency Contact Information

Device Information

□	Device settings or preferences (e.g., security level, sharing options, ringtones)	□	Cell tower records (e.g., logs, user location, time, etc.)	□	Network communications data

Specific Information/File Types					
□	Personnel Files	□	Law Enforcement Information	□	Credit History Information
□	Health Information	□	Academic/Professional Background Information	□	Civil/Criminal History Information/Police Record
□	Case files	□	Security Clearance/Background Check	□	Taxpayer Information/Tax Return Information

2.2. What are the sources of the information in the system/program?

Data sources include payments made by customers using cash, credit cards, and paper checks. When payments are made via check, customer Personally Identifiable Information (PII) such as name, address, phone number, and bank routing and account numbers are captured. These paper check images, containing bank routing and account numbers, are temporarily stored in NRE FS ERS before being submitted to a Treasury-designated system for further processing.

2.2.1. How is the information collected?

Credit cards are inserted into the credit card chip reader 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.

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 check scanner to collect and store images of the front and back of the check as well as the check MICR account 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.

2.3. Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

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

2.4. How will the information be checked for accuracy? How often will it be checked?

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.

2.5. Does the system/program use third-party websites?

No

2.5.1. What is the purpose of the use of third-party websites?

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

2.5.1.1. What PII will be made available to the agency through the use of third-party websites?

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

2.6. PRIVACY IMPACT ANALYSIS: Related to Characterization of the Information.

Privacy Risk: One potential risk is the loss or disclosure of PII data during payment collection. 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.

Mitigation: Data is transmitted to MS Dynamics Headquarters immediately and it is not retrievable by collection officers once the payment transaction is successfully completed. 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. If the system is offline, data is held until proper communication channels are established.

Privacy Risk: Checks might be visible to nearby persons who do not have a need to know this data.

Mitigation: 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.

Privacy Risk: Physical checks may not be controlled properly after scanning.

Mitigation: Physical paper checks are secured temporarily and destroyed in accordance with FS financial management policy and procedures.

Section 3.0 Uses of the Information

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

3.1. Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

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.

3.2. Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

No

3.3. PRIVACY IMPACT ANALYSIS: Related to uses of the information.

Privacy Risk: The potential risk is the loss or disclosure of PII data.

Mitigation: In addition to the mitigation strategies outlined in section 2.6 of this document, NRE FS ERS is assessed annually against National Institute of Standards and Technology (NIST) security controls (800-53 rev 5) at a moderate security baseline. The PII collected is of low value to a potential threat. Data is maintained in the information system, which is configured and maintained in accordance with policies and procedures established by the Forest Service and the USDA. In addition, all users of the system are required to take Information Security Awareness Training annually as well as acknowledge they have read and agree to the Rules of Behavior for using Government information systems. Both cover the use and handling of PII.

Section 4.0 Notice

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

4.1. How does the project/program/system provide notice to individuals prior to collection?

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.

4.2. What options are available for individuals to consent, decline, or opt out of the project?

Consent: An individual provides consent by choosing to provide a check as payment

Declining or Opting Out: Individuals may decline or opt out by choosing not to pay with a check or by not completing the transaction.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Privacy Risk: Individuals unaware of the collection of their data.

Mitigation: Individuals have the choice of whether or not to pay by check. If they choose to pay by check, they are voluntarily submitting any personal information that may be displayed on the check. The information is used solely to process the transaction. Forest Service point-of-sale locations have signage that prominently explains what information may be collected and how that information will be used.

Section 5.0 Data Retention

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

5.1. What information is retained and for how long?

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.

5.2. Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

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.

5.3. PRIVACY IMPACT ANALYSIS: Related to retention of information

Privacy Risk: The potential risk is the loss or disclosure of PII data while being stored.

Mitigation: 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 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 a need-to-know 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 6.0 Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

6.1. With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

N/A – Transactional data is shared internally. The check images containing the PII are not.

6.2. PRIVACY IMPACT ANALYSIS: Related to internal sharing and disclosure.

Privacy Risk: N/A

Mitigation: N/A

6.3. With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Check images are transferred to the Federal Reserve Bank of Cleveland for processing via a secure connection.

6.4. PRIVACY IMPACT ANALYSIS: Related to external sharing and disclosure.

Privacy Risk: Files could be intercepted during transmission.

Mitigation: NRE FS ERS PII data is transferred to the Federal Reserve Bank of Cleveland every night for processing via a secure TLS 1.2 connection on TCP port 443. The processing system is hosted by the Treasury Web Application Infrastructure (TWAI). The TWAI provides a multi-tiered web interface and common services for multiple Treasury applications. Guiding principles for the TWAI include the provision of generally accessible applications in a suitably robust environment, giving precedence to security over other considerations, the use of segmented, layered security, and the placement of all operations and data as far away from internet access as is reasonable. Internal users access the TWAI via Virtual Private Networks (VPNs) using smart card-based authorization and authentication.

Privacy Risk: Unauthorized internal users could access the information.

Mitigation: Access to the TWAI applications and services must be authorized by the U.S. Department of the Treasury - Fiscal Service and deemed necessary for the user to carry out assigned job functions. Privileges granted for that purpose must comply with the principles of separation of duties and of least privilege defined for the system. That is, a potential user has no access to enterprise resources or applications unless authorized by the owner of the resource or application and the user has only as much access privilege as is needed to perform the assigned tasks. All administrative personnel with access to systems on which the data resides will have a current Treasury-approved background investigation.

Section 7.0 Redress

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

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

N/A

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

N/A

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

N/A

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

The personal information on the checks is static. If something is incorrect on a check, it's up to the individual to correct it themselves or by working with their financial institution.

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

N/A

Section 8 Auditing and Accountability

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

8.1. How is the information in the system/project/program secured?

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.

8.2. What procedures are in place to determine which users may access the program or system/project, and are they documented?

The FS CFO, System Owner, Program Manager, Information Systems Security Manager (ISSM), Information System Security Officer (ISSO), and contractors share responsibility for determining user access to the system. 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. User access determinations are done in accordance with the procedures contained within the internal Access Control SecureCAP documents as well as the internal SharePoint NRE FS ERS FAQ webpage.

8.3. How does the program review and approve information sharing requirements?

Information sharing requirements are documented, reviewed, and approved as part of the Interconnection Security Agreement (ISAs) review process.

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

Annual Security Awareness Training and Rules of Behavior Training, which also covers privacy 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.

Approval Signatures:

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

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

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

QUANISHA JONES Digitally signed by QUANISHA JONES
Date: 2024.10.22 12:30:04 -04'00'

Office of the Chief Privacy Officer
United States Department of Agriculture