Privacy Impact Assessment

for

e-Collections (e-Collections)

Policy, E-Government and Fair Information Practices

Version: 2.2

Date: November 8, 2019

Prepared for: USDA FS CIO

Contact Point

Mona Rayside

System Owner

USDA NRE Forest Service

703-605-4681

Reviewing Official

Cynthia Towers

Privacy Officer

USDA NRE Forest Service

(816) 844-4000

Abstract

The Privacy Impact Assessment (PIA) addresses the US Forest Service (FS) e-Collections System. The primary objective of e-Collections 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 of name and financial data currently present in the e-Collections System.

Overview

e-Collections 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 customer payment information. Payment from a customer can take the form of cash, paper check, or plastic cards (credit or debit). Note, debit cards are processed as credit card transactions.

Plastic 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 mode to the US Treasury Over-the-Counter Channel (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, 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 e-Collections. If the customer does not have a valid form of payment, the transaction is cancelled.

This PIA has been updated to reflect the incorporation of “an electronic chip” in addition to the current magnetic strip credit card processing. Department of the Treasury mandated this in instances where the system is operating in off-line mode (i.e. the connectivity to the network is not operational), but there is telephone access. In this case, FS personnel will contact the bank directly to get an authorization code that will be manually entered into the transaction.

e-Collections connects to the following:

Forest Service General Support System (GSS) where e-Collections servers reside.

Forest Service Computer Base (FSCB) Network: GSS that serves as a transmission medium for e-Collections.

FSCB Legacy: GSS that provides the framework for essential FS applications, including e-mail platforms, the local area network (LAN), wide area network (WAN), and FS World Wide Web.

USDA Financial Management Modernization Initiative (FMMI): FMMI is the Department's financial system of record and all e-Collections' collection-related transactions are recorded in FMMI. A Memorandum of Understanding (MOU) between the USDA and FS is in place to address the connection between e-Collections and FMMI.

USDA E-Authentication System (e-Auth): The e-Authentication system is used to validate access to the Central Office functions located on the Application Computing Environment (ACE) servers. A separate MOU between USDA and FS regarding use of the Department-mandated e-Authentication system has been drafted and is awaiting signature.

Department of the Treasury's Collection Information Repository (CIR): CIR is the system used by Treasury to show transactions that have been cleared and deposited. E-Collections users utilize information from CIR to reconcile deposits with collections and sales.

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 plastic card transactions. A MOU outlining the agreement between FS and Department of the Treasury is already in place.>>

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?

e-Collections collects name, financial data (including credit card and check numbers), and miscellaneous local identification numbers as it pertains to citizens versus federal employees.

1.2 Source

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

The sources of the data are from sales transactions using cash, plastic cards, and checks.

1.3 Justification

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

This is a point-of-sale system with an EMV (Europay, MasterCard, and Visa) terminal; only the obfuscated credit card numbers with first five digits and last four digits are collected if the customer pays by credit card.

Bank routing number and account number is collected if paying by check. The check image is transmitted to the financial institution selected by Department of the Treasury for storage and processing. An electronic image of the check is stored. All information is used to collect payments owed to the Government.

1.4 Collection

How is the information collected?

Financial institutions selected by Department of the Treasury collect information from credit card and check transactions for processing. 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. Check images are digitally captured at

the time the check is presented and transmitted as payment. 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 that financial institutions perform all required validity checks on the collected information. Accuracy of the data gets verified during reconciliation of FMMI and CIR data with the sales transaction as the supporting data.

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 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 in the e-Collections System. 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 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 e-Collections:

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 has determined 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 is 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?

No data analysis is performed within e-Collections POSS. Credit card information is read from the magnetic strip on the back of each card, or the electronic chip on the front of the card and sent directly to Treasury's designated financial institutions for electronic processing. Check information contained on the scanned check image is also sent directly to the financial institutions mandated by Treasury for processing.

e-Collections is not responsible for processing or aggregating financial information from checks and credit card transactions. The resulting data from credit card and check processing is sent directly to the Treasury Department's mandated financial institutions. Customers who do not wish to have their credit card or check information processed by Treasury's mandated institutions may elect to complete their purchases anonymously by means of cash payments.

2.3 Commercial/Public Use

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

The system 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.

This system of records collects the minimum amount of personally identifiable information necessary to verify the identity of those requesting or using the information. Data is maintained in the information technology application, which is configured and maintained in accordance with policies and procedures established by the National Institute of Standards and Technology (NIST) standards and guidance.

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?

e-Collections data is retained for 6 and a half years.

3.2 Approval

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

e-Collections abides by the FS and the Federal Government's policies regarding the record retention policies for legal contracts and similar documents. Unless the records were shared for routine use purposes, the accounts of the disclosures should be available to the data subject upon request. The disposition instructions in mission area, agency, or staff office record schedules are mandatory.

Officials may not dispose of records prior to their authorized disposal date, or retain records beyond their authorized disposal date, except for situations in which records might be relevant to pending or threatened litigation. If a program official determines that records need to be retained longer than authorized by the schedule, the mission area, agency, or the Staff Office Records Officer, shall be contacted to obtain approval from NARA and, if necessary, revise the schedule.

The actions taken regarding records and non-records no longer needed for current Government business include transfer to agency storage facilities or federal records centers, transfer from one federal agency to another, transfer of permanent records to the National Archives, and the disposal of temporary records.

For non-records, these actions include screening and destruction. Destruction is the primary type of disposal action and can include burning, shredding, deleting, or discarding with other waste materials. In the electronic realm, destruction is typically accomplished by overwriting or degaussing, depending on security requirements.

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 e-Collections is that check, or credit card 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 ASC Security Administrator to ensure that the proper paperwork for access to the financial management system is completed and signed. In addition, it is also the responsibility of the ASC 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?

e-Collections connects to the following:

FS Application Computing Environment (ACE) where e-Collections servers reside.

FSCB Network: ACE that serves as a transmission medium for e-Collections.

FSCB Legacy: ACE that provides the framework for essential FS applications, including e-mail platforms, the LAN, WAN, and FS World Wide Web.

USDA FMMI: FMMI is the Department's financial system of record and all e-Collections' collection-related transactions are recorded in FMMI. A Memorandum of Understanding (MOU) between USDA and FS is in place to address the connection between e-Collections and FMMI.

USDA E-Authentication System (e-Auth): The e-Authentication system is used to validate access to the Central Office functions located on the ACE servers. A separate MOU between USDA and FS regarding use of the Department-mandated e-Authentication system is in place.

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

The information is transmitted to FMMI via a nightly batch file upload. All core data (users, products) are centrally stored and managed from the Central Office module and pushed nightly to maintain consistency. Information collected at the registers, i.e. sales transaction information, is transmitted to the Central Office at the time of the transaction via the FS Network.

Encrypted credit card information and digital check images are sent at the time of the transaction to Treasury's designated financial institutions using secure transmission protocols.

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 Application Computing Environment (ACE) General Support System (GSS).

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.

All records containing personal information are maintained in secured file cabinets or in restricted areas, access to which is limited to authorized personnel. Access to computerized files is password-protected and under the direct supervision of the System Manager. The System Manager has the capability of printing audit trails of access from the computer media, thereby permitting regular ad hoc monitoring of computer usage.

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?

e-Collections connects to the following:

Department of the Treasury's Collections Information Repository (CIR) System: CIR is the system used by Treasury to show transactions that have been cleared and deposited. e-Collections users use information from CIR to reconcile deposits with collections and sales. The connection to CIR occurs via a secure transmission using protocols mandated by Treasury. The banks send information to CIR for consolidation and reporting. Only select members of the Forest Service Budget & Finance staff have access to the CIR reports.

Two Department of the Treasury-specific banks – Federal Reserve Bank of Cleveland and Comerica Bank: The Department of the Treasury has mandated that the FS use the Federal Reserve Bank of Cleveland to process paper checks (via OTCnet) and Comerica Bank to process plastic card transactions (via Worldpay).

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. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

The sharing of personally identifiable information is compatible with Agency and Department policy and is covered by an appropriate routine use in a System of Record Notice (SORN). The applicable SORN is USDA/OCFO-10

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 Treasury for any agency connecting to their mandated financial partners (Federal Reserve Bank of Cleveland and Comerica Bank). In addition, e-Collections relies on the ACE GSS and the FS Chief Information Officer (CIO) procedures for secure telecommunications and transfer protocols to be in place

5.4 Risk Mitigation

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

Information is only released on a 'need-to-know' basis under statutory or other lawful authority to maintain such information. The information is used in accordance with the statutes, authority and purpose stated.

USDA agencies and offices will review the quality (including objectivity, utility, and integrity) of information before it is disseminated to ensure that it complies with the standards set forth in the Department's general information quality guidelines.

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 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 and if so, please provide SORN name and URL?

(Note: If a SORN is not required, answer "No" to this question, and "N/A" for questions 6.2 through 6.5.)

The Privacy Act of 1974 requires any agency collecting information to publish a System of Record Notice (SORN) in the Federal Register no less than 40 days prior to collection of the information. The applicable SORN is USDA/OCFO-10, which is found on the OCIO SORN page.

6.2 Individual Notification

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

FS policy adheres to Treasury regulations which state that agencies or entities processing credit card or check payments made by customers must prominently display signage that explains what information may be collected and how that information will be used. Each FS location states checks will be processed electronically.

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.

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 according to the prescribed guidelines at the Treasury-designated banks that process 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) that checks are processed electronically at the point-of-sale.

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 Access

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

Users may access a variety of detailed information regarding sales or collection transactions by contacting the Albuquerque Service Center (ASC) Budget and Finance (B&F) Customer Support Staff at 1-877-372-7248.

USDA Employees or contractors seeking access should follow the procedure described by the USDA's Quality of Information Guidelines.

In compliance with the requirements of the Quality of Information Guidelines, there are documents that provide information pertaining to requests for access or correction of information disseminated by the U.S. Forest Service. USDA's information quality guidelines and administrative mechanisms conform to the requirements of OMB's information quality guidelines.

USDA's guidelines include revisions to incorporate the detailed guidance contained in OMB's supplemental guidance of June 10, 2002. USDA's information quality guidelines adopt the definitions included in OMB's guidelines.

Though access to the system may be denied, any person, including U.S. citizens, foreign nationals, organizations, universities, businesses, and state and local governments, can file a Freedom of Information Act (FOIA) Request to acquire copies of records of the system. Federal employees may not use government time or equipment when requesting information under the FOIA.

7.2 Correction

What are the procedures for correcting inaccurate or erroneous information?

Users may access a variety of detailed information regarding sales or collection transactions by contacting the Albuquerque Service Center (ASC) Budget and Finance (B&F) Customer Support Staff at 1-877-372-7248.

Though access to the system may be denied, any person, including U.S. citizens, foreign nationals, organizations, universities, businesses, and state and local governments, can file a Freedom of Information Act (FOIA) Request to acquire copies of records of the system.

7.3 Notification

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

Customer can contact the FS Budget and Finance staff at the Albuquerque Service Center via phone or written correspondence. Users may submit requests for corrections via the methods described in section 7.1.

7.4 Redress Alternatives

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

Users may access a variety of detailed information regarding sales or collection transactions by contacting the Albuquerque Service Center (ASC) Budget and Finance (B&F) Customer Support Staff at 1-877-372-7248.

Though access to the system may be denied, any person, including U.S. citizens, foreign nationals, organizations, universities, businesses, and state and local governments, can file a Freedom of Information Act (FOIA) Request to acquire copies of records of the system.

Write to: USDA FS, FOIA Service Center 1400 Independence Avenue, SW, Mail Stop: 1143, Washington, DC 20250-1143. Correspondence may also be sent via fax or e-mail: Fax your request to: (202) 260-3245. E-mail correspondence to: wo_foia@fs.fed.us.

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 e-Collections application.

However, though access to the system may be denied, any person, including U.S. citizens, foreign nationals, organizations, universities, businesses, and state and local governments, can file a Freedom of Information Act (FOIA) Request to acquire copies of records of the system. Federal employees may not use government time or equipment when requesting information under the FOIA.

Individuals who have reason to believe that this system might have records pertaining to them should write to the FS Freedom of Information Act Office. Personnel in that division will then forward the request to the section of the Agency believed to be most likely to maintain the records being sought. The individual must specify that he or she wishes the records of the system to be

checked. At a minimum, the individual's request should include their name, date and place of birth, current mailing address and zip code, signature, and a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that this system has records pertaining to him or her. Write to USDA FS, FOIA Service Center 1400 Independence Avenue, SW, Mail Stop: 1143, Washington, DC 20250-1143. Correspondence may also be sent via fax or e-mail: Fax your request to: (202) 260-3245. E-mail correspondence to: wo_foia@fs.fed.us.

The guidance for the content of requests for correction of information is not intended to constitute a set of legally binding requirements. Requestors bear the 'burden of proof' with respect to the necessity for correction, as well as the type of correction they seek. However, the U.S. Forest Service may be unable to process, in a timely fashion or at all, any requests that omit one or more of the required elements.

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, ISSPM, ISSO, and contractors share responsibility for ensuring proper use of system data. User access to data will be limited to roles established in the e-Collections System. 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 e-Collections 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 the Central Office must have an active e-Authorization account.

8.2 Contractor Access

Will Department contractors have access to the system?

No. Access is limited to current FS personnel only.

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.

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. ATO expiration date is 4/13/2021

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 records on a periodic and as-needed basis for reasons such as: suspected activity violations, investigate suspicious activity, indications of inappropriate or unusual activity, and report findings to appropriate officials to take necessary actions.

Examples of an unusual activity are anomalies regarding day-to-day activity, such as too many logins to or logoffs from the system. Upon investigating unusual activity, findings will be reported up to the CFO if the System Owner deems it necessary. The level of audit monitoring and analysis activity within the information system is increased whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

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?

e-Collections uses separation of duties and multi-layered levels of security to mitigate privacy risk for transferring information to other agencies. By keeping the information disseminated across internal and external systems (i.e. Treasury’s collections processing partners), no single source can be accessed to illicitly create a complete profile of an individual’s privacy data. Separated roles prevent any one user from having full access for fraudulent use of the data and information.

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?

e-Collections is a major application that resides on FS ACE.

9.2 Privacy Concerns

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

The security controls in place, both physically and internal to the FS ACE GSS, mitigate or eliminate any privacy concerns. This GSS works in tandem with other GSS to support the security of the FS core 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 e-Collections.

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 e-Collections.

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 e-Collections.

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 e-Collections.

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 e-Collections.

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 e-Collections.

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 e-Collections.

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 e-Collections.

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?

e-Collections does not use web measurement and customization technology.

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?

e-Collections does not use web measurement and customization technology.

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 e-Collections.

Responsible Official

ANSTIENETTE SHARPE
Digitally signed by ANSTIENETTE SHARPE
Date: 2020.05.11 12:28:34 -04'00'

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: 2020.05.12 14:21:54 -05'00'

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

ROBERT CHADDERDON
Digitally signed by ROBERT CHADDERDON
Date: 2020.05.18 08:17:17 -06'00'

Laura Hill
Information System Security Program Manager (ISSPM)
Natural Resources and Environment, Forest Service
United States Department of Agriculture