Privacy Impact Assessment
Publication Distribution System (PDS)

Policy, E-Government and Fair Information Practices

- Version: 1.2
- Date: July 30, 2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

USDA

United States Department of Agriculture

Privacy Impact Assessment for the Publication Distribution System

July 30, 2020

Contact Point

Sudha Sriparameswaran
FPAC Program Manager Supervisor
817-509-3260

Reviewing Official

James Flickinger
Chief Information Security Officer
United States Department of Agriculture
(816) 926-6010

Abstract

The Publication Distribution System is designed to provide an inventory management and delivery system. Requests for publications are received from the general public, processed by NRCS staff, and shipped to the requester. This PIA is being conducted because PII is collected for the delivery of these publications.

Overview

The purpose of NRCS' Publication Distribution System application is to disseminate information about conservation activities to the requesting public. The information that can be stored in the system is the requesters' name, address, email address phone, and fax number.

An example of a typical Internet Transaction; John Q Public places an order for two posters and a brochure. He enters his information (name, shipping address, email and phone). The application generates an email (if applicable) verifying the order. An Administrator user (level 2 eAuth) then accesses the order and prepares it for shipping (pick, pack, etc.). "Pick, pack" represents phases of shipping an order. Administrator user then prints shipping label (via a call to a secure web service provided by UPS) and ships the order.

An example of a typical Telephone Transaction; John Q Public calls the NRCS Distribution center and requests a poster to be shipped to him. The Admin user who answers the call collects the Ship to name, shipping address, and the Phone number and Email address (optional) and enters the information into the application. The order is completed like web orders (pick, pack, etc.).

Information is shared with UPS in order to generate tracking numbers and actually ship/deliver the package(s).

Section 1.0 Characterization of the Information

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

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

Name, Shipping Address, Email address, Phone/Fax numbers and customer number generated randomly through the application. The shipping address is just where the requested items get shipped.

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

The general Public provides this information when requesting publications

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

To mail the requested publications to public consumers.

1.4   How is the information collected?

Internet or telephone. The information is entered into the database via either mechanism, depending on how they reach us.

1.5   How will the information be checked for accuracy?

The user validates their information, in order to ensure that they receive the documents that they have requested. Zip codes are validated against an authoritative source. We get the zip code data from FMS, Inc http://www.fmsinc.com. FMS is not an additional vendor-NRCS merely orders zip code data from FMS, FMS provides it and NRCS merges the zip code data into existing data.

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

- Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.)
- Privacy Act of 1974

1.7   <u>Privacy Impact Analysis</u>: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The design of this application ensures that only the minimum required amount/type of data is collected to meet the requirement of distributing publications to the requesting public. The customer information is stored in a secure SQL Server database in the USDA enterprise data center in Kansas City. This information is not displayed anywhere in the application publicly and is used only for the purpose of generating a shipping label using a web service call hosted and provided by UPS. This web service call is secure (i.e., uses secure https protocol). HTTPS is another design element which ensures this system merits a moderately low classification.

Section 2.0 Uses of the Information

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

2.1   Describe all the uses of information.

A secure web service call to UPS generates a shipping label that uses the information provided by the requesting user of this application. UPS was selected by USDA. We are required to use ONLY approved providers.

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

No tools are implemented to analyze data.

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

Publicly available Zip code data is used by the system to ensure the correct codes are used to match with the city and state that supplied by the user. The zip code provided is matched with the FMS data to verify the city and state.

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

This application is in compliance with the Federal Information Security Management Act of 2014 (FISMA), USDA Office of the Chief Information Officer (OCIO) Directives, and U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4 guidance: • Access Control (AC)
• Awareness and Training (AT)
• Audit and Accountability (AU)
• Security Assessment and Authorization (CA)
• Configuration Management (CM)
• Contingency Planning (CP)
• Identification and Authentication (IA)
• Incident Response (IR)
• Maintenance (MA)
• Media Protection (MP)
• Physical and Environmental Protection (PE)
• Planning (PL)
• Personnel Security (PS)
• Risk Assessment (RA)
• System and Services Acquisition (SA)
• System and Communication Protection (SC)
• System and Information Integrity (SI)

NIST 800-53, Appendix J, Revision 4 controls include: • Authority and Purpose (AP)
• Accountability, Audit, and Risk management (AR)
• Data Quality and Integrity (DI)
• Data Minimization and Retention (DM)

- Individual Participation and Redress (IP)
- Security (SE)
- Transparency (TR)
- Use Limitation (UL)

If any residual risks are identified, they will be managed and reported via the FISMA mandated risk assessment processes.

The controls listed in this section shall be implemented in compliance with Federal and USDA standards regardless of deployment environment.

Section 3.0 Retention

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

3.1 How long is information retained?

Due to a business decision, the retention period is indefinite.

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

Disposal is TBD. Retention period is consistent with requirements given at: http://www.archives.gov/about/laws/disposal-of-records.html#!ists

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

- The risks associated with this application are LOW TO MODERATE. The data that is collected from the requesting public is the minimum required to ship conservation-related publications. Most of the address information supplied by users belongs to schools, institutions or NRCS offices, and thus is publicly available via phone books or the internet.
- This is LOW TO MODERATE because the minimal risks that exist related to this PII are mitigated by the design of this application, which ensures that only the minimum required amount/type of data is collected to meet the requirement of distributing publications to the requesting public.
- System owner may consider modifying the request form to indicate that only one address is necessary-the "shipping address." Noted that the data columns are called address, address2, address3 and address4. However, they all refer to a 'single address' and are multiple address lines of the same address. The system could, in fact, be updated to call it "ship-to-address."

- It may be thought that the "internal system-generated numeric customer/user ID which allows system owner to track the individual. However, the ability to track the individual is limited since the customer information is stored in a secure SQL Server database in the USDA NITC enterprise data center in Kansas City.
- This Information System (i.e. this application) is hosted by ITS, and is covered by the ITS Service Level Agreement (SLA) that has been uploaded in CSAM

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Not applicable, information is not shared internally

4.2 How is the information transmitted or disclosed?

Not applicable

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Security Risk are nominal since information is not shared internally.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

The information is securely shared with UPS, the shipping carrier; Information is only used to generate shipping labels and tracking numbers

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the

program or system is allowed to share the personally identifiable information outside of USDA.

The sharing of PII with UPS is completely compatible with the purpose of the original collection of data, since UPS needs the address information to ship the package. This is covered by an appropriate routine use in the NRCS SORN.

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

The information is securely shared with UPS via an HTTPS web service call.

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

The minimal risks that exist related to sharing of this PII externally with UPS are mitigated because this information is used only for the purpose of generating a shipping label using a secure web service call hosted and provided by UPS. Risks also include the internal threat - Since "UPS is the authoritative carrier for USDA," UPS ensures that backgrounds are checked. Human error and natural disasters are also risks. This answer was checked against the NRCS-1 SORN and is consistent with the SORN.

Section 6.0 Notice

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

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

This is covered by the NRCS-1 SORN. The NRCS System of Record Notice is accessible at: https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS-1.txt .

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

Yes. Notice is stated on the website: 'We collect information in order to ship the requested products and contact requesters if there is a problem. We share this information with UPS in order to generate a tracking number. We do not share the information with anyone else."

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

Yes

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

The user has the right to consent to the SOLE use of this information, which is to ensure that the publication is shipped to the address of their choice. A level 2 eAuth is required to access the information. It is assumed that the user is trusted to use the information appropriately.

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

Notice is given upon users accessing the system. We treat all user information in a secure manner as described above. A banner is on the Web site. Also, this is verbally presented to callers as well when they call to order.

Section 7.0 Access, Redress and Correction

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

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

Users may call the distribution center and verify/update their information. Administrator users of the application can then modify the information, if necessary. The NRCS distribution center is the physical location of the warehouse. All shipments originate there and all business in conducted out of that location. The NRCS distribution center is located in Urbandale, Iowa. Rules of behavior are expected to be adhered to regarding PII information. Administrators are not to provide information to callers.

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

An administrator user securely edits the information.

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

Instructions for contacting the distribution center are prominently displayed on the PDS website. This is covered by an appropriate routine use in the NRCS SORN.

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

Not applicable, risk of a possible formal redress is very low.

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

One possible risk is unauthorized system access through the USDA OCIO eAuthentication system. Access authentication is not an NRCS controlled feature, but a service provided to NRCS Applications by the USDA OCIO eAuthentication system at the Department level for all Applications with personal information. The USDA OCIO eAuthentication PIA is available at http://www.usda.gov/documents/ eAUTH_PIA.doc.

A second possible risk is improper identification through the USDA OCIO eAuthentication system. Individuals are identified via personal contact and documents by Local Registration Authorities (LRA) as described at https:1/app.eauth.egov.usda.gov!AccountServices!MainPages/eauthWhatlsLRA.as px. Local Registration Authorities (LRAs) are USDA employees who are trained to act as the trusted entity to validate the identity of a customer seeking a level 2 eAuthentication account. The role of the LRA can be compared to a Notary Public who ensures the identity of an individual conducting official business transactions. This process is called "identity proofing". Training and a list of approved forms of photo identification for Identity proofing Services for USDA eAuthentication mitigate this risk.

Section 8.0 Technical Access and Security

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

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

Anyone may access the public ordering system. A level 2 eAuth is required to access the administration application. A Secure Socket Layer (SSL) is also available.

8.2   Will Department contractors have access to the system?

Yes.

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

Mandatory Information Security Awareness (ISA) training, annually provided by AgLearn and written PII training/Rules of Behavior for system users.

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

Yes; the initial ATO was awarded in March 2014.

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

- NRCS complies with the "Federal Information Security Management Act of 2014" (FISMA). Assessment and Accreditation, as well as annual key control self-assessments, and continuous monitoring procedures are implemented for this application per the requirements given in National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4.
- NRCS complies with the specific requirements for "auditing measures and technical safeguards" that are provided in OMB M-07-16, including the security requirement that all data on mobile computers/devices containing agency data must be encrypted using only NIST certified cryptographic modules.
  - **Encryption** that is performed outside of the accreditation boundary of this application is discussed in Section 8.6 below. Given the limited sensitivity and scope of the information retained, this application does not encrypt PII within the database.
  - **Controlled access** to PII is implemented outside the accreditation boundary of this application (e.g., via multi-factor authentication for remote access). While the PII information retained has limited sensitivity and scope (i.e., the Name of non-employee "affiliates"), this application does control (limit) access to PII. The access of an Affiliate user (i.e., an NRCS employee) is generally limited to the "scope" of their office.
  - **Timeout for remote access** is implemented outside of the accreditation boundary of this application (e.g., by eAuth), so this application does not need to implement timeout for remote access to PII due to inactivity.
  - **System audit logs** are implemented outside of the accreditation boundary of this application. This includes internal audit logs that are used to ensure that administrative functions and activities are being logged and monitored (e.g., modifications, additions, and deletions of privileged accounts per the eAuthentication SLA). Given the limited sensitivity and scope of the information retained, this application does not implement system audit logs related to PII integrity, nor does this application implement a Security Information and Event Management (SIEM) log management system.

8.6 <u>**Privacy Impact Analysis**</u>**: 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?**

- The sensitivity and scope of the information collected is LOW TO MODERATE as the minimal risks that exist related to this PII are mitigated by the design of this application. The design ensures that only the minimum required amount/type of data is collected to meet the requirement of distributing publications to the requesting public.
- Noted that the data columns are called address, address2, address3 and address4. However, they all refer to a 'single address' and are multiple address lines of the same address. The system could, in fact, be updated to call it "ship-to-address."
- It may be thought that the "internal system-generated numeric customer/user ID which allows system owner to track the individual. However, the ability to track the individual is limited since the customer information is stored in a secure SQL Server database in the USDA NITC enterprise data center in Kansas City.
- The minimal risks that exist related to this PII are mitigated by the design of this application, which ensures that only the minimum required amount/type of data is collected to meet the requirement of distributing publications to the requesting public. The customer information is stored in a secure SQL Server database in the USDA enterprise data center in Kansas City. The risks that exist related to sharing of this PII externally with UPS are mitigated because this information is used only for the purpose of generating a shipping label using a secure web service call hosted and provided by UPS.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1   What type of project is the program or system?

- The Publication Distribution System accepts requests/orders for items (brochures, posters, DVDs, etc.) from the public via the Internet and by phone, and ships the requested items via USPS or UPS.
- The Administration site is an asp.net application using mvc (Model View Controller, http://www.asp.net/mvc/tutorials/overview/asp-net-mvc-overview), entity framework (architecture) and SQL server. The public site is an asp.net application using entity framework and SQL server.

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

No.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes.

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

The application uses UPS's web service to generate shipping labels and tracking numbers for items that are shipped via UPS:
http://www.ups.com/content/us/en/resources/ship/terms/privacy.html

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

Shipping information is made available via secure web services to UPS for the purpose of shipping publications. This information includes Name, Address, phone, and email address.

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

Shipping information is made available via secure web services to UPS for the purpose of shipping publications, in order to create shipping labels/records, and tracking numbers.

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

Only the minimum required amount/type of data is shared with UPS to meet the requirement of distributing publications to the requesting public. UPS meets all PCI-Data Security Standard (DSS) requirements. Data is purged according to UPS policy.

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

PII that is shared with UPS is purged according to UPS policies.

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

The original requester of publications receives a tracking number from UPS via NRCS. That user's PII is viewable through the use of that tracking number. Administrative users can view all data (with level 2 eAuth). General public users may only access via tracking number.

10.8 **With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?**

The PII that is made available to UPS is governed by UPS's privacy policies which are consistent with USDA approved policy.

10.9 **Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?**

Not applicable, a third party application or website is not utilized.

10.10 **Does the system use web measurement and customization technology?**

Not applicable, a third party application or website is not utilized.

10.11 **Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?**

Not applicable web measurement and customization technology is not used.

10.12 <u>**Privacy Impact Analysis**</u>**: 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.**

Risk are nominal as Third Party Websites and Applications are not utilized by this system.

Agency Responsible Officials

_____

Jake Zebell
PDS Information System Owner
United States Department of Agriculture

Agency Approval Signature

_____

Lanita Thomas
Information Systems Security Program Manager
United States Department of Agriculture

Agency Privacy Approval Signature

_____

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture