Privacy Impact Assessment for the VA IT System called:

Pitney Bowes Send Pro - Enterprise

Enterprise Mail Management

Date PIA submitted for review:

February 23, 2021

System Contacts:

<table>
<thead>
<tr>
<th>System Contacts</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Rita Grewal</td>
<td><a href="mailto:Rita.Grewal@va.gov">Rita.Grewal@va.gov</a></td>
<td>202-632-7861</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Mark McGee</td>
<td><a href="mailto:James.McGee5@va.gov">James.McGee5@va.gov</a></td>
<td>520-629-4834</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Terrill Harrison</td>
<td><a href="mailto:Terrill.Harrison@va.gov">Terrill.Harrison@va.gov</a></td>
<td>202-461-5468</td>
</tr>
</tbody>
</table>
Abstract

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

Pitney Bowes Send Pro - Enterprise is a mailing solution that consist of Commercial-Off-The-Shelf (COTS) and Software-as-a-Service (SaaS) which generates mailing indices and shipping labels, provides best cost shipping options, allows for accurate reporting, accountability of volume and expenditures of mail and parcels. Mailing equipment, products and services collect PII/PHI mailing metrics (number of letters/packages mailed, cost for mailing) and collates the data within the SaaS tool to provide a single solution for sending mail and streamlining the mailing process allowing mail management at the VA Enterprise Level.

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 overview should contain the following elements:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes
- Whether the completion of this PIA could potentially result in technology changes
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?
- Does the system use cloud technology? If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.
- Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
• **NIST 800-144** states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?

• **What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?**

Pitney Bowes Send Pro - Enterprise facilitates VA Mail operations by increasing the efficiency of the mailing process such as printing compliant labels and postage to be placed on parcels, letters, and flats being sent via US Mail or shipping vendors. The information used and stored in the application includes United States Postal Service (USPS), FedEx, DHL, and United Parcel Service (UPS) Tracking Number, USPS/shipping vendor service type (e.g., First Class mail, Priority Mail, etc.), USPS/shipping vendor service type add-on information (e.g., Registered Mail, Certified Mail, etc.) mail recipient (addressee) name, mail recipient mailing street address and zip code, weight of the package, the date and time of packages, parcels, and letters sent, and value of postage used to send a parcel. The mailing COTS equipment and SaaS software application the VA uses to provides the solution for sending mail and streamlining the mailing processing. The application will handle and store mail and delivery service labeling associated with VA’s use of United Parcel Service (UPS), United States Postal Service (USPS) and other like delivery services. The application will also store tracking information and system user authentication information. The types of information the application collects, maintains and shares are the names, addresses and phone numbers for members of the public who receive mail from the VA’s mail operations. They will also track the number of pieces mailed and the costs by piece and overall costs. The system will also hold the VA office mailing address for agency offices sending mail and in some cases the names of individual employees sending outbound mail. The mailing solution is VA Enterprise solution with expected usage in VA Medical Centers, National Cemeteries, Regional Offices, etc. that have mail operations. The mailing solution collects, maintains, uses or shares non-PHI and PII. The type of PII are names, Mailing Addresses, Phone Numbers, VA personnel (user) login information (Username and Password).

The Pitney Bowes Send Pro – Enterprise SaaS software application uses cloud technology. Pitney Bowes Send Pro - Enterprise is hosted on Amazon Web Services East/West, and a FedRAMP ATO is in process at a moderate impact level. A FedRAMP ATO is expected to be granted in May 2021.

**Section 1. 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.

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

*Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series ([https://vaww.va.gov/vapubs/](https://vaww.va.gov/vapubs/)). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.*
If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system. This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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

- Name
- Social Security Number
- Date of Birth
- Mother’s Maiden Name
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Fax Number
- Personal Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial Account Information
- Health Insurance Beneficiary Numbers
- Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Other Unique Identifying Number (list below)

VA personnel user logon information (Username and Password).

**PII Mapping of Components**

Pitney Bowes Send Pro - Enterprise consists of 4 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Pitney Bowes Send Pro - Enterprise and the reasons for the collection of the PII are in the table below.

**PII Mapped to Components**

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Mailing Address, Phone Numbers</td>
<td>Comply with UPS, USPS regulations General Service Administration (GSA) Schedule</td>
<td>User training, system document; implementation role-based access settings, firewalls,</td>
</tr>
<tr>
<td>Public Citizens</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Mailing Address, Phone Numbers</td>
<td>Comply with UPS, USPS regulations</td>
<td>General Services Administration (GSA) Schedule 48, Next Generation Delivery Service (NGDS)</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----</td>
<td>-----</td>
<td>-------------------------------------</td>
<td>-------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Business Partners/Contracts (Federal/State/Local Agencies)</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Mailing Address, Phone Numbers</td>
<td>Comply with UPS, USPS regulations</td>
<td>General Services Administration (GSA) Schedule 48, Next Generation Delivery Service (NGDS)</td>
</tr>
<tr>
<td>Vendors/Suppliers/Contractors</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Mailing Address, Phone Numbers</td>
<td>Comply with UPS, USPS regulations</td>
<td>General Services Administration (GSA) Schedule 48, Next Generation Delivery Service (NGDS)</td>
</tr>
</tbody>
</table>
1.2 What are the sources of the information in the system?

List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The information originates from VA business systems, address books, directories, and other programs supplying name and addresses and is entered into the system and subsequently provided to Pitney Bowes. Application data may be used for testing or training in a secure test environment and zip codes of mailing recipients may be used for determining and forecasting postage expenses. VA’s use of information in Pitney Bowes Send Pro - Enterprise is authorized by 5 U.S.C. 301 which permits agency heads to create the usual and expected infrastructure necessary for the organization to accomplish its purposes and mission. In addition, the security and privacy measures for the system are required by the Federal Information Security Management Act (FISMA) and the statutes underlying OMB Circular A-130 for the secure and efficient use of government systems and resources.

1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?
If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number. 
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The Sources of information is collected by Hardcopy directly from the individual about whom the information pertains, the Government Sources are collected within the Enterprise Mail Management program office and the Non-Government Sources are collected from the public.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose. This question is related to privacy control AP-2, Purpose Specification.

The information is used to comply with shipping vendor and USPS regulations for successfully sending parcels, letters, and flats via US Mail in accordance with Federal Management Regulations (FMR 102-192). The application data may be used for testing or training in a secure test environment. Zip codes of mailing recipients may be used for determining and forecasting postage expenses.

1.5 How will the information be checked for accuracy? How often will it be checked?

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract. This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

There is no process in place due to short duration of handling information. Current records control schedules have such data being destroyed after 2 years (and sometimes less) in most situations.

1.6 What specific legal authorities, arrangements, and agreements defined the collection of information?
List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.

This question is related to privacy control AP-1, Authority to Collect

VA’s use of information in Pitney Bowes Send Pro - Enterprise is authorized by 5 U.S.C. 301 which permits agency heads to create the usual and expected infrastructure necessary for the organization to accomplish its purposes and mission. In addition, the security and privacy measures for the system are required by the Federal Information Security Management Act (FISMA) and the statutes underlying OMB Circular A-130 for the secure and efficient use of government systems and resources.

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: Name and mailing address are well established publicly accepted standard PII elements needed to send parcels, letters, and flats via US mail with USPS or shipping vendors. Members of the public are aware of and voluntarily provide their name and address when corresponding with the VA.

Mitigation: The system only collects PII in accordance with shipping vendor and USPS regulations. The VA relies on shipping vendor and USPS to adequately communicate any changes in their regulations to the public.
Section 2. Uses of the Information

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

2.1 Describe how the information in the system will be used in support of the program’s business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained.
This question is related to privacy control AP-2, Purpose Specification.

The information in the system will facilitate VA mail operations by increasing the efficiency of the mailing process such as printing compliant labels and postage to be placed on parcels, letters, and flats being sent via US Mail or shipping vendors. Business rules on carrier usage will be monitored and enforced to ensure compliance to policy. The system will modernize and transform VA’s mail operations by standardizing and integrating mail centers across the VA enterprise. The information in the system will establish trends on key performance indicators over time to maintain a cycle of continuous improvement and drive operational excellence.

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

Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual’s existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The system meters mail, provides best cost shipping options, allows for accurate reporting, accountability of volume and expenditures of mail and parcels. Mailing equipment, products and services collect mailing metrics (number of letters/packages mailed, cost for mailing) and collates the data within the SaaS tool to provide a single solution for viewing aggregate mail data at the VA Enterprise Level.

In reference to above: If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual’s existing record? Logon credentials remain available as long each user
has authorized access to the system. Credentials are revoked when access is no longer needed, including if individual moves a different office within VA or leaves employment.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

**Principle of Transparency:** Is the PIA and SORN, if applicable, clear about the uses of the information?

**Principle of Use Limitation:** Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

The system has the minimum amount of information necessary to mail documents which are the name, mailing address, and phone number for recipients. This information is required in printing USPS and shipping vendor compliant postage labels. Access to the PII is determined by Business System owner who will review all user account request, which contain justification, and utilize their subject matter expertise to determine in a “need to know” before granting access. Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical safeguards include role-based access settings, firewalls, and passwords. Other appropriate controls have been selected from the National Institute of Standards and Technology’s (NIST’s) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199. Technical settings ensure that only Administrators are allowed to reset the password for users if needed.

**Section 3. Retention of Information**

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

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system.
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

The information that is retained in the system is Name, Mailing Address, Phone Numbers, weight date and time of the package, letter, or flat, and VA personnel (user) logon information (Username and Password).

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

This question is related to privacy control DM-2, Data Retention and Disposal.

Logon credentials remain available as long each user has authorized access to the system. Credentials are revoked when access is no longer needed, including if individual moves a different office within VA or leaves employment.

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

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.

This question is related to privacy control DM-2, Data Retention and Disposal.

The retention schedule has been approved by the NARA. The guidance for retention of records is found in the Records Control Schedule 10-1 [http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf](http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf) and NARA: [https://www.archives.gov/records-mgmt/grs.html](https://www.archives.gov/records-mgmt/grs.html)

Official record held in the office of record. Temporary; destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use. (GRS 1.1, Item 010 [https://www.archives.gov/](https://www.archives.gov/) (DAA-GRS-2013-0003-0001)

According to VA Handbook 6500, once records are entered into the system they remain as part of the protected system information. System logs are maintained for one year and then flagged for deletion by their automated processes. System logs are not retained after one year and any SPI containing them will be overwritten as part of the process for audit management. When virtual machines are no longer required to support the system they are wiped clean and the data overwritten. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans’
Affairs VA Directive 6371, (April 8, 2014),
https://www.va.gov/digitalstrategy/docs/VA_Directive_6500_24_Jan_2019.pdf  In addition, any equipment that is decommissioned and is leaving the controlled data center will be sanitized (e.g., degaussing) or destroyed in accordance with VA Handbook 6500 and the Veterans Affairs Dedicated Cloud Media Sanitization Procedure. VA Dedicated Cloud Media Sanitization policy outlines the VA Dedicated Cloud policy and procedure for tracking, documentation and disposal of storage media within the environment and their return to the VA, in accordance with VA Handbook 6500.

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?
This question is related to privacy control DM-2, Data Retention and Disposal

The VA records office will be consulted, and process for destroying or eliminating records will be documented as requested. More information on how to reach out can be found at https://www.va.gov/records/.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

All personnel will take mandatory annual Information Security Awareness and Records Management Training. In addition, administrators with privileged accounts will be required to take role-based training annually to maintain account access. The Pitney Bowes Send Pro – Enterprise system provides training for proper use of the system. VA personnel may take advantage of information security and privacy awareness events and workshops held within VA.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.
Consider the following FIPPs below to assist in providing a response:

**Principle of Minimization:** Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

**Principle of Data Quality and Integrity:** Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged? This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

**Privacy Risk:** Pitney Bowes Send Pro - Enterprise retains only the minimum amount of information necessary in order to mail documents which are name, mailing address, and phone numbers for recipients. Logon credentials remain available as long as each user has authorized access to the system. Credentials are revoked when access is no longer needed.

**Mitigation:** Records are maintained under NARA GRS 20, Item 1c; superseded by the new GRS 3.2, item 030, which is for records created as part of their user identification and authorization process to gain access to systems. Retention is until “business use ceases”. NARA concurs that agencies may dispose of these records as soon as they are no longer needed. NARA Approved citation GRS 23-8. Disposition: Temporary, destroy or delete when 2 years old, or 2 years after the date of the latest entry, whichever is applicable.

**Section 4. Internal Sharing/Receiving/Transmitting and Disclosure**

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

**4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?**

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise mail Management Program Office</td>
<td>VA Mail Operations</td>
<td>Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)</td>
<td>https</td>
</tr>
<tr>
<td>Veterans’ Benefits Administration (VBA)</td>
<td>VA Mail Operations</td>
<td>Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)</td>
<td>https</td>
</tr>
<tr>
<td>Veterans’ Health Administration (VHA)</td>
<td>VA Mail Operations</td>
<td>Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)</td>
<td>https, sftp</td>
</tr>
<tr>
<td>National Cemetery Administration (NCA)</td>
<td>VA Mail Operations</td>
<td>Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)</td>
<td>https</td>
</tr>
<tr>
<td>Staff Offices</td>
<td>VA Mail Operations</td>
<td>Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)</td>
<td>https</td>
</tr>
</tbody>
</table>

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure
Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. This question is related to privacy control UL-1, Internal Use.

Follow the format below:

**Privacy Risk:** The information used and stored in the application includes United States Postal Service (USPS), FedEx, DHL, and United Parcel Service (UPS) Tracking Number, USPS/shipping vendor service type (e.g., First Class mail, Priority Mail, etc.), USPS/shipping vendor service type add-on information (e.g., Registered Mail, Certified Mail, etc.) mail recipient (addressee) name, mail recipient mailing street address and zip code, and value of postage used to send a parcel. The mailing COTS equipment and SaaS software application the VA uses to provides the solution for sending mail and streamlining the mailing processing. The application will handle and store mail and delivery service labeling associated with VA’s use of United Parcel Service (UPS), United States Postal Service (USPS) and other like delivery services. The application will also store tracking information and system user authentication information. The types of information the application collects, maintains and shares are the names, addresses and phone numbers for members of the public who receive mail from the VA’s mail operations. They will also track the number of pieces mailed costs by piece and overall costs. The system will also hold the VA office mailing address for agency offices sending mail and in some cases the names of individual employees sending outbound mail, in addition to username and login information for VA employees using the system.

**Mitigation:** The system has the minimum amount of information necessary to mail documents which are the name, mailing address, and phone number for recipients. This information is required in printing shipping vendors compliant postage labels. Access to the PII is determined Business System owner who will review all user account request, which contain justification, and utilize their subject matter expertise to determine in a “need to know” exist before granting access. Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical safeguards include role-based access settings, firewalls, and passwords. Other appropriate controls have been selected from the National Institute of Standards and Technology’s (NIST’s) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199. Technical settings ensure that only Administrators are allowed to reset the password for users if needed.

**Section 5. External Sharing/Receiving and Disclosure**

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

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

Version Date: February 27, 2020  
Page 15 of 28
Note: This question is #7 in the Privacy Threshold Analysis.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties.
## Data Shared with External Organizations

<table>
<thead>
<tr>
<th>Program Office or IT System</th>
<th>Purpose of Information Shared</th>
<th>Specific Data Element Types</th>
<th>Legal Authority, Binding Agreement, SORN Routine Use, etc. That Permit External Sharing (Can Be More Than One)</th>
<th>Method of Transmission and Measures in Place to Secure Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pitney Bowes Send Pro - Enterprise</td>
<td>Sending Parcels/Mail</td>
<td>Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)</td>
<td>National MOU/ISA</td>
<td>Site to Site (S2S)</td>
</tr>
<tr>
<td>United States Postal Service (USPS)</td>
<td>Sending Parcels/Mail</td>
<td>Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)</td>
<td>5, U.S.C. 301 Federal Information Security Management Act (FISMA) OMB Circular A-130</td>
<td>User Training System Documentation Need to Know Minimum Necessary Principles Role-based Access Settings Firewalls</td>
</tr>
<tr>
<td>United Parcel Service (UPS)</td>
<td>Sending Parcels/Mail</td>
<td>Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)</td>
<td>5, U.S.C. 301 Federal Information Security Management Act (FISMA) OMB Circular A-130</td>
<td>User Training System Documentation Need to Know Minimum Necessary Principles Role-based Access Settings Firewalls</td>
</tr>
<tr>
<td>Federal Express (FedEx)</td>
<td>Sending Parcels/Mail</td>
<td>Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)</td>
<td>5, U.S.C. 301 Federal Information Security Management Act (FISMA) OMB Circular A-130</td>
<td>User Training System Documentation Need to Know Minimum Necessary Principles Role-based Access Settings Firewalls</td>
</tr>
</tbody>
</table>
If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

The Director and Business System Owner review all user account request, which contain justification. All personnel take mandatory Information Security Awareness and Records Management Training.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure
Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

**Privacy Risk:** The mailing COTS equipment and SaaS software application uses cloud technology to provide a single solution for sending mail and streamlining the mailing process.

**Mitigation:** The Pitney Bowes SendPro – Enterprise system is FedRAMP “In Process”. As such Pitney Bowes has developed a System Security Plan and supporting documents that comply with 325 FedRAMP Moderate controls across 17 control families plus additional VA-Specific controls. These include comprehensive access and audit families of controls. Pitney Bowes SendPro - Enterprise is undergoing rigorous, independent third-party audit that includes testing, examination, evidence and pen testing. FedRAMP access, audit, and other controls are followed and evidenced continually, weekly, monthly, quarterly, etc. as prescribed by the FedRAMP Moderate impact SSP statements. VA Authority to Operate is expected May 2021.

**Section 6. 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.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?
This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.

If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

No prior notice is provided. Name and mailing address are well established publicly accepted standard PII elements needed to send parcels, letters, and flats via US mail with shipping vendors. Members of the public are aware of and voluntarily provide their name and address when corresponding with the VA. The submission of PII is Voluntary and if the recipient would like to request to opt-out of receiving mail from the VA, they may notify the VA sender to not send them mail via US Mail or shipping vendor.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

The submission of information is Voluntary and if the recipient would like to request to opt-out of receiving mail from the VA, they may notify the VA sender via mail or contact number to not send them mail via US Mail or delivery service and there is no penalty or denial of service.

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

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

The submission of information is Voluntary and if the recipient would like to request to opt-out of receiving mail from the VA, they may notify the VA sender via mail or contact number to not send them mail via US Mail or other delivery services.

6.4 PRIVACY IMPACT ASSESSMENT: Notice
Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

Consider the following FIPPs below to assist in providing a response:

**Principle of Transparency**: Has sufficient notice been provided to the individual?

**Principle of Use Limitation**: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

**Privacy Risk**: The system only collects information in accordance with shipping vendor and USPS regulations.

**Mitigation**: The VA relies on shipping vendor and USPS to adequately communicate any changes in their regulations to the public.

### Section 7. Access, Redress, and Correction

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

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

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency’s FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency’s procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

The submission of information is Voluntary and if the recipient would like to request to opt-out of receiving mail from the VA, they may notify the VA sender via mail or contact number to not send them mail via US Mail or other delivery services.
7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The submission of information is Voluntary and if the recipient would like to request to opt-out of receiving mail from the VA, they may notify the VA sender via mail or contact number to not send them mail via US Mail or other like delivery services. The system only collects information in accordance with shipping vendor and USPS regulations. The VA relies on USPS and shipping vendors to adequately communicate any changes in their regulations to the public.

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The system only collects information in accordance with shipping vendor and USPS regulations. The VA relies on shipping vendor and USPS to adequately communicate any changes in their regulations to the public.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.

Individuals may contact VA using contact information available on VA.gov and by phone.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department’s access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program’s effectiveness because the individuals involved might change their behavior.
Consider the following FIPPs below to assist in providing a response:

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: The submission of information is Voluntary, and the system only collects information in accordance with shipping vendor and USPS regulations.

Mitigation: If the recipient would like to request to opt-out of receiving mail from the VA, they may notify the VA sender via mail or contact number to not send them mail via US Mail or other shipping vendors. The system only collects information in accordance with shipping vendor and USPS regulations. The VA relies on shipping vendors and USPS to adequately communicate any changes in their regulations to the public.

Section 8. 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?

Describe the process by which an individual receives access to the system.

Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

The system has the minimum amount of information necessary to mail documents which are the name, mailing address, and phone number for recipients. This information is required in printing USPS compliant postage labels. Access to the information is determined Business System owner who will review all user account request, which contain justification, and utilize their subject matter
expertise to determine in a “need to know” exist before granting access. Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical safeguards include role-based access settings, firewalls, and passwords. Other appropriate controls have been selected from the National Institute of Standards and Technology’s (NIST’s) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199. Technical settings ensure that only Administrators are allowed to reset the password for users if needed. If a user that is not given access to the Active Directory group attempts to access the link, the application will open but they will not be able to log into it.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Contractors will have access to the Pitney Bowes Send Pro - Enterprise system. The PII access is the same as they currently hold while performing mail duties as a mail clerk or mail supervisor in a VA Mail Center. Most contractors do have NDAs in place already.

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

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.

This question is related to privacy control AR-5, Privacy Awareness and Training.

All personnel take mandatory Information Security Awareness and Records management Training. Administrators with privileged accounts are required to take role-based training annually to maintain account access.

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

If Yes, provide:

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

Please note that all systems containing SPI are categorized at a minimum level of “moderate” under Federal Information Processing Standards Publication 199.

If No or In Process, provide your Initial Operating Capability (IOC) date.

Authorization and Accreditation (A&A) has not been completed for the system. It is categorized as ‘moderate’ impact and is in process to receive an ATO in May 2021. The system is currently in development at VA.
### Section 9. References

#### Summary of Privacy Controls by Family

<table>
<thead>
<tr>
<th>ID</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td>Authority and Purpose</td>
</tr>
<tr>
<td>AP-1</td>
<td>Authority to Collect</td>
</tr>
<tr>
<td>AP-2</td>
<td>Purpose Specification</td>
</tr>
<tr>
<td>AR</td>
<td>Accountability, Audit, and Risk Management</td>
</tr>
<tr>
<td>AR-1</td>
<td>Governance and Privacy Program</td>
</tr>
<tr>
<td>AR-2</td>
<td>Privacy Impact and Risk Assessment</td>
</tr>
<tr>
<td>AR-3</td>
<td>Privacy Requirements for Contractors and Service Providers</td>
</tr>
<tr>
<td>AR-4</td>
<td>Privacy Monitoring and Auditing</td>
</tr>
<tr>
<td>AR-5</td>
<td>Privacy Awareness and Training</td>
</tr>
<tr>
<td>AR-7</td>
<td>Privacy-Enhanced System Design and Development</td>
</tr>
<tr>
<td>AR-8</td>
<td>Accounting of Disclosures</td>
</tr>
<tr>
<td>DI</td>
<td>Data Quality and Integrity</td>
</tr>
<tr>
<td>DI-1</td>
<td>Data Quality</td>
</tr>
<tr>
<td>DI-2</td>
<td>Data Integrity and Data Integrity Board</td>
</tr>
<tr>
<td>DM</td>
<td>Data Minimization and Retention</td>
</tr>
<tr>
<td>DM-1</td>
<td>Minimization of Personally Identifiable Information</td>
</tr>
<tr>
<td>DM-2</td>
<td>Data Retention and Disposal</td>
</tr>
<tr>
<td>DM-3</td>
<td>Minimization of PII Used in Testing, Training, and Research</td>
</tr>
<tr>
<td>IP</td>
<td>Individual Participation and Redress</td>
</tr>
<tr>
<td>IP-1</td>
<td>Consent</td>
</tr>
<tr>
<td>IP-2</td>
<td>Individual Access</td>
</tr>
<tr>
<td>IP-3</td>
<td>Redress</td>
</tr>
<tr>
<td>IP-4</td>
<td>Complaint Management</td>
</tr>
<tr>
<td>SE</td>
<td>Security</td>
</tr>
<tr>
<td>SE-1</td>
<td>Inventory of Personally Identifiable Information</td>
</tr>
<tr>
<td>SE-2</td>
<td>Privacy Incident Response</td>
</tr>
<tr>
<td>TR</td>
<td>Transparency</td>
</tr>
<tr>
<td>TR-1</td>
<td>Privacy Notice</td>
</tr>
<tr>
<td>TR-2</td>
<td>System of Records Notices and Privacy Act Statements</td>
</tr>
<tr>
<td>TR-3</td>
<td>Dissemination of Privacy Program Information</td>
</tr>
<tr>
<td>UL</td>
<td>Use Limitation</td>
</tr>
<tr>
<td>ID</td>
<td>Privacy Controls</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>UL-1</td>
<td>Internal Use</td>
</tr>
<tr>
<td>UL-2</td>
<td>Information Sharing with Third Parties</td>
</tr>
</tbody>
</table>
Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

RITA K GREWAL
114938
 Digitally signed by RITA K GREWAL 114938
 Date: 2021.03.25 20:06:35 -04'00'

Privacy Officer, Rita Grewal

James M. McGee 926698
 Digitally signed by James M. McGee 926698
 Date: 2021.03.29 12:08:42 -07'00'

Information Systems Security Officer, Mark McGee

Terrill N. Harrison 1079525
 Digitally signed by Terrill N. Harrison 1079525
 Date: 2021.03.31 09:33:07 -04'00'

System Owner, Terrill Harrison
APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).