Privacy Impact Assessment for the VA IT System called:

Production Print Operations (PPO)

VACO

IT Infrastructure Operations and Services

eMASS ID # 2100

Date PIA submitted for review:

August 27, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	Gina.siefert@va.gov	(202) 632-8430
Information System Security Officer (ISSO)	Eric Abraham	Eric.Abraham@va.gov	512-326-7422
Information System Owner	Pete Sevilla	Peter.Sevilla@va.gov	708-483-5137

Abstract

The abstract provides the simplest explanation for "what does the system do?".

A product that manages print output and ensures the efficient and timely delivery of business-critical documents to the intended printing device or other destination. The purpose is to transform data streams into print files and pass them on to a large-scale production printing devices within the VA or an authorized contractor who provides print and mail services where Veteran letters are printed and mailed. Recipient name and address is collected on our server for reference should a privacy incident arise so we can trace the recipient to a print file and research the cause of the privacy incident.

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:

1 *General Description*
   A. *What is the IT system name and the name of the program office that owns the IT system?*
   Production Print Operations (PPO) – IT Infrastructure Operations and Services

   B. *What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*
   A product that manages print output and ensures the efficient and timely delivery of business-critical documents to the intended printing device or other destinations. PPO provides the data owner an output to print and mail their completed product at a designated print location.

   The purpose is to transform data streams into print files and pass them on to a large-scale production printing devices within the VA or an authorized contractor who provides print and mail services where Veteran letters are printed and mailed.
   C. *Who is the owner or control of the IT system or project?*
   VA Owned and VA Operated Information System

2. *Information Collection and Sharing*
   D. *What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?*
   100 Users. 3,000,000 Unique Records that have name and address of veterans receiving letters from the VA.

   E. *What is a general description of the information in the IT system and the purpose for collecting this information?*

A product that manages print output and ensures the efficient and timely delivery of business-critical documents to the intended printing device or other destinations. PPO provides the data owner an output to print and mail their completed product at a designated print location. The purpose is to transform data streams into print files and pass them on to a large-scale production printing devices within the VA or an authorized contractor who provides print and mail services where Veteran letters are printed and mailed. Recipient name and address is collected on our server for reference should a privacy incident arise so we can trace the recipient to a print file and research the cause of the privacy incident.

F. *What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.*

No Information is Shared across to other systems. The system does receive data internally from Veterans Benefits Administration, Veterans Health Administration, and Debt Management Center. The system shares data externally with NPC Inc Server and CCG Server

G. *Is 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?*

The Austin Information Technology Center (AITC) is the primary hosting site. The Philadelphia Information Technology Center (PITC) is the alternate site should the primary site become unavailable.

3. *Legal Authority and SORN*

H. *What is the citation of the legal authority to operate the IT system?*

The legal authority to operate this IT System is: Federal Managers Financial Integrity Act of 1982 (FMFIA) • OMB Circular A-123 - "Internal Control Systems" • OMB Circular A-130 - "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources" • Federal Information Security Management Act of 2002 (FISMA) (Title III, 2002 E-Gov Act) • OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002. The following SORNs are applicable as well:

24VA10A7/85 FR 62406 Patient Medical Records-VA
27VA047/ 77 FR 39346 Personnel and Accounting Integrated Data System-VA
41VA41/87 FR 10283 Veterans and Dependents National Cemetery Gravesite Reservation Records-VA
58VA21/22/28 86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA
88VA244/ 83 FR 40140 Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO)
168VA005/ 86 FR 6975 Health Information Exchange-VA

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The current SORN needs to be updated. PPO does not use cloud technology. It is hosted at the Austin Information Technology Center (AITC)

4. *System Changes*

J.   *Will the completion of this PIA will result in circumstances that require changes to business processes?*
> There will not be any changes to the business processes for PPO.

K.   *Will the completion of this PIA could potentially result in technology changes?*
> There will not be any changes to the technology currently in use.

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/). 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.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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:

X Name
X Social Security Number
☐ Date of Birth
☐ Mother's Maiden Name
X 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 Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records

☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integrated Control Number (ICN)
☒ Military History/Service Connection
☐ Next of Kin
X Other Data Elements (list below)

---

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

Other Data Elements: Individual File Number
PII Mapping of Components (Servers/Database)

Production Print Operations consists of **0** key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Production Print Operations** and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A	N/A	N/A	N/A	N/A	N/A

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a 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?

The information is not collected directly from an individual. The information is collected from various VA systems across the enterprise to include Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), Debt Management Center (DMC).

1.2b 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 indicate why the system is using this source of data.

This system receives information from various VA systems. PPO provides the data owner an output to batch print and mail their communications at a designated print location. All data is passed to PPO from established VA internal system.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

PPO does not create nor modify any information.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a 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 technologies used in the storage or transmission of information in identifiable form?

    PPO receives the information via electronic transmission from other VA internal systems.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

PPO does not create or collect information on a form.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a 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.

PPO does not examine the files received for accuracy. Files transmitted to PPO are examined by the data owner prior to transmittal.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

    PPO system is not designed to check the information stored. The data owner checks for accuracy utilizing their internal processes.

1.5 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

24VA10A7/85 FR 62406 Patient Medical Records-VA

27VA047/ 77 FR 39346 Personnel and Accounting Integrated Data System-VA

41VA41/87 FR 10283 Veterans and Dependents National Cemetery Gravesite Reservation Records-VA

58VA21/22/28 86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

88VA244/ 83 FR 40140 Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO)

168VA005/ 86 FR 6975 Health Information Exchange-VA

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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. (Work with your System ISSO to complete this section)

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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: PPO does not own, create, or collect the data that contains PII information. PPO provides an output for data owner to print and mail their completed product. All data is collected and stored by the data owner on their designated VA system. If there was an unauthorized access during transmission, there is a potential risk of individual financial harm.

Mitigation: PPO employs a variety of measures to ensure the information is not disclosed or released. These measure includes, physical site visit, privacy awareness training and CSCA. VA enforces two factor authentication for all employees and contractor accessing information.

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 that 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.

PII/PHI Data Element	Internal Use	External Use
Name	File Identification purposes	File Identification purposes
Address	File Identification purposes	File Identification purposes
Social Security Number	File Identification purposes	File Identification purposes
Individual file Number	File Identification purposes	File Identification purposes
Military History/Service Connection	File Identification purposes	File Identification purposes

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a 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?

Not applicable. PPO does not provide or conduct any analysis on data received.

2.2b 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.

PPO's system is not designed to create or make changes to the data, any required changes are made by the owner of the data and retransmitted to the PPO team

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

Data is transmitted utilizing FIPPS-140 encryption

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

PPO uses FIPS 140-2 encryption at rest and in transit. While an SSN may be included in a letter, it is not an individually collected/searchable data element. Under the SSN reduction act, all data owners are actively working to remove SSN from their batch data PPO processes.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

Access to the system is determined by IO Operations Control. Access is based on the user's supporting role in the information system. All system users are required to complete VA Privacy and Information Security Training and Rules of Behavior.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

<u>Principle of Transparency:</u> Is the PIA and SORN, if applicable, clear about the uses of the information?

<u>Principle of Use Limitation:</u> 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.

2.4a How is access to the PII determined?
Access is determined by IO Operations Control based on the user's supporting role in the information system.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?
PPO has an internal SOP outlining a request for access.

2.4c Does access require manager approval?

Yes. PPO staff reviews and approves/disapproves all access requests.

2.4d Is access to the PII being monitored, tracked, or recorded?

Yes. Access is monitored for logons/logoff, transactions performed (i.e. release, print, etc.) of data.

2.4e Who is responsible for assuring safeguards for the PII?

The PPO Supervisor is responsible for safeguarding PII.

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*

Name, Address, Social Security Number, Individual File Number, Military History/ Service Connection

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.** If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

File are retained in the PPO system for 90 days.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

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. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Information retained by PPO cannot be retrieved by a personal identifier. PPO provides the data owner an output to print and mail their completed product at a designated print location. PPO

does not own or maintain the data; record management is done by the data owner. PPO temporarily stores the data for up to 90 days to assist the letter owner in the event of a privacy incident.

3.3b Please indicate each records retention schedule, series, and disposition authority?

PPO provides the data owner an output to print and mail their completed product at a designated print location. PPO does not maintain or store the data permanently; the data is purged from the PPO system after 90 days. The data owner creates and maintains the record management process for their data. https://www.archives.gov/

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory 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.

PPO provides the data owner an output to print and mail their completed product at a designated print location. PPO does not maintain, create, or retain paper copies of the data. The data owner is responsible for managing the destruction of paper copies.

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. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

PPO does not own the data and the PPO system is not designed for testing, training, or research.

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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: There is a risk that data could be kept longer than the intended retention period.

Mitigation: PPO does not maintain or store the data permanently. The data is purged from the PPO system after 90 days.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

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?
NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

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.

List the Program Office or IT System information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT system	List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system	Describe the method of transmittal
Veterans Benefits Information	Batch file for print purposes only	Name Address Social Security Number Individual File Number Military History/ Service Connection	SFTP/TCP/IP Printing Protocol
Veterans Health Administration	Batch file for printing purposes only	Name Address Social Security Number Individual File Number Military History/ Service Connection	TCP/IP Printing Protocol
Debt Management Center	Batch file for printing purposes only	Name Address Social Security Number Individual File Number Military History/ Service Connection	TCP/IP Printing Protocol

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: There is a risk that the data could be shared with an inappropriate VA organization or institution which could result in a breach of privacy and disclosure of PII to unintended parties or recipients.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

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.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

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

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*

NPC Inc. Server	Contracted Print Vendor that prints documents for PPO	Name Address Social Security Number Individual File Number Military History/ Service Connection	ISA/MOU	Business Partner Extranet
Corporate Communications Group Server	Contracted Print Vendor that prints documents for PPO	Name Address Social Security Number Individual File Number Military History/ Service Connection	ISA/MOU	Business Partner Extranet

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.

*If no External Sharing listed on the table above, (**State there is no external sharing in both the risk and mitigation fields**).*

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: Possibility of mishandled printed material containing VA sensitive information.

Mitigation: Annual Site audits are conducted. ISA/MOUs are in place. Contractors Security Control Assessments are conducted. Contractors are required to complete annual VA Privacy and Awareness Training.

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 6.1 on the last page of the document. Also provide notice given to individuals by the source system (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?

These questions are 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.

6.1a 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, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

The following SORN's provide notice:

24VA10A7/85 FR 62406 Patient Medical Records-VA
27VA047/ 77 FR 39346 Personnel and Accounting Integrated Data System-VA
41VA41/87 FR 10283 Veterans and Dependents National Cemetery Gravesite Reservation Records-VA
58VA21/22/28 86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA
88VA244/ 83 FR 40140 Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO)
168VA005/ 86 FR 6975 Health Information Exchange-VA

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Please provide response here
This system does not collect information from individuals. Notice before the collection of information is provided by various source systems. The following SORN's provide notice:

24VA10A7/85 FR 62406 Patient Medical Records-VA
27VA047/ 77 FR 39346 Personnel and Accounting Integrated Data System-VA
41VA41/87 FR 10283 Veterans and Dependents National Cemetery Gravesite Reservation Records-VA
58VA21/22/28 86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA
88VA244/ 83 FR 40140 Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO)
168VA005/ 86 FR 6975 Health Information Exchange-VA

6.1c 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.

PPO system is designed to be an output for data. Data owners create and vet the notices utilizing their internal process prior to transmission. PPO provides the data owner an output to print and mail their completed product at a designated print location. Notice before the collection of information is provided by various source systems with the publication of System of Record Notices (SORN) in the

Federal Register and the publicly available Privacy Impact Assessment for the system. The SORN explains the purpose of the system, the categories of individuals covered by the system, and how the information that is collected will be used.

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 right to decline to provide information would be provided by the source system. Individuals communicating with the VA do have the opportunity and right to decline to provide information. However, failure to provide requested identifying information may cause the denial of services, based on the totality of circumstances for each situation. Individuals may communicate with the VA anonymously, and they may decline to provide additional identifying information at their discretion. These situations may also cause the denial of service or VA's inability to provide a response to anonymous correspondence. These situations are handled on a case-by-case basis. Information about individuals who correspond with VA is collected and stored in the source systems, as described in the various SORN. Both the SORN and Privacy Impact Assessment serve as public notice of these data collection policies. The following SORN's provide this information:

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.

Yes, Individuals have a right to consent to particular uses of their information. Individuals voluntarily provide information when submitting correspondence or other documents to the Department. PPO does not collection information from individuals. The information is collected in various source systems and the processes related to consent is explained in the applicable source system SORN:

24VA10A7/85 FR 62406 Patient Medical Records-VA
27VA047/ 77 FR 39346 Personnel and Accounting Integrated Data System-VA
41VA41/87 FR 10283 Veterans and Dependents National Cemetery Gravesite Reservation Records-VA
58VA21/22/28 86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA
88VA244/ 83 FR 40140 Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO)
168VA005/ 86 FR 6975 Health Information Exchange-VA

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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: There is a risk that veterans and other members of the public will not know that the data exists or that it collects, maintains, and/or disseminates PII, about them.

Mitigation: The author of the letter (data owner) ensures the risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans are enrolled for health care.

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?
These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

The Production Print Operation system does not collect information directly from individuals. Procedures that allow access to information are handled by the source systems that initially collect the information. Access procedures are listed in the applicable SORN.

7.1a 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.***

Procedures that allow access to information are handled by the systems that initially collect the information. Access procedures are found in the appliable SORN.

7.1b 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)?

The Production Print Operations system is exempt from these provisions as it does not collect or write any information about individuals; the system only transfers a printable file with information taken from various source systems.

7.1c 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?

PPO provides the data owner an output to print and mail their completed product at a designated print location. Request for access is done by the data owner via their internal system and processes

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.

Individuals seeking to contest or amend records in this system should contact the source system manager in writing as indicated in the applicable SORN. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

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 SORN and the PIA are ways that individuals are notified. Individuals seeking to contest or amend records in the source system should contact the system manager in writing as indicated in the applicable SORN. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

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. **Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The Production Print Operation system does not offer a formal redress process. The Formal redress procedure is provided within the various source system and information on this process is found in the applicable SORN.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

*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.** (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
<u>Principle of Individual Participation:</u> Is the individual provided with the ability to find out whether a project maintains a record relating to him?

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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 Production Print Operations system does not directly collect any information from individuals and thus does not have any provision for providing access, redress, and correction.

Although this system does not collect information from individuals, there is still a privacy risk associated to individuals not having access, redress, and correction.

Mitigation: Access, redress, and correction activities take place through the systems that originally collect the information that is shared with the Production Print Operations system. The applicable source system SORN and this PIA provides the public with information on the relevant procedures.

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?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

Request for Access to PPO is done be contacting OIT DSO IO Print Production Control (AITC) (OISIPPC@va.gov). The Print Production Control office approves/denies all access requests.

8.1b 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?

No users from other agencies have access to the PPO system.

8.1c 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.

Roles are as follows: Guest - Limited access to only view files specific to their originating system; Administrator – Reserved for PPO owner group to manage all functionality within the system.

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, Business Associate Agreement (BAA), 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.

An ISA/MOU is in place between Production Print Operations and the print vendors. The contractors do not have access to the system. The contractors only have access to the print file output of the data that is sent by PPO staff.

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 individuals accessing the PPO system must complete a VA Privacy Awareness Training and Rules of Behavior.

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

No

8.4a If Yes, provide:

1. *The Security Plan Status:* <<ADD ANSWER HERE>>
2. *The System Security Plan Status Date:* <<ADD ANSWER HERE>>
3. *The Authorization Status:* <<ADD ANSWER HERE>>
4. *The Authorization Date:* <<ADD ANSWER HERE>>
5. *The Authorization Termination Date:* <<ADD ANSWER HERE>>
6. *The Risk Review Completion Date:* <<ADD ANSWER HERE>>
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

*8.4b If No or In Process, provide your **Initial Operating Capability (IOC) date.***

Submittal for initial Authority to Operate is targeted for the end of September 2024.

Submittal for initial Authority to Operate is targeted for the end of April 2023. ## Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?
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. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.
Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1. (Refer to question 3.3.1 of the PTA)

No cloud technology is being utilized.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

PPO does not have a contract with Cloud Service
9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?
Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in

the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.
This question is related to privacy control DI-1, Data Quality.

PPO does not utilize cloud technology.

9.4 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 are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

PPO does not have a Cloud provider.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.
Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

PPO does not use Robotics Process Automation (RPA).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

_____

Privacy Officer, Gina Siefert

_____

Information System Security Officer, Eric Abraham

_____

Information System Owner, Pete Sevilla

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; screen shot of a website collection privacy notice).

24VA10A7/85 FR 62406 Patient Medical Records-VA https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

27VA047/ 77 FR 39346 Personnel and Accounting Integrated Data System-VA
https://www.govinfo.gov/content/pkg/FR-2012-07-02/pdf/2012-16167.pdf

41VA41/87 FR 10283 Veterans and Dependents National Cemetery Gravesite Reservation Records-VA
https://www.govinfo.gov/content/pkg/FR-2022-02-23/pdf/2022-03795.pdf

58VA21/22/28 86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

88VA244/ 83 FR 40140 Centralized Accounts Receivable System/Centralized Accounts Receivable OnLine System (CAR/CAROLS, combined system referred to as CAO)
https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf

168VA005/ 86 FR 6975 Health Information Exchange–VA
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices