Privacy Impact Assessment for the VA IT System called:

Department of Veterans Affairs (VA)
Section 504 Automated System Tracking Remediation Authentication

(VA 504 ASTRA)

Office of Resolution Management, Diversity and Inclusion (ORMDI)

Date PIA submitted for review:

<< 4/13/2021 >>

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.Grewal@va.gov	202-632-7861
Information System Security Officer (ISSO)	Mark McGee	James.McGee5@va.gov	520-260-9194
Information System Owner	Roberto Rojo	Roberto.Rojo@va.gov	202-302-5013

Abstract

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

The Department of Veterans Affairs (VA) Section 504 Automated System Tracking Remediation Authentication (VA 504 ASTRA) will be implemented to ensure VA's required compliance per legal mandate stipulated by Section 504 of the Rehabilitation Act of 1973, as codified at 29 U.S.C. § 794, henceforth referenced as (Section 504). The system provides four alternate formats: Braille, Large Print, Audio Compact Discs (CDs), and Digital CDs, which conform to Section 504 compliance.

The Department of Commerce, National Technical Information Service (NTIS) provides a variety of dissemination services for other agencies with the specialized resources, systems, equipment, financial infrastructure, and personnel expertise needed to produce and disseminate their information products on a large scale. The VA 504 ASTRA is implemented and operated by NTIS and its Joint Venture Partners (JVPs), VASTEC and Braille Works. In the context of VA 504 ASTRA, this partnership is referred to as the VA NTIS Partnership Team.

The VA 504 ASTRA System receives notices, attachments, addressee information, and ancillary data from the VA through a secure persistent state VPN connection. Files are uploaded to a Secure File Transfer Server through the use of Secure File Transfer Protocol (SFTP). Notice tasking is forwarded to the VASTEC Production Facility for Section 504 remediation and returned to NTIS, via SFTP. Subsequently, notices designated for CD media are burned and mailed from the NTIS Production Facility. Remediated notices designated for Braille are forwarded to Braille Works via SFTP; remediated for Braille and mailed from the Braille Works Production Facility. The status of the workflow is tracked by an online system, which is updated by production facilities and available to VA online. Personally Identifiable Information (PII) will be periodically purged from the system.

The VA 504 ASTRA System is a Moderate Impact System and its minimum-security requirements will be based on the Moderate baseline defined in NIST SP 800-53 revision 4 Recommended Security Controls for Federal Information Systems. VA and NTIS have agreed upon the following legal authority to collect PII within the system; 38 U.S.C. 7105(d)(3).

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 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?*

The VA 504 ASTRA System will be implemented to ensure VA's required compliance per legal mandate stipulated by Section 504 of the Rehabilitation Act of 1973, as codified at 29 U.S.C. § 794. The system provides four alternate formats: Braille, Large Print, Audio Compact Discs (CDs), and Digital CDs, which conform to Section 504 compliance.

The NTIS provides a variety of dissemination services for other agencies with the specialized resources, systems, equipment, financial infrastructure, and personnel expertise needed to produce and disseminate their information products on a large scale. The VA 504 ASTRA is implemented and operated by NTIS and its Joint Venture Partners (JVPs), VASTEC and Braille Works. In the context of VA 504 ASTRA, this partnership is referred to as the VA NTIS Partnership Team.

The VA 504 ASTRA System receives notices, attachments, addressee information, and ancillary data from the VA through a secure persistent state VPN connection. Files are uploaded to a Secure File Transfer Server through the use of Secure File Transfer Protocol (SFTP). Notice tasking is forwarded to the VASTEC Production Facility for Section 504 remediation and returned to NTIS, via SFTP. Subsequently, notices designated for CD media are burned and mailed from the NTIS Production Facility. Remediated notices designated for Braille are forwarded to Braille Works via SFTP; remediated for Braille and mailed from the Braille Works Production Facility. The status of the workflow is tracked by an online system, which is updated by production facilities and available to VA online. Personally Identifiable Information (PII) will be periodically purged from the system.

The VA 504 ASTRA System is a Moderate Impact System and its minimum-security requirements will be based on the Moderate baseline defined in NIST SP 800-53 revision 4 Recommended

Security Controls for Federal Information Systems. VA and NTIS have agreed upon the following legal authority to collect PII within the system; 38 U.S.C. 7105(d)(3).

Please take note of the following additional information, which is being provided. The VA's Total Visually Impaired Veterans (417,166) with VA Medical Visual Diagnostic Codes. The completion of this PIA will not result in circumstances that require changes to business processes and will not result in technology changes. The NTIS System does not use cloud technology and thus a Cloud Service Provider (CSP) is not applicable. Accordingly, a CSP and VA customers will not be affected by security vulnerabilities of cloud technology due to its non-applicability to the NTIS System. Per the aforementioned non-applicability to cloud technology the magnitude of harm to VA is minimal.

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.

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)

PII Mapping of Components

<VA 504 ASTRA > consists of 22 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by <VA 504 ASTRA > and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Components of the information system (servers) collecting/storing PII	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
File Transfer Server (Redhat Linux 7)	No	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	The "VA Network" is a completely segmented network. The network is monitored by various Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
VA File Tracking Systems – Application Server (Windows 2006)	Yes	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive	The "VA Network" is a completely segmented network. The network is monitored by various

				letter notifications, which are Section 504 Compliant.	IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
VA Reporting Server (Windows 2016)	Yes	No	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	The "VA Network" is a completely segmented network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
VA Tracking System DB Server (Windows 2006) (MS SQL Server 2017)	Yes	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	The "VA Network" is a completely segmented network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the

					capturing of PII data.
OCR/Manufacturing Server (Redhat Linux 6)	No	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	The "VA Network" is a completely segmented network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
Optical Character Recognition (OCR)/ Manufacturing Server (Ubuntu 18.04)	No	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	The "VA Network" is a completely segmented network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
SQL Server [Open Database Connectivity (ODBC)] to Shipping Stations) (Windows 2016) (MS SQL Server 2017)	Yes	Yes	Name, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being	The "VA Network" is a completely segmented network. The network is monitored by

				able to receive letter notifications, which are Section 504 Compliant.	various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
2 x Duplicator Workstations (Windows 10)	Yes	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	The "VA Network" is a completely segmented network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
2 x EPSON Duplicator Printers	Yes	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	The "VA Network" is a completely segmented network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to

					avoid the capturing of PII data.
File Transfer server (Redhat Linux 7)	No	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 compliant.	The "VA Network" is a completely segmented network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
VA File tracking Systems - Application Server (Windows 2016)	Yes	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	The "VA Network" is a completely segmented network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
VA Reporting Server (Windows 2016)	Yes	No	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired	The "VA Network" is a completely segmented network. The network is

				Veterans being able to receive letter notifications, which are Section 504 Compliant.	monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
VA Tracking System DB Server (Windows 2016) (MS SQL Server 2017)	Yes	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	The "VA Network" is a completely segmented network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
OCR/Manufacturing Server (Ubuntu 18.04)	No	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	The "VA Network" is a completely segmented network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA

					Workspace to avoid the capturing of PII data.
2 X Domain Controllers (Windows 2016)	No	No	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	The "VA Network" is a completely segmented network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
9 x Quality Control Workstations (Windows 10)	Yes	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	The "VA Network" is a completely segmented network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
SQL Server (ODBC to Shipping Stations) (Windows 2016) (MS SQL Server 2017)	Yes	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-	The "VA Network" is a completely segmented network. The

				Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
2 x Shipping Stations (Shawnee) (Windows 10)	Yes	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	The "VA Network" is a completely segmented network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
2 x Shipping Stations (Florida) (Windows 10)	Yes	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	The "VA Network" is a completely segmented network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the

					dedicated VA Workspace to avoid the capturing of PII data.
2 x Duplicator Workstations (Windows 10)	Yes	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	The "VA Network" is a completely segmented network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
6 x EPSON Duplicator Printers	Yes	Yes	Name, DOB, SSN, Mailing Address	NTIS is operating a system on the behalf of the VA regarding Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	The "VA Network" is a completely segmented network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.
VA Printer	No	Yes	Name, DOB, SSN, Mailing	NTIS is operating a system on the behalf of the VA regarding	The "VA Network" is a completely segmented

			Address	Visually-Impaired Veterans being able to receive letter notifications, which are Section 504 Compliant.	network. The network is monitored by various IDS/IPS tools. All mobile devices are stored and are not permitted within the dedicated VA Workspace to avoid the capturing of PII data.

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 VA 504 ASTRA System receives notices, attachments, addressee information, and ancillary data from the VA through a secure persistent state VPN connection. Files are uploaded to a Secure File Transfer Server through the use of Secure File Transfer Protocol (SFTP). Please additionally note, per VA compliance with Section 504 of the Rehabilitation Act of 1973, VA Notifications will be remediated to the preferred Section 504 Alternate Format selected by Blind or Visually Impaired Veterans.

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 PII is not collected from individuals but is supplied by VA to NTIS via the VA 504 ASTRA System to satisfy the VA mission to serve Veterans. Please note, PII (Complete Name, Social Security Number, and Date of Birth) plus their Personal Mailing Address is needed by the VA for Blind or Visually Impaired Veterans to be able to provide their Identity Verification to the VA in order to receive Section 504 Compliant Notifications in their preferred Alternate Formats.

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 VA 504 ASTRA System will be implemented to ensure VA's required compliance per legal mandate stipulated by Section 504 of the Rehabilitation Act of 1973, as codified at 29 U.S.C. § 794. The system provides four alternate formats: Braille, Large Print, Audio Compact Discs (CDs), and Digital CDs, which conform to Section 504 compliance.

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.

The NTIS has employed an automated script to perform the checksum processes, which are performed as files are uploaded to the SFTP server, on information received at all levels through the VA 504 ASTRA Information System Processes. The checksum processes validate consistency between information received from the VA and the information processed by the NTIS. Failed checksum processes are identified and provided to the source of the received file and will be remedied by the VA NTIS Partnership Team.

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

NTIS' legal authority for the collection of information provided by VA is a Memorandum of Understanding and Interconnection Security Agreement between NTIS and VA. The VA's legal authority for the collection of information that it provides to NTIS is the Federal Statute, 38 U.S.C. 7105(d)(3).

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.

Privacy Risk:

Risks Identified -

- Identifiability:
  The system specifically identified individuals using their name, dates of birth, social security number, and home address.
- Quantity of PII:
  The system uses PII for all United States citizens that request VA documents in alternate formats. As of (date), there are over (number of documents) documents for the VA 504 ASTRA System.

- Data Field Sensitivity: The system includes sensitive personal information that could be used for identity theft. This includes full name, Social Security Number, date of birth, and home address.
- Obligation to Protect Confidentiality:
  Must be protected per the Privacy Act.
- Access to and Location of PII:
  Protected in a secure access area and on an encrypted server. The system is accessible only on the internal NTIS network. Only authorized individuals have access to PII.

Mitigation:

As required by FIPS 199, the System and its components were reviewed for the sensitivity of the information in them and were determined to require protection appropriate for Moderate Impact systems. All relevant policies, procedures and guidelines, including NIST Special Publication 800-53, have been followed to ensure the security of the systems and the information in them. The NTIS VA 504 ASTRA System Security Plan (SSP) on file with NTIS' Chief Information Security Officer (CISO) contains additional details.

Operational Controls: At the NTIS Shawnee Facility located in Alexandria, Virginia, the NTIS VA 504 ASTRA System servers are maintained in a secure Data Center where access is limited to only those support personnel with a demonstrated access need. The NTIS VA 504 ASTRA System Servers require a network logon and a server log-on process. All entrance doors are identified and marked. A log is kept of all staff and contractors who are issued a security card, key and/or combination that grant access to the Data Center and the building. All NTIS visitors are escorted while in the Data Center and the building. Separate access control lists are maintained for the Data Center and the building. Where appropriate environmental security controls are implemented, which include measures implemented to mitigate damage to automated information system resources caused by fire, electricity, water and inadequate climate controls. Authorized individuals must use a security key card for elevator and floor access to where the Data Center is located. A Personal Identity Verification (PIV) Common Access Card (CAC) and PIN Code combination is
required to gain entry to the Data Center.

Threats to privacy for VA 504 ASTRA System are minimized by controls deployed to protect information at rest and in transit. The VA 504 ASTRA system utilizes the latest cryptographic technologies and methods such as Transit Layer Security (TLS) 1.2 (HTTPS) for data in transit, and Advance Encryption Standard (AES)-256 encryption for data at rest.

Network controls ensure the stability and integrity of NTIS' network and provide the maximum availability and security for hosted Websites in the production environment. The VA 504 ASTRA System components are located on dedicated domains and VLANs to limit and restrict external communication.

NTIS proactively monitors all activity on its network through human vigilance and automated tools. NTIS makes necessary modifications to the network based on security notifications from government and nongovernment security watchdog agencies on a routine basis. These updates

include countermeasures against the latest product security holes, hacker attacks, and hacker tools and/or strategies for compromising Internet sites.

Technical controls: All Business Identifiable Information (BII) and PII data are secured through the use of user identification and authentication (e.g., user id, password), and other access controls, as detailed in the NTIS-VA 504 ASTRA System Security Plan.

Authorized users include system administrators, workflow managers, 504 and Braille remediators, operators of printers, embossers, CD burners, and labelers, QA checkers, and mail clerks. All users sign a nondisclosure agreement.

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 PII is not collected from individuals but is supplied by VA to NTIS via the VA 504 ASTRA System to satisfy the VA mission to serve Veterans. Please note, PII (Complete Name, Social Security Number, and Date of Birth) plus their Personal Mailing Address is needed by the VA for Blind or Visually Impaired Veterans to be able to provide their Identity Verification to the VA in order to receive Section 504 Compliant Notifications in their preferred Alternate Formats.

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 VA 504 ASTRA System receives notices, attachments, addressee information, and ancillary data from VA through a secure persistent state VPN connection. Files are uploaded to a Secure File Transfer Server through the use of Secure File Transfer Protocol (SFTP). Notice tasking is forwarded to a JVP production facility for Section 504 remediation and returned to NTIS, via SFTP. Subsequently, notices designated for CD media are burned and mailed from the NTIS production facility. Remediated notices designated for Braille are forwarded to a JVP via SFTP; remediated for Braille, embossed, and mailed from the JVP production facility. Status of workflow is tracked by an online system which is updated by production facilities and available to VA online. PII is periodically purged from the system. The system also produces audio CDs and large print notices as well.

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.

All BII and PII data are secured through the use of user identification and authentication (e.g., user id, password), and other access controls, as detailed in the NTIS-VA 504 ASTRA System Security Plan. Authorized users include system administrators, workflow managers, Section 504 and Braille remediators, operators of printers, embossers, CD burners, and labelers, QA checkers, and mail clerks. All users sign a nondisclosure agreement.

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 PII is not collected from individuals but is supplied by VA to NTIS via the VA 504 ASTRA System to satisfy the VA mission to serve Veterans. Please note, PII (Complete Name, Social Security Number, and Date of Birth) plus their Personal Mailing Address is needed by the VA for Blind or Visually Impaired Veterans to be able to provide their Identity Verification to the VA in order to receive Section 504 Compliant Notifications in their preferred Alternate Formats.

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.

Records will be created, maintained and disposed of in accordance with Department of Veterans Affairs, Records Control Schedule (RCS) 005-1 (August 3, 2009). Please refer to (RCS 005-1) located within (http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf). Additionally, under the Office of Management and Budget (OMB) and National Archives and Records Administration (NARA) Guidelines, the Records Management Resources within the General Records Schedule will be referenced. These specific resources can be located within (http://www.archives.gov/records-mgmt/grs). When managing and maintaining VA data and records, the guidelines established in the Department of Veterans Affairs, (RCS 10-1) will be followed, located within (http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf).

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.

Managing and maintaining VA data and records, will follow guidelines established in NARA-Approved Department of Veterans Affairs, Office of Information and Technology, RCS 005-1, located within (https://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf) and VA RCS-10-1, located within (http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf).

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

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans Affairs Directive 6371, (April 8, 2014), https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans Affairs Directive 6500, (February 24, 2021), "Media sanitization on all electronic storage media must comply with NIST SP 800-88."

https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=1254&FType=2

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

The VA 504 ASTRA System will not use PII for testing, training, or research purposes. The system has been developed through NTIS's proven process and SDLC.

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.

Privacy Risk:

There is a risk that the information contained in the VA 504 ASTRA Information System will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached**.**

Mitigation:

In addition to collecting and retaining only the information necessary for fulfilling the VA mission, the disposition of data housed is based on standards developed by the National Archives and Records Administration (NARA). This ensures that data is held for only as long as necessary. Per managing and maintaining VA data and records, VA 504 ASTRA will follow guidelines established in NARA, VA RCS 005-1, VA RCS-10-1, and VA Directive 6500, (February 24, 2021), "Media sanitization on all electronic storage media must comply with NIST SP 800-88."

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

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
N/A	N/A	N/A	N/A

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.

Privacy Risk:
There is no risk to privacy originating from internal sharing and disclosure, because there is no internal sharing or disclosure of information.

Mitigation:
N/A

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: 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

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 data element types such as PII/PHI that are shared/received 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***
NTIS Data Center	Provide Blind or Visually Impaired Veterans Section 504 Compliant Notifications in their preferred Alternate Formats.	Please note, the specific data element types: Complete Name, Date of Birth, Social Security Number, Mailing Address, Telephone Number, E-Mail Address, Veterans Health Information.	MOU/ISA	Site to Site (S2S), IPSEC Tunnel, Secure FTP
NTIS Joint Venture Partners	Provide Blind or Visually Impaired Veterans Section 504 Compliant Notifications in their preferred Alternate Formats.	PII is produced by the NTIS Joint Venture in the process of creating products in alternate formats, (Braille, Large Print, Audio Compact Discs (CDs), and Audio CDs.	MOU/ISA	Site to Site (S2S), IPSEC Tunnel, Secure FTP

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

Please note, VA 504 ASTRA - System Security Plan was signed on 2/17/2021 and uploaded to eMASS.

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

Privacy Risk:

NTIS shares this information with Joint Venture Partners (VASTEC and BrailleWorks) for remediation of optical character recognition, braille conversions and printing, as well as large format printing. While this might be a risk, the NTIS System Security Plan, inclusively provides security coverage for the NTIS JVPs (VASTEC and BrailleWorks).

Mitigation:

NTIS MOU established with JVPs to ensure that all contractors working on VA 504 ASTRA information processing and Section 504 Compliance must adhere to background investigations and non-disclosure agreements, as well as facilities prohibiting the admittance of any electronic devices, to include cell phones, cameras, USB drives, etc. in areas where information processing and Section 504 Compliance is performed.

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.

The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to Veterans applying for VA Benefits. NOPPs are provided to Veterans when they enroll or make updates. Employees and contractors are required by VA Directive 6500 (February 24, 2021) to complete mandatory annual Information Security and Privacy Awareness Training plus review, sign, and abide by the VA National Rules of Behavior.

Additionally, VA's Privacy Act statement and/or VA's Privacy Policy can be located within: https://www.va.gov/privacy-policy/

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

There is no penalty or denial of service attached, however PII is needed for Blind or Visually Impaired Veterans to provide their Identity Verification to the VA in order to receive Section 504 Compliant Notifications in their preferred Alternate Formats.

The PII is not collected from individuals but is provided by VA to NTIS via the VA 504 ASTRA System to satisfy the VA's Mission to Serve Veterans.

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 PII pertains to Veterans, whom have requested from the VA to be provided notices with their preferred Section 504 Alternate Format.

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.

Privacy Risk:

There is a risk that an individual may not understand what their information is being collected or maintained about them.

Mitigation:

This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans apply for benefits. VA new NOPPs are mailed to beneficiaries when there is a change in regulation. Employees and contractors are required by VA Directive 6500 (February 24, 2021) to complete annual mandatory Information Security and Privacy Awareness Training plus review, sign, and abide by VA National Rules of Behavior also on an annual basis.

This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans apply for benefits. VA new NOPPs are mailed to beneficiaries when there is a change in regulation. Employees and contractors are required by VA Directive 6500 (February 24, 2021) to complete mandatory annual Information Security and Privacy Awareness Training plus also on an annual basis review, sign, and abide by VA National Rules of Behavior.

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.

Veterans may access information about themselves from the following ways. The Department of Veterans Affairs (VA), Veterans Health Administration (VHA) created the MyHealtheVet program to allow online access to their health records. More information on this program and how Veterans sign up to participate is located within (https://www.myhealth.va.gov/index.html). Veterans may also request copies of their medical records and other records containing personal data from the VA Medical Facility's Release of Information (ROI) Office.

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 procedure for correcting inaccurate or erroneous information begins with the Veteran requesting their records in question from Release of Information (ROI). The Veteran then crosses out information they feel is inaccurate or erroneous from their records and writing in what the Veteran believes to be accurate. The request for amendment and correction is sent to the Facility Privacy Office for processing. The documents are then forwarded to the practitioner who entered the data by the Facility Privacy Officer. The practitioner either grants or denies the request. The Veteran will be provided a correspondence notification of the decision by means of a letter, which will be sent by the Facility Privacy Officer.

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.

Veterans are informed of the amendment process by the Notice of Privacy Practice (NOPP) which states:

Right to Request Amendment of Health Information

You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the Facility Privacy Officer at the VHA Health Care Facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights.

In response, you may do any of the following:

- File an Appeal;
- File a "Statement of Disagreement";
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information.

Information can also be obtained by contacting the Facility ROI Office.

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 ensures data accuracy.

Veterans should use the formal redress procedures, which are provided within Section (7.3).

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.

Privacy Risk:

There is a risk that Veterans do not know how to obtain access to their records or how to request corrections to their records and that their records could contain inaccurate information that may subsequently effect the care the Veterans receive.

Mitigation:

As stated in Section (7.3), the Notice of Privacy Practice (NOPP), which every patient receives when enrolled, the correction process for requesting an amendment to their records is provided. The Facility Release of Information (ROI) offices assist Veterans with obtaining access to

their health records and other records containing personal information. VHA established MyHealtheVet program to provide Veterans remote access to their health records. The Veteran must enroll to obtain access to all the available features. In addition, VHA Directive 1605.1, Privacy and Release of Information, establishes VHA procedures for Veterans to have their records amended where appropriate.

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.

All access authorization and group/role membership is explicitly determined through the use of User Access Request Form (UARF) or email communication, that must be approved by and/or received from Office of the Chief Information Officer (OCIO) Managers. New users must undergo a full background investigation prior to being granted access to any VA 504 ASTRA System components. NTIS has clearly defined, identified, and selected account types to support the business functions of the VA 504 ASTRA Information System (IS): Quality Control (QC) and Shipping Station User, QC and Shipping Station Administrator, User, and Administrator. AD managed accounts or local accounts on system components are monitored, reviewed, and managed in accordance with NTIS Access Control Policy & Procedure (ACP&P) to ensure acceptable creation, modification, removal, and usage of all account types.

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.

Yes, One VA Contractor signed VA Form 0752, "Confidentiality of Sensitive Information Non-Disclosure Agreement" access the VA 504 ASTRA System and to its corresponding PII.

Please additionally note, NTIS will design the system as well as provide system maintenance. Solely, VA 504 ASTRA's designated Information System Steward (ISS), whom is a Booz Allen Hamilton Contractor, will have system access to provide - VA's Office of Information Technology (OIT) Development, Security, and Operations (DevSecOps) Support. Per the (roles/responsibilities) provisions contained within the VA Form 0752, Confidentiality of Sensitive Information Non-Disclosure Agreement was signed by the VA 504 ASTRA IIS on 12/15/2020. The VA 504 ASTRA Information System Owner will review this signed documentation on an annual basis. The Signed VA Form 0752 is required to grant system access, which has only been securely granted to the VA 504 ASTRA ISS.

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.

NTIS combats the potential for Insider Threat through on-going training exercises, such as Phishing Initiatives, Departmental Annual Security and Privacy Awareness Training, and on-going newsletters and email alerts sent to NTIS Staff. Accounts are reviewed on a quarterly basis to ensure stale accounts and accounts that are no longer needed are removed and inaccessible.

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,
   December 7, 2020;
2. Whether it was a full ATO or ATO with Conditions,
   ATO with Conditions;
3. The amount of time the ATO was granted for, and on December 3, 2020, 180-Day ATO was granted. However, upon being uploaded to eMASS on December 7, 2020, the time scope completion for 180 Days was entered as May 5, 2020. Correctly, the full-time scope for 180 Days calculates up to June 5, 2021.
4. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).
   Moderate

Section 9. References

ID	Summary of Privacy Controls by Family
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 Privacy Officer

The Privacy Officer 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: 2021.05.04 19:56:20 -04'00'

Privacy Officer

Signature of Information Security System Officer

The Information Security System Officer below attest that the information provided in this Privacy Impact Assessment is true and accurate.

James M. McGee 926698

Digitally signed by James M. McGee 926698
Date: 2021.05.05 06:26:32 -07'00'

Information Security System Officer

Signature of Information System Owner

The Information System Owner below attests that the information provided in this Privacy Impact Assessment is true and accurate.

Robert Rojo 100916 Digitally signed by Robert Rojo 100916
Date: 2021.05.05 09:44:23 -04'00'

Information System Owner

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).

Inclusively, VA's Privacy Act statement and/or VA's Privacy Policy can be located within: https://www.va.gov/privacy-policy/