Privacy Impact Assessment for the VA IT System called:

VA POLICE RECORDS MANAGEMENT SYSTEM CLOUD

Office of the Secretary of Veterans Affairs; Office of Operations, Security, and Preparedness

Date PIA submitted for review:

11/17/2020

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita K.Grewal	Rita.Grewal@va.gov	202-632-7861

	Name	E-mail	Phone Number
Information System Security Officer (ISSO)	Edgardo Rivera	Edgardo.Rivera1@va.gov	787-692-4583
Information System Owner	Christopher Oakleaf	Christopher.Oakleaf@va.gov	512-326- 6690

Abstract

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

Veterans Administration Police Records Management System (VAPOLICERMS) is owned by the Office of Security and Law training branch, the Law Enforcement Training Center. Veterans Administration Police Records Management System (VAPOLICERMS) is used by the VA Police Services and Office of Security and Law Enforcement at VA facilities nationwide for tracking activities, incidents and offenses occurring on VA property.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*

- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.*
- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?*
- *What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

Veterans Administration Police Records Management System (VAPOLICERMS) is owned by the Office of Security and Law training branch, the Law Enforcement Training Center. Veterans Administration Police Records Management System (VAPOLICERMS) is used by the VA Police Services and Office of Security and Law Enforcement at VA facilities nationwide for tracking activities, incidents and offenses occurring on VA property. The system stores PII that covers veterans, federal government employees, VA police officers, retirees, volunteers, contractors, subcontractors, and other individuals, including private citizens, involved in activities within the assigned responsibilities of Police and Security Service at VA field facilities.

The 223783 records in the system contain information retrieved by quick name check, offense reports, violations, motor vehicle registrations, wants and warrants, police daily operations journal, police officer training records, photographs, uniform offense reports, accident reports, information on identification cards, records of evidence and property, and records of citations. The records and information contained in this system is necessary for the effective administration and management of the Department's nationwide Police and Security program.

VA Police Records Management System (VAPOLICERMS) is a commercial off the shelf application. VAPOLICERMSS is a client-server application that is resident on a Windows 2012 R2 server running Internet Information Server (IIS) with secure Independent Computing Architecture (ICA) used for encryption. Access to VAPOLICERMSS data is highly restrictive and controlled at two network points (Active Directory Server and database). VA Police Officers and authorized personnel are initially authenticated at the Austin Information Technology Center (AITC) by the active directory domain server. VAPOLICERMS users are then further authenticated by the database internal access security.

VAPOLICERMS does not connect with other systems/entities internally or externally. The information sharing described in table 4.1 and 5.1 is only physical reports (paper).

The authority to maintain these records is Title 38, United States Code (U.S.C.), Section 501 and 901–905. The records and information contained in this system of records are necessary for the effective administration and management of the Department's nationwide Security and Law Enforcement program.

This requires the collection and use of accurate, up-to-date data for enforcing the law and protecting persons and property on VA property and at VA Central Office in accordance with Title 38, U.S.C., Chapter 9. The System of Records Notice associated with this system is ''Police and Security Records—VA'' (103VA07B).

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)

For identification purposes a record may include a VA Medical ID or Passport Number.

PII Mapping of Components

VA Police RMS Cloud consists of 6 key components (servers). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VA Police RMS Cloud and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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
Vac20sqlprs200	Yes	Yes	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Vehicle License Plate Number, Current medications, Race/Ethnicity, VA Medical ID, Passport Number.	Police Reports	**Server-side encryption of data at rest, TLS encryption of data in transit, error checking and validation routines, backups**
Vac20sqlprs400	Yes	Yes	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Vehicle License Plate Number, Current medications, Race/Ethnicity, VA Medical ID,	Police Reports	**Server-side encryption of data at rest, TLS encryption of data in transit, error checking and validation routines, backups**

			Passport Number.		
Vac20webprs200	Yes	Yes	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Vehicle License Plate Number, Current medications, Race/Ethnicity, VA Medical ID, Passport Number.	Police Reports	**Server-side encryption of data at rest, TLS encryption of data in transit, error checking and validation routines, backups**
Vac20webprs201	Yes	Yes	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Vehicle License Plate Number, Current medications, Race/Ethnicity, VA Medical ID, Passport Number.	Police Reports	**Server-side encryption of data at rest, TLS encryption of data in transit, error checking and validation routines, backups**
Vac20webprs400	Yes	Yes	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number(s), Personal Email Address,	Police Reports	**Server-side encryption of data at rest, TLS encryption of data in transit, error checking**

			Vehicle License Plate Number, Current medications, Race/Ethnicity, VA Medical ID, Passport Number.		**and validation routines, backups**
Vac20webprs401	Yes	Yes	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Vehicle License Plate Number, Current medications, Race/Ethnicity, VA Medical ID, Passport Number.	Police Reports	**Server-side encryption of data at rest, TLS encryption of data in transit, error checking and validation routines, backups**

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

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

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

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The information is collected directly from individuals. The collection and use of accurate information, requires up-to-date data for enforcing the law and protecting persons and property on VA grounds.

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 officer will collect the initial incident information on paper; this is not subject to the Paperwork Reduction Act..

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 purpose of the VAPOLICERMS, including collection of the information, is to give the Office of Security and Law Enforcement the information needed to track activities and offenses occurring at VA facilities. The records and information contained in are necessary for the effective administration and management of the Department's nationwide Police and Security program. VAPOLICERMS uses an Incident Report. This report contains information of all types of offenses and incidents, criminal and non-criminal, that occur at a facility and to which VA police respond (i.e., criminal investigations, investigative stops, patient and staff assistance calls, missing patient searches, and motor vehicle accidents).

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.

Information is collected directly from the individual; The officer refers to his written case notes to verify accuracy.

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

The authority to maintain these records is Title 38, United States Code (U.S.C.), Section 501 and 901–905. The records and information contained in this system of records are necessary for the effective administration and management of the Department's nationwide Security and Law Enforcement program. This allows the collection and use of accurate, up-to-date data for enforcing the law and protecting persons and property on VA property and at VA Central Office in accordance with Title 38, U.S.C., Chapter 9. The System of Records Notice associated with this system is ''Police and Security Records—VA'' (103VA07B). https://www.gpo.gov/fdsys/pkg/FR-2008-12-08/pdf/E8-29029.pdf

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:
Privacy Risk: VAPOLICERMS collects Personally Identifiable Information (PII) and other highly delicate Sensitive Personal Information (SPI). If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify the potential issues and concerns, and aid the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA can better protect the individual's information. adheres to information security requirements instituted by the VA Office of Information Technology (OIT). All users with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually and must complete a background investigation before being granted access to the system. Every system user signs a national Rules of Behavior where they acknowledge they will follow VA privacy and information security rules. VA Handbook 5021 establishes and defines personnel sanctions for privacy and information security violations. Separation of duties controls limit the information available to individual users to what they need to do their job. Access to information on the system is restricted by access control lists/permissions. Actions on the system are logged in the system logs.

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.

Name/Date of Birth - Assists in uniquely identifying the person's record.
SSN - Assists in uniquely identifying the person's record.
Mailing Address - Assists in uniquely identifying the person's record.
Email Address – Assists in communication with identified person.

Certificate/License Numbers: used for identifying vehicle owners at a facility.
Photographic images - Persons and/or scenes pertinent to an incident or police investigation

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

VAPOLICERMS uses an Incident Report. This system is used by VA Police to track all types of offenses and incidents, criminal and non-criminal, that occur at a facility and to which VA police respond (i.e., criminal investigations, investigative stops, patient and staff assistance calls, missing patient searches, and motor vehicle accidents. A new record is created whenever there is a new police incident by the same individual. The information in this system is used by VA Police to track and document offenses and incidents related to criminal and non-criminal incidents. The information can be used when pursuing administrative or criminal action against an individual that committed a criminal or non-criminal offense within VA facilities.

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.

- Yes. The current SORN lists the approved routine uses for the data collected.
- All employees with access to Veteran's information are required to have the appropriate level background investigation and must complete the VA Privacy and Information Security awareness training and rules of behavior annually.

- Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.
- Individual users are given access to medical center staff, visitor's and/or veteran's data through the issuance of a user ID and password and using a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication. The user's user ID limits the access to only the information required to enable the user to complete their job.

- The minimum-security controls for the VAPOLICERMS application cover 17 security areas about protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The VAPOLICERMS application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks.

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

All information listed in Section 1.1 is retained within VAPOLICERMS.
Name/Date of Birth
SSN
Mailing Address
Email Address
Certificate/License Numbers
Photographic images

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.

VAPOLICERMS records are retained and disposed of in accordance with General Records Schedule 18, Item 22a, approved by the National Archives and Records Administration (NARA). Records are retained indefinitely until destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable. https://www.archives.gov/files/records-mgmt/grs/trs29-sch-only.pdf. The applicable SORN is 103VA07B - Police and Security Records – VA - https://www.oprm.va.gov/docs/Current_SORN_List_11_19_2020.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.

These records are retained and disposed of in accordance with General Records Schedule 5.6: Security Records , , approved by the National Archives and Records Administration (NARA). https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs-2017-0006_sf115.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

Records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable. The records are disposed of by electronic erasure or shredding by following the sanitization procedures in VA 6300 Records and Information Management and VA 6500.1 Electronic Media Sanitization. Paper records are destroyed under VA Record Office Supervision.
Paper records are shredded using an approved National Security Agency (NSA) High Security Crosscut Shredder from the NSA High Security Crosscut Shredder List.

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

Dummy (fake/made-up) data is used for testing. Pre-production environment is used for training purposes. This system is not used for research purposes.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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:

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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 the information contained in the system will be retained for longer than is necessary to fulfill the VA mission. If this occurs, the potential impact is that we could be in violation of the established records control schedule.

Mitigation: To mitigate the risk posed by information retention, the VAP ensures that records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable. The records are disposed of by electronic erasure or shredding by following the sanitization procedures in VA 6300 Records and Information Management and VA 6500.1 Electronic Media Sanitization. Paper records are destroyed under VA Record Office Supervision. Paper records are shredded using an approved National Security Agency (NSA) High Security Crosscut Shredder from the NSA High Security Crosscut Shredder List.

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***
VA/VHA Management	Senior management awareness, human resources corrective actions and as input into management responses to congressional and OIG inquiries.	Name, SSN, address, email, health address, Age, Eye Color, Gender, Hair Color, Hair Length, Race	Physical/Digital copy (VA email)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:
Privacy Risk: Although VAPOLICERMS does not share information internally, privacy information may be released to unauthorized individuals.

Mitigation:

- All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- VAPOLICERMS adheres to all information security requirements instituted by the VA Office of Information Technology (OIT).
- Information is shared in accordance with VA Handbook 6500.

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***
Local Police	Law Enforcement Investigation/Prosecution	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Vehicle License Plate Number, Current medications, Race/Ethnicity, VA Medical ID, Passport Number.	103VA07B	Physical Reports, Station Privacy Procedures
County Police	Law Enforcement Investigation/Prosecution	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Vehicle License Plate Number, Current medications, Race/Ethnicity, VA Medical ID, Passport Number.	103VA07B	Physical Reports, Station Privacy Procedures
State Police	Law Enforcement Investigation/Prosecution	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number(s), Personal Email	103VA07B	Physical Reports, Station Privacy Procedures

		Address, Vehicle License Plate Number, Current medications, Race/Ethnicity, VA Medical ID, Passport Number.		
Federal Marshalls	Law Enforcement Investigation/Prosecution	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Vehicle License Plate Number, Current medications, Race/Ethnicity, VA Medical ID, Passport Number.	103VA07B	Physical Reports, Station Privacy Procedures
Federal Attorneys	Law Enforcement Investigation/Prosecution	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Vehicle License Plate Number, Current medications, Race/Ethnicity, VA Medical ID, Passport Number.	103VA07B	Physical Reports, Station Privacy Procedures
FBI	Law Enforcement Investigation/Prosecution	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number(s),	103VA07B	Physical Reports, Station Privacy Procedures

		Personal Email Address, Vehicle License Plate Number, Current medications, Race/Ethnicity, VA Medical ID, Passport Number.		
Defendant Attorneys	Law Enforcement Investigation/Prosecution	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Vehicle License Plate Number, Current medications, Race/Ethnicity, VA Medical ID, Passport Number.	103VA07B	Physical Reports, Station Privacy Procedures
Omnigo	Software technical support	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Vehicle License Plate Number, Current medications, Race/Ethnicity, VA Medical ID, Passport Number.	103VA07B	Physical Reports,

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

To protect Veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:
1. The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.
4. Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:
Privacy Risk: Privacy information may be released to unauthorized individuals.

Mitigation:

- All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- VAPOLICERMS adheres to all information security requirements instituted by the VA Office of Information Technology (OIT)
- Information is shared in accordance with VA Handbook 6500
- All personnel accessing Veteran's information must first have a successfully adjudicated fingerprint check. This fingerprint check is conducted by the Federal Bureau of Investigation (FBI) Justice Information and criminal history records. Individual users are given access to Veteran's data through the issuance of a user ID and password and using a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication.

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 Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 3 ways:

1. The System of Record Notice (SORN) "The System of Records Notice associated with this system is ''Police and Security Records—VA'' (103VA07B). (December 8, 2008). This SORN can be found online at https://www.gpo.gov/fdsys/pkg/FR-2008-12-08/pdf/E8-29029.pdf
2. This Privacy Impact Assessment (PIA) also serves as notice of the VAP system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available.
3. Individuals are verbally notified that their information is being used to record contact and incident information at the time the data is collected.

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

Individuals must provide all required information requested by a VA Police Officer. No penalty or denial of service is attached with not providing needed information; The system stores PII that covers veterans, Federal government employees, VA police officers, retirees, volunteers, contractors, subcontractors, and other individuals, including private citizens, involved in activities within the assigned responsibilities of
Police and Security Service at VA field facilities for enforcing the law and protecting persons and property on VA property.

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

Individuals, whose information is stored within VAPOLICERMS, are not able to provide consent for specific uses of their information. Individuals must provide all required information requested by a VAPOLICERMS for enforcing the law and protecting persons and property on VA property.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:
Privacy Risk: There is a risk that veterans and other members of the public will not know that the VAPOLICERMS exists and it process or collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Act statement and a System of Record Notice.

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.

Individuals seeking information regarding access to and amendment of records in the VAPOLICERMS system may write, call or visit the VA facility where the records are maintained. Director, Police Service (07B), Department of Veterans Affairs, 810 Vermont Avenue, NW., Washington, DC 20420, telephone (202) 461–5544.

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.

Written comments may be submitted through www.Regulations.gov; by mail or hand delivery to the Director, Regulations Management (02REG), Department of Veterans Affairs, 810 Vermont Ave., NW., Room 1068, Washington, DC 20420; or by fax to (202) 273–9026. Copies of comments received will be available for public inspection in the Office of Regulation Policy and Management, Room 1063B, between the hours of 8 a.m. and 4:30 p.m. Monday through Friday (except holidays). Please call (202) 461–4902 for an appointment. In addition, during the comment period, comments may be viewed online through the Federal Docket Management System (FDMS) at www.Regulations.gov. as directed in the System of Record Notice (SORN) "The System of Records Notice associated with this system is ''Police and Security Records—VA'' (103VA07B). (December

8, 2008). This SORN can be found online at https://www.gpo.gov/fdsys/pkg/FR-2008-12-08/pdf/E8-29029.pdf

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.

Individuals are notified of the procedures to correct their information by the publishing of the PIA as well as by SORN 103VA07B – Police and Security Records (December 8, 2008). This SORN can be found online at https://www.gpo.gov/fdsys/pkg/FR-2008-12-08/pdf/E8-29029.pdf

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.

Written comments may be submitted through www.Regulations.gov; by mail or hand delivery to the Director, Regulations Management (02REG), Department of Veterans Affairs, 810 Vermont Ave., NW., Room 1068, Washington, DC 20420; or by fax to (202) 273–9026. Copies of comments received will be
available for public inspection in the Office of Regulation Policy and Management, Room 1063B, between the hours of 8 a.m. and 4:30 p.m. Monday through Friday (except holidays). Please call (202) 461–4902 for an appointment. In addition, during the comment period, comments may be viewed online
through the Federal Docket Management System (FDMS) at www.Regulations.gov. as directed in the System of Record Notice (SORN) "The System of Records Notice associated with this system is ''Police and Security Records—VA'' (103VA07B). (December 8, 2008). This SORN can be found online at https://www.gpo.gov/fdsys/pkg/FR-2008-12-08/pdf/E8-29029.pdf

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to

be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.

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

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:
Privacy Risk: There is a risk that individual may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt

Mitigation: By publishing this PIA and the applicable SORN, the VA makes the public aware of the unique status of applications and files, such as those stored on the VAP System. The System of Record Notice (SORN) "The System of Records Notice associated with this system is ''Police and Security Records—VA'' (103VA07B). (December 8, 2008). This SORN can be found online at https://www.gpo.gov/fdsys/pkg/FR-2008-12-08/pdf/E8-29029.pdf. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files contained within VAPOLICERMS.

Section 8. Technical Access and Security

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

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

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

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

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

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development. The defined user roles are 1-Administrative/Clerical, 2-Chief/Deputy Chief Master, 3-Detective/Evidence Custodian, 4-Dispatch Supervisor, 5-Dispatcher, 6-Dispatcher/Evidence Custodian, 7-Evidence Custodian/Officer, 8-Evidence Custodian/Supervisor, 9-Investigator, 10-Investigator/Supervisor, 11-No Access, 12-Office Master, 13-Officer/Dispatcher, 14-Physical Security Specialist, 15-Police Secretary/Admin, 16-RE LETC Admin, 17-Report Reader (Read-Only), 18-Supervisor Master, 19-VACO Inspector

- Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

- OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring is performed through the use of Talent Management System (TMS). All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

- Access to VAPOLICERMS is controlled through the combination of Active Directory and twenty-six assigned user roles, each with unique combinations of privileges within the system. Annual training on VA Privacy and Information Security Awareness is tracked on the VA Talent Management System (TMS).

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, there are contract system administration personnel within the VAEC Amazon Web Services who maintain the server hardware and Omnigo software who maintains the software, software but are not primary users of the VAPOLICERMS system itself. Omnigo signed a Business Associate

Agreement (BAA) with VA and each individual Omnigo contractor undergoes a background investigation, completes the VA Privacy and Information Security and Rules of Behavior training and must sign a Rules of Behavior before having access to the system.
Each contract is reviewed prior to approval based on the contract guidelines by the appropriate Contracting Officer's Representative. This review is conducted each time the contract period expires.
• Individuals are subject to a background investigation before given access to Veteran's information.
• All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
• Personnel including contractors that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.
• After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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.

VA requires Privacy and Information Security Awareness training be completed on an annual basis. The Talent Management System offers the following applicable privacy courses:
VA 10176: Privacy and Information Security Awareness and Rules of Behavior
VA 10203: Privacy and HIPPA Training
VA 3812493: Annual Government Ethics

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

If Yes, provide:

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

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

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

An ATO with conditions (Authority to Operate) was granted on September 10, 2020 for this system with an expiration date of March 9, 2021. This system is a cloud migration of the VA Police RMS system which was hosted in AITC and had an ATO granted on April 25, 2019 which expired April 24, 2020.
The FIPS 199 Classification for this system is 'MODERATE'.

Section 9. 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**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2021.01.17 22:01:53 -05'00'

PO, Rita K.Grewal

EDGARDO RIVERA-URRUTIA 116970

Digitally signed by EDGARDO RIVERA-URRUTIA 116970
Date: 2021.01.14 11:32:33 -04'00'

Information Security Systems Officer, Edgardo Rivera

Christopher B Oakleaf 157574

Digitally signed by Christopher B Oakleaf 157574
Date: 2021.01.19 14:57:35 -06'00'

System Owner, Christopher Oakleaf

APPENDIX A-6.1

The System of Record Notice (SORN) "The System of Records Notice associated with this system is ''Police and Security Records—VA'' (103VA07B). (December 8, 2008). This SORN can be found online at https://www.gpo.gov/fdsys/pkg/FR-2008-12-08/pdf/E8-29029.pdf