Privacy Impact Assessment for the VA IT System called:

Netskope Security Cloud

Enterprise Cloud Solution Office

VA Corporate

Date PIA submitted for review:

12/14/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.Facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	Andrew Vilailack	andrew.vilailack@va.gov	813-970-7568
Information System Owner	Scottie Ross	Scottie.Ross@va.gov	478-595-1349

Abstract

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

Netskope's Security Cloud (NSC) platform is a highly scalable, secure solution that processes and protects customer data traffic without the need to deploy on-premise physical hardware. The NSC services help customers eliminate cloud blind spots and to quickly analyze, target and control activities across thousands of cloud services and millions of websites with full control from one cloud platform. The full suite of services provided through the NSC provides 360-degreee data protection that guards data backed by advanced threat protection that stops intrusive attacks.

NSC's services provide real-time analytics and policies for third-party application used by its customers. The service allows for the termination of private cloud-based Software-as-a-Service (SaaS) application as well as standard web traffic to a single Netskope cloud endpoint that allows for auditing and policy enforcement on the use of these application and web sites. NSC enables businesses to use SaaS applications and web services while still being compliant with business and/or auditing policies.

Overview

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

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

Netskope Security Cloud is owned by the Enterprise Cloud Solutions Office (ESCO).

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

The system provides an enhanced and streamlined cybersecurity program that further protects VA data and defense against threats in cloud applications, cloud infrastructure, and the web.

C. Indicate the ownership or control of the IT system or project.

The system is a Commercial-Off-The-Shelf (COTS) SaaS solution, and therefore is VA controlled, but non-VA owned and operated.

2. Information Collection and Sharing

D. *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*

Information stored in this system consists of metadata correlated for reporting and synced back to security event/incident automation appliances/applications in the VA, no individual information will be affected or stored as information is for security monitoring and reporting.

E. *A general description of the information in the IT system and the purpose for collecting this information.*

The only information sharing leveraged by the system is with VA Active Directory, for name, username, and User ID. Netskope capability is for advanced detection and reporting and is not used by Veterans or other entities outside of the VA.

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

Metadata information collected or alerts generated is shared with the Enterprise Security Event Management system of the Security Operations Center.

G. *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.*

Information is stored in a Netskope SaaS cloud and does not reside in any VA sites.

3. Legal Authority and SORN

H. *A citation of the legal authority to operate the IT system.*

Department of Veterans Affairs Identity Management System (VAIDMS)-VA
E8-6120.pdf (govinfo.gov)

SORN: “146VA005Q3/73 FR 16093”

“The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.”

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

The system is not in process for a SORN.

D. System Changes

J. *Whether the completion of this PIA will result in circumstances that require changes to business processes*

This system does not store sensitive information which would require changes to business processes.

K. Whether the completion of this PIA could potentially result in technology changes

This system does not store sensitive information which would require technical changes to support PIA.

Section 1. Characterization of the Information

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

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

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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

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 Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers*
☐ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integrated Control Number (ICN)

☐Military History/Service Connection

☐ Next of Kin

☒ Other Data Elements (list below)

- Internet Source and Destination IP of the network traffic flow.
- Username and User ID of individuals accessing the system or passing traffic to the system
- Network traffic flows

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

PII Mapping of Components (Servers/Database)

Netskope Security Cloud consists of one key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Netskope Security Cloud and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system 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
VA Active Directory	Yes	Yes	Name, Username, User ID	Provide user identity and access groups to Netskope	Encryption, access controls

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

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

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

No data is collected from individuals. VA sends Active Directory data via System for Cross-domain Identity Management (SCIM) to Netskope Security Cloud. VA sends network logs through Netskope on-prem appliances at VA to NSC.

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

System data is required for the application functionality and to analyze the security of VA network traffic.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

The system only creates reports on metadata information collected.

1.3 How is the information collected?

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

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Metadata is collected from logs and traffic inspection of traffic going to SaaS applications.

1.3b 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.

Not Applicable – No information is collected by a form for this system.

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

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

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that *receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.*

Data is collected to further security practices at VA for the Cybersecurity Operations Center (CSOC) and Data Loss Prevention (DLP) reporting for the Enterprise efforts. The data is reviewed by CSOC and DLP for checks for accuracy and User data is continuously synchronized with the VA user system of record "Active Directory" to maintain accuracy and integrity.

1.4b 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.

Not Applicable – The Netskope Security Cloud system's use of any personal data is peripheral to the security services being provided and is not used for user/customer contact, interaction, or marketing purposes. As such, this data is not checked for accuracy through commercial aggregators of information. User data is continuously synchronized with the VA user system of record "Active Directory" to maintain accuracy and integrity.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

Netskope is the Cloud Access Security Broker tool used for the VA Enterprise for providing reporting on the VA environments from the VAEC and VA contracted SaaS.

The following SORN supports the collection of names, email addresses, phone numbers and user IDs for employees and contractors who need access to VA systems to perform their jobs:

Department of Veterans Affairs Identity Management System (VAIDMS)-VA
146VA005Q3/73 FR 16093

"The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317."

https://www.oprm.va.gov/docs/Current_SORN_List_2_25_2022.pdf

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

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: Information sent in the active directory SCIM communication contains the systems username, group information. If this information was intercepted systems users' risk having their name and proprietary VA Active Directory group information released.

Mitigation: The CSP will follow the FedRAMP and VA approved Incident Response Plans (IRP). This includes:
a. **Preparation**: Netskope conducts proactive investigation of potential issues, runs tabletop drills, and completes proactive identification of tooling/monitoring
b. **Detection**: When Netskope Security Operations becomes aware of an incident and initiates the Incident Response Process described here. The focus during this phase is to develop a clear problem statement and engage the key stakeholders to work the issue.
c. **Analysis**: Security Incident Response and Network Operations teams, work to identify the problem causing the incident and the appropriate restoration path. The focus during this phase is to identify the problem causing the incident, identify the proper restoration path, determine if there is a security exposure resulting from the incident, and determine if there is potential data loss or corruption resulting from the incident.
d. **Reporting**: Netskope will report the Incident to the System Owner and other designated POCs listed for that account as well as the US-CERT for us government (non-Department of Defense) customers
e. **Containment**: Responders take action to restore service and mitigate the problem causing the incident. The focus during this phase is to restore normal operations, restore the customer experience, and stop the loss of information.
f. **Eradication**: Responders work to address urgent problems that could allow the issue to repeat. The focus during this phase is to prevent an immediate recurrence of the issue and risk mitigation controls in place.
g. **Recovery**: Normal service operation is restored, and risk of recurrence is mitigated. The focus during this phase is documenting the issue, collecting forensic data for the Postmortem, and communicating the "All Clear" to stakeholders.

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.

Data collected is to further security practices at VA for the Cybersecurity Operations Center (CSOC) and Data Loss Prevention (DLP) reporting for the Enterprise efforts.

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

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

The Netskope Security Cloud analyzes VA network traffic and user cloud service usage to identify potential security issues include malicious software, malicious web sites, data loss prevention, and an unauthorized use of VA cloud services. The service creates event logs based on this activity, i.e. User X accessed cloud application Y at this data and time and attempted to upload a file with malicious software Z.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The Netskope Security Cloud can be configured to provide reports based on application and web usage by individuals; the source is derived directly from the end-user's device if the user traffic is routed to the Netskope Security Cloud. VA authorized administrators additionally have the ability to configure to route or non-route specific web sites or applications to Netskope Security Cloud.

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

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

The Netskope Security Cloud has been implemented and assessed to FedRAMP High requirements including FIPS approved encryption and storage as well as all of the other security and monitoring controls required by FedRAMP High.

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

Social Security Numbers are not being collected.

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

The Netskope Security Cloud has been implemented and assessed to FedRAMP High requirements including FIPS approved encryption and storage as well as all of the other security and monitoring controls required by FedRAMP High.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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.

2.4a How is access to the PII determined?

Need to know, role-based access controls, and access request and approval processes as required by FedRAMP High.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes, criteria, procedures, controls, and responsibilities regarding access are document in alignment with FedRAMP High Requirements.

2.4c Does access require manager approval?

Yes

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

Yes

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

Shared responsibility: The VA System Owner and the Netskope Global Information Security Team

Section 3. Retention of Information

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

3.1 What information is retained?

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

Name, username, User ID, network traffic, IP address

3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. **For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods**. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

On the Netskope side, it is only held for 90 days online and another 30 days in backups 120 days total. VA side data is retained based on Splunk policies. Active Directory (AD) user info is retained indefinitely for as long as the service is active, and users are active through synchronized AD interface. Once they are no longer active, data is only retained for 30 more days.

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

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA Records Officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.
This question is related to privacy control DM-2, Data Retention and Disposal.

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

Yes

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

120 days

Record Type	Retention Schedule	Series	Disposition Authority
User Name	1 year online – Transferred to VA Security Incident Event Management System	General Technology Management Records	DAA-GRS-2013-0005-0004
Group Information	1 year online – Transferred to VA Security Incident Event Management System	General Technology Management Records	DAA-GRS-2013-0005-0004
IP Information	1 year online – Transferred to VA Security Incident Event Management System	General Technology Management Records	DAA-GRS-2013-0005-0004
Meta Data	1 year online – Transferred to VA Security Incident Event Management System	General Technology Management Records	DAA-GRS-2013-0005-0004

This system complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records will be retained as long as the information is needed in accordance with a NARA-approved retention period. Records are retained according to Record Control Schedule 10-1 (reference: https://www.archives.gov/). Also see the General Record Schedule located here: https://www.archives.gov/files/records-mgmt/grs/grs04-2.pdf

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

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

Netskope Security Cloud – No paper records. Digital data is purged from databases and backups on an automated rotating cycle. All digital storage devices are encrypted with full disk encryption and physically destroyed prior to removal from our secured data centers and certificates of destruction are provided.

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 VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1

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

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

Netskope Security Cloud: No PII is used for research, testing, or training.

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

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

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

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

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

Follow the format below:

Privacy Risk: Information including the systems username and group information could be released.

Mitigation: The CSP will follow the FedRAMP and VA approved Incident Response Plans (IRP). This includes:
a. **Preparation**: Netskope conducts proactive investigation of potential issues, runs tabletop drills, and completes proactive identification of tooling/monitoring
b. **Detection**: When Netskope Security Operations becomes aware of an incident and initiates the Incident Response Process described here. The focus during this phase is to develop a clear problem statement and engage the key stakeholders to work the issue.
c. **Analysis**: Security Incident Response and Network Operations teams, work to identify the problem causing the incident and the appropriate restoration path. The focus during this phase is to identify the problem causing the incident, identify the proper restoration path, determine if there is a security exposure resulting from the incident, and determine if there is potential data loss or corruption resulting from the incident.
d. **Reporting**: Netskope will report the Incident to the System Owner and other designated POCs listed for that account as well as the US-CERT for us government (non-Department of Defense) customers
e. **Containment**: Responders take action to restore service and mitigate the problem causing the incident. The focus during this phase is to restore normal operations, restore the customer experience, and stop the loss of information.
f. **Eradication**: Responders work to address urgent problems that could allow the issue to repeat. The focus during this phase is to prevent an immediate recurrence of the issue and risk mitigation controls in place.
g. **Recovery**: Normal service operation is restored, and risk of recurrence is mitigated. The focus during this phase is documenting the issue, collecting forensic data for the Postmortem, and communicating the "All Clear" to stakeholders.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

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 PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VA Active Directory (Numerous)	Provide user identity and access groups to Netskope	Name, username, group ID	TLS (Transport Layer Security)

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk: Information including the systems username and group information could be released.

Mitigation: The CSP will follow the FedRAMP and VA approved Incident Response Plans (IRP). This includes:
a. **Preparation**: Netskope conducts proactive investigation of potential issues, runs tabletop drills, and completes proactive identification of tooling/monitoring
b. **Detection**: When Netskope Security Operations becomes aware of an incident and initiates the Incident Response Process described here. The focus during this phase is to develop a clear problem statement and engage the key stakeholders to work the issue.
c. **Analysis**: Security Incident Response and Network Operations teams, work to identify the problem causing the incident and the appropriate restoration path. The focus during this phase is to identify the problem causing the incident, identify the proper restoration path, determine if there is a security exposure resulting from the incident, and determine if there is potential data loss or corruption resulting from the incident.
d. **Reporting**: Netskope will report the Incident to the System Owner and other designated POCs listed for that account as well as the US-CERT for us government (non-Department of Defense) customers
e. **Containment**: Responders take action to restore service and mitigate the problem causing the incident. The focus during this phase is to restore normal operations, restore the customer experience, and stop the loss of information.
f. **Eradication**: Responders work to address urgent problems that could allow the issue to repeat. The focus during this phase is to prevent an immediate recurrence of the issue and risk mitigation controls in place.
g. **Recovery**: Normal service operation is restored, and risk of recurrence is mitigated. The focus during this phase is documenting the issue, collecting forensic data for the Postmortem, and communicating the "All Clear" to stakeholders.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

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

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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:

<u>Privacy Risk:</u>

Due to the sensitive nature of this user data, there is a risk that, if the data were accessed or received by unauthorized parties/recipients or otherwise breached, serious personal, professional and/or financial harm may result for the affected individuals. VA would be required to provide credit monitoring and ID theft insurance.

<u>Mitigation:</u>

The FedRAMP approved NSC (Netskope Security Cloud) uses a number of security measures designed to ensure that the information is not inappropriately disclosed or released. Use of encryption to secure data during transmission and at rest; user information security and privacy education and training; restricted use of removable media, weekly administrative rounds to identify any potential issues, security screens. The measures also include, access controls, security assessments, contingency planning, incident response, system and communications protection

Our facilities employ all security controls in the respective high impact control baseline unless specific exceptions have been allowed based on the guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives.

The NSC applications uses VA active directory roles and permissions.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Netskope is a data processor and not a data controller. Netskope maintains an agreement with the VA for processing data provided to it from the VA, but Netskope does not provide notice directly to VA users. Netskope does maintain a public privacy policy posted on our public website.

SORN: "Department of Veterans Affairs Identity Management System (VAIDMS)-VA, 146VA005Q3/73 FR 16093
E8-6120.pdf (govinfo.gov)
https://www.oprm.va.gov/docs/SORN/Current_SORN_List_10_21_2022.pdf

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

Netskope is a data processor and not a data controller. Netskope maintains an agreement with the VA for processing data provided to it from the VA, but Netskope does not provide notice directly to VA users.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

Users of the system accept a splash page notification.

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.

Netskope is a data processor and not a data controller. Netskope maintains an agreement with the VA for processing data provided to it from the VA, but Netskope does not provide notice directly to VA users.

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.

No, data is being collected and used for VA information security purposes.

Netskope is a data processor and not a data controller. Netskope maintains an agreement with the VA for processing data provided to it from the VA, but Netskope does not provide notice or manage consent directly with VA users.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

Privacy Risk: End user notices are not provided; therefore, it is not applicable.

Mitigation: N/A

Section 7. Access, Redress, and Correction

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

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

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

*7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. **For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

VA process for system administration for an IT security monitoring system are followed for access.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

System is not exempt.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

VA process for system administration for an IT security monitoring system are followed for access.

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.

Not applicable as the data is security related and not made available to the individual.

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.

Not applicable as the data is security related and not made available to the individual.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Not applicable as the data is security related and not made available to the individual.

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

Consider the following FIPPs below to assist in providing a response:
Principle of 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: Not applicable because data is security related and not made available to the individual

Mitigation: N/A

Section 8. Technical Access and Security

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

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

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

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

Not applicable as the data is security related and not made available to the individual

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

System is for VA access only

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Not applicable as the data is security related and not made available to the individual

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Confidentiality agreement include NDA in place between VA and contractors.

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.

Yearly Security & Privacy training is mandated for all Netskope personnel who may have access the NSC (Netskope Security Cloud). All individuals who access VA IT systems are required to take annual VA security training such as HIPPA, RoB (TMS) as well.

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

8.4a If Yes, provide:

1. *The Security Plan Status: Completed*
2. *The System Security Plan Status Date:*12/17/2021
3. *The Authorization Status:* In progress
4. *The Authorization Date:* TBD
5. *The Authorization Termination Date: TBD*
6. *The Risk Review Completion Date:* TBD
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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

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

N/A

Section 9 – Technology Usage

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

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

***Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1**. (Refer to question 3.3.1 of the PTA)*

Netskope is a COTS SaaS that is currently pursuing a FedRAMP High authorization. It will be within the VAEC boundary, but the SaaS portion will be hosted on Netskope's cloud boundary that will be authorized at the high impact level.

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

VA owns the data and NSC is solely the processor.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

Cloud Security Provider will not be collecting any ancillary data.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

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

Netskope has provided the VA as part of its FedRAMP package a clearly defined CIS/CRM document that details the controls that are either shared or solely the responsibility of the VA.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

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

Netskope Security Cloud does not use RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress

ID	**Privacy Controls**
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Tonya L.
Facemire 234776

Digitally signed by Tonya L.
Facemire 234776
Date: 2022.12.21 20:27:25 -05'00'

Privacy Officer, Tonya Facemire

Digitally signed by ANDREW
VILAILACK
Date: 2022.12.22 09:21:57
-05'00'

Information Systems Security Officer, Andrew Vilailack

SCOTTIE ROSS

Digitally signed by SCOTTIE
ROSS
Date: 2022.12.22 09:37:07 -05'00'

Information Systems Owner, Scottie Ross

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).

“Department of Veterans Affairs Identity Management System (VAIDMS)-VA, 146VA005Q3/73 FR 16093

E8-6120.pdf (govinfo.gov)

https://www.oprm.va.gov/docs/SORN/Current_SORN_List_10_21_2022.pdf

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices