



Privacy Impact Assessment for the VA IT System called:

Microsoft Defender Extended Detection and Response (MS-XDR)

Office of Information Technology (OIT)

Infrastructure Operations Cyber Security Management (ICSM)

eMASS ID 2374

04/12/2024

System Contacts:

System Contacts

| | Name | E-mail | Phone Number |
|--|----------------|--|--------------|
| Privacy Officer | Tonya Facemire | OITPrivacy@va.gov; tonya.facemire@va.gov | 202-632-8423 |
| Information System Security Officer (ISSO) | Eric Abraham | eric.abraham@va.gov | 512-326-7422 |
| Information System Owner | Gregory Watson | Gregory.watson@va.gov | 303-947-8137 |

Abstract

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

Microsoft Defender Extended Detection and Response (MS-MS-XDR) is a Microsoft SaaS solution that will operate in Microsoft Azure Government and Commercial Clouds. MS-XDR is an endpoint detection and response tool that broadens the scope of protection by providing data analysis across the VA network. MS-XDR includes Microsoft Defender for Cloud, Microsoft Defender for Endpoint, Defender for Identity, Microsoft 365 Defender, Defender for Office 365, Defender for Cloud Apps, Azure AD Identity Protection, Microsoft Defender for IoT, and Microsoft Sentinel. MS-XDR provides analysis of endpoints, networks, servers, cloud workloads, SIEM and much more by sifting through thousands of information logs. MS-XDR leverages the power of artificial intelligence, machine learning and automation. The goal of MS-XDR is to provide accurate, context-rich alerts to security teams. MS-XDR stores its data within the Azure Sentinel product for 1 year (first in a hot storage table for 90 days and then moved to a cold storage table for 9 months within the Log Analytics workspace in Azure Monitoring). Access to MS-XDR is limited to Privileged Users with Fob Tokens.

Microsoft limits collection of customer data to four specific data categories: Customer data, Service-generated data, Diagnostic data, and Professional services data. Microsoft uses data from these categories to perform a limited set of legitimate business operations (LBOs) required for us to provide services to our customers. When data is collected and processed to perform LBOs, Microsoft protects individual customers and users by pseudonymizing diagnostic data and aggregating data prior to use. Microsoft does not access the contents of customer data to determine which specific pieces of data might be considered personal. Instead, it is assumed that all customer data and all professional services data contain personal data and protect the data accordingly.

Overview

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

1 General Description

A. *What is the IT system name and the name of the program office that owns the IT system?*
The IT System name is Microsoft Defender Extended Detection and Response (MS-XDR). The Program office that owns it is Infrastructure Operations Cybersecurity Management (ICSM).

B. *What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*
MS-XDR provides analysis of endpoints, networks, servers, cloud workloads, SIEM and much more by sifting through thousands of information logs. MS-XDR leverages the power of artificial intelligence, machine learning and automation. The goal of MS-XDR is to provide accurate, context-rich alerts to security teams.

C. *Who is the owner or control of the IT system or project?*
The Data/Business/Information Owner is Chad Oglesbee. The Information System Owner is Gregory Watson.

2. Information Collection and Sharing

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

MS-XDR provides analysis of endpoints, networks, servers, cloud workloads, SIEM and much more by sifting through thousands of information logs. MS-XDR leverages the power of artificial intelligence, machine learning and automation. The goal of MS-XDR is to provide accurate, context-rich alerts to security teams. MS-XDR stores its data within the Azure Sentinel product for 1 year (first in a hot storage table for 90 days and then moved to a cold storage table for 9 months within the Log Analytics workspace in Azure Monitoring). Microsoft limits collection of customer data to four specific data categories: Customer data, Service-generated data, Diagnostic data, and Professional services data. Microsoft uses data from these categories to perform a limited set of legitimate business operations (LBOs) required for us to provide services to our customers. When data is collected and processed to perform LBOs, Microsoft protects individual customers and users by pseudonymizing diagnostic data and aggregating data prior to use. Microsoft does not access the contents of customer data to determine which specific pieces of data might be considered personal. Instead, it is assumed that all customer data and all professional services data contain personal data and protect the data accordingly.

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

The general description of the information in MS-XDR is the users' and assets' information gained from the Microsoft Sentinel Azure Active Directory Data connector and other data connectors. These data connectors then collect the Active directory logs and system logs where the data elements: host IPs and ports, User name, email address, phone number, domain name, computer name, logon events, password changes, group membership, service principal names, Kerberos tickets, and LDAP queries may be collected and stored for 90 days.

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

MS-XDR shares information from Active Directory via the Microsoft Entra (formerly known as Azure Active Directory) data connector.

G. Is the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?

MS-XDR is operated on both the Microsoft Azure Government and Microsoft Azure Commercial clouds. The same controls are use on both clouds to encrypt and protect PII. Please see the FedRAMP Package Microsoft Azure Government ID# F1603087869 and Microsoft Azure Commercial ID# F1209051525 SSPs for more details.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system? AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Executive Orders 9397, 10450, 10865, 12333, and 12356; 5 U.S.C 3301 and 9101; 42 U.S.C 2165 and 2201; 50 U.S.C 781 to 887; 5 C.F.R 5, 732, and 736; and Homeland Security Presidential Directive 12.

SORN from the OPRM site.

<https://www.govinfo.gov/content/pkg/FR-2022-07-01/pdf/2022-14118.pdf>

- 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 SORN does not require an amendment.

4. System Changes

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

No

- K. *Will the completion of this PIA could potentially result in technology changes?*

No

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://vawww.va.gov/vapubs/>). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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

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

- | | | |
|---|---|---|
| <input type="checkbox"/> Name | <input type="checkbox"/> Personal Phone Number(s) | Number, etc. of a different individual) |
| <input type="checkbox"/> Social Security Number | <input type="checkbox"/> Personal Fax Number | <input type="checkbox"/> Financial Information |
| <input type="checkbox"/> Date of Birth | <input type="checkbox"/> Personal Email Address | <input type="checkbox"/> Health Insurance Beneficiary Numbers |
| <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Emergency Contact Information (Name, Phone | Account numbers |
| <input type="checkbox"/> Personal Mailing Address | | |

- Certificate/License numbers¹
- 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)

Other PII/PHI data elements: host IPs and ports, Username, Display Name, work email address, Work phone number, domain name, computer name, logon events, password changes, group membership, service principal names, Kerberos tickets, and LDAP – Lightweight Directory Access Protocol- queries

PII Mapping of Components (Servers/Database)

Microsoft Defender Extended Detection and Response (MS-XDR) consists of 2 Log analytic workspaces which are tied to the Sentinel instance one in Microsoft Azure Government and one in Microsoft Azure Commercial as key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Microsoft Defender Extended Detection and Response (MS-XDR) and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

| Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI | Does this system collect PII? (Yes/No) | Does this system store PII? (Yes/No) | Type of PII (SSN, DOB, etc.) | Reason for Collection/ Storage of PII | Safeguards |
|--|---|---|--|--|--|
| Azure Monitoring Log Analytics Workspace | Yes | yes | host IPs and ports, User name, Display Name, email address, phone number, domain | Authentication | Encryption of data, controlled access, logical isolation between each account, |

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

| | | | | | |
|--|--|--|---|--|----------------------|
| | | | name, computer name, logon events password changes, group membership, service principal names, Kerberos tickets, LDAP queries | | logging of access |
|--|--|--|---|--|----------------------|

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

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

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

The data is collected from data connectors which collect the Active Directory logs, system logs, event logs etc. The logs are stored for 1 year (first in a hot storage table for 90 days and then moved to a cold storage table for 9 months) within the Azure Monitoring Logs in case the data needs to be rehydrated to investigate a cyber security incident.

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.

The MS-XDR data is sourced from logs. MS-XDR is an endpoint detection and response tool that broadens the scope of protection by providing data analysis across the VA network. MS-XDR includes Microsoft Defender for Cloud, Microsoft Defender for Endpoint, Defender for Identity, Microsoft 365 Defender, Defender for Office 365, Defender for Cloud Apps, Azure AD Identity Protection, Microsoft Defender for IoT, and Microsoft Sentinel. MS-XDR provides analysis of endpoints, networks, servers, cloud workloads, SIEM and much more by sifting through thousands of information logs. MS-XDR leverages the power of artificial intelligence, machine learning and automation. The goal of MS-XDR is to provide accurate, context-rich alerts to security teams.

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

MS-XDR creates alerts and incident reports from the data which is being reviewed and analyzed.

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?

The data is collected from data connectors which collect the Active Directory logs, system logs, event logs etc. This data is fed into the Azure Log Analytics Workspace.

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

Information is not collected on a form. N/A

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.

The data is collected from data connectors which collect the Active Directory logs, system logs, event logs etc. The logs are stored for 1 year (first in a hot storage table for 90 days and then moved to a cold storage table for 9 months) within the Azure Monitoring Logs in case the data needs to be rehydrated to investigate a cyber security incident. Active Directory integration has real-time synchronization in place. Log Analytics' custom data ingestion process provides a high level of control over the data that gets ingested. Log Analytics uses data collection rules (DCRs) to collect data. Azure Monitor is enabled and collects metrics and activity logs on the Log Analytic workspace.

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

NO

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

- Laws and Regulations: Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) circulars, Public Law, United States Code, and Homeland Security Presidential Directives.

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: (Very Low) A user of the system shares his/her PIV card and Personal PIN along with their FOB key and password with someone, and that person or persons access the MS-XDR system without proper credentials and attempts to retrieve or destroy data.

Mitigation: Limit Access based on log activity, appropriate responses can be executed immediately. User would have to be logged into VA Network first to access MS-XDR and then would have to use elevated privileges to access the MS-XDR components in Azure.

Section 2. Uses of the Information

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

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

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

| PII/PHI Data Element | Internal Use | External Use |
|----------------------|--------------|--------------|
|----------------------|--------------|--------------|

| | | |
|---|---|----------|
| host IPs and ports, Username, Display Name, email address, phone number, domain name, computer name, logon events password changes, group membership, service principal names, Kerberos tickets, LDAP queries | Security alert, Incident alert, Threat hunting and cyber security investigation | Not used |
|---|---|----------|

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 MS-XDR data is sourced from logs. MS-XDR is an endpoint detection and response tool that broadens the scope of protection by providing data analysis across the VA network. MS-XDR includes Microsoft Defender for Cloud, Microsoft Defender for Endpoint, Defender for Identity, Microsoft 365 Defender, Defender for Office 365, Defender for Cloud Apps, Azure AD Identity Protection, Microsoft Defender for IoT, and Microsoft Sentinel. MS-XDR provides analysis of endpoints, networks, servers, cloud workloads, SIEM and much more by sifting through thousands of information logs. MS-XDR leverages the power of artificial intelligence, machine learning and automation. The goal of MS-XDR is to provide accurate, context-rich alerts to security teams.

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 data is collected from data connectors which collect the Active Directory logs, system logs, event logs etc. The logs are stored for 1 year (first in a hot storage table for 90 days and then moved to a cold storage table for 9 months) within the Azure Monitoring Logs in case the data needs to be rehydrated to investigate a cyber security incident.

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?

All data at rest and data in transit is encrypted. Azure encrypts data using 256-bit AES encryption. For data in transit, Azure uses TLS/SSL to secure the communication between applications and Azure services.

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

MS-XDR does not collect, process or retain Social Security Numbers. N/A

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

To safeguard PII/PHI, Azure offers several features and tools, such as data masking, role-based access control, auditing, and compliance certifications. The MS-XDR system utilizes role-based access and elevated privileges access to the MS-XDR system along with all data at rest and in transit is encrypted.

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?*

Users access the MS-XDR via their VA Network Account and then via their assigned elevated privileges. To get a VA Network Account, the user has gone through the VA onboarding process, which includes background check. Administrative access is granted via the VA's Non-eMail Enabled Account (NMEA - 0 account) request process. The VA requires manager approval on NMEA requests, processed through ePAS.

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

Yes. Administrative access is granted via the VA's Non-eMail Enabled Account (NMEA - 0 account) request process.

2.4c *Does access require manager approval?*

Yes

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

Yes via Microsoft Entra (formerly known as Azure Active Directory) logs

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

The system owner, who is the approver of the requested access.

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

Host IPs and ports, Username, Display Name, email address, phone number, domain name, computer name, logon events password changes, group membership, service principal names, Kerberos tickets, LDAP queries data is collected from data connectors which collect the Active Directory logs, system logs, event logs etc. The logs are stored for 1 year (first in a hot storage table for 90 days and then moved to a cold storage table for 9 months) within the Azure Monitoring Logs in case the data needs to be rehydrated to investigate a cyber security incident.

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.*

The logs are stored for 1 year (first in a hot storage table for 90 days and then moved to a cold storage table for 9 months) within the Azure Monitoring Logs in case the data needs to be rehydrated to investigate a cyber security incident.

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

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

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

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

SORN from the OPRM site. (https://www.oprm.va.gov/privacy/systems_of_records.aspx).
145VA005Q3.

<https://www.govinfo.gov/content/pkg/FR-2022-07-01/pdf/2022-14118.pdf>

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

The logs are stored for 1 year (first in a hot storage table for 90 days and then moved to a cold storage table for 9 months) within the Azure Monitoring Logs in case the data needs to be rehydrated to investigate a cyber security incident.

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.

SORN from the OPRM site. (https://www.oprm.va.gov/privacy/systems_of_records.aspx).

145VA005Q3. Department of Veterans Affairs Personnel Security File System (VAPFS) - VA <https://public-inspection.federalregister.gov/2022-14118.pdf>

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.

MS-XDR data is not used for research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: Very Low. There is a risk information could be stored for longer than necessary.

Mitigation: The Azure Monitoring Logs are stored in the Log Analytics Workspace. The tables for the data will be configured with how long the data should be retained whether in hot (analytic/basic logs) or cold (archived logs) log status. Once that data has reached the configured time of retention in the archived logs the data is purged/permanently deleted from the system.

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.

| <i>List the Program Office or IT System information is shared/received with</i> | <i>List the purpose of the information being shared /received with the specified program office or IT system</i> | <i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i> | <i>Describe the method of transmittal</i> |
|---|---|---|---|
| Active Directory | MS-XDR is an endpoint detection and response tool that broadens the scope of protection by providing data analysis across the VA network. The goal of MS-XDR is to provide accurate, context-rich alerts to security teams. | host IPs and ports, Username, Display Name, email address, phone number, domain name, computer name, logon events password changes, group membership, service principal names, Kerberos tickets, LDAP queries | MS-XDR gains user information from the Microsoft Sentinel Azure Active Directory Data connector. The connector then collects the Active Directory logs where the data elements listed in this table may be collected and stored for 1 year. |

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Very Low There is a very low risk for information shared internally being shared internally.

Mitigation: MS-XDR obtains data from the Active Directory Data connector. The information in MS-XDR is not shared internally with the Active Directory system. The log analytics workspace is read only access for the data. MS-XDR also has Role Based Access Control (RBAC) enforced for users. The MS-XDR user requires elevated privileges and the correct RBAC assignment to access the log analytics workspace. The assignment and approval of personnel assigned to MS-XDR has several check and balances with approval from COR and System Owner for assignments.

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

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Version date: October 1, 2023

Page 15 of 32

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

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

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

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

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

Follow the format below:

Privacy Risk: Very Low: A user must be on the VA network, authenticated with their PIV, possess elevated privileges, and be assigned the correct RBAC role via security groups to be able to access the MS-XDR system. If a user is not supposed to have access to the VA network and somehow still possess their elevated privileges, but still does, the user could still access the MS-XDR if permissions to the security groups for access to the portal was not removed.

Mitigation: The mitigation for this is to have personnel access removed when they leave the team or no longer need access to MS-XDR. MS-XDR's System Owner or person designated by MS-XDR's System Owner completes a monthly review of the MS-XDR user accounts and validates they still need access.

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.

<https://www.govinfo.gov/content/pkg/FR-2022-07-01/pdf/2022-14118.pdf>

[2022-14118.pdf \(federalregister.gov\)](#)

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

Yes, a notice will be provided and attached is a copy of the current notice.

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.

All MS-XDR are internal VA users and must select OK to the banner below when logging onto MS-XDR which states that “All transactions that occur are subject to reviewing-retrieving-copying-auditing-inspecting-investigating-restricting-access-blocking-tracking-disclosing to authorized personnel or any other authorized actions by all authorized VA and law enforcement personnel” This notice lets the individual know that anything they do on this system is being tracked and monitored (which would include any PII they enter).

Bulletins are also emailed out when changes occur to the MS-XDR system. An example of a bulletin is provided as an attachment in APPENDIX A-6.1.

Security Warning

This U.S. government system is intended to be used by authorized VA network users for viewing and retrieving information only except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA. All use is considered to be with an understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government Intranet or Extranet (non-public) networks or systems. All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring- recording- retrieving- copying- auditing – inspecting-investigating- restricting access- blocking-tracking- disclosing to authorized personnel or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms.

Unauthorized attempts or acts to either (1) access- upload- change- or delete information on this system (2) modify this system (3) deny access to this system or (4) accrue resources for unauthorized use on this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal civil or administrative penalties.

These words are followed by a checkbox where the user has to select “OK”

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

Yes, the user can refuse to select OK. If user refuses to click OK they will not gain access to the VA network and MS-XDR system.

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

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

The consent the user is agreeing to is in the security warning.

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: Very low. Somehow the Security warning did not populate when user was attempting to sign into VA Network, or a user is able to bypass the security warning without selecting the OK button.

Mitigation: The Security warning is controlled by VA policy and access to the VA network will not be granted if OK is not selected. Even if a user would be able to gain access to the VA Network, they would still require the elevated privileges and correct assigned security groups to gain access to the MS-XDR system.

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.***

Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above. A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort. (From [2022-14118.pdf \(federalregister.gov\)](#))

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)?

It is not a Privacy Act System. It is a security tool, so access is restricted Via elevated privilege

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?

It is not a Privacy Act System. It is a security tool, so access is restricted Via elevated privilege

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above. A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort. (From [2022-14118.pdf \(federalregister.gov\)](#))

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.

From [2022-14118.pdf \(federalregister.gov\)](#)

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 ensure data accuracy.***

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

Per the bulletin (Appendix A) that is provided to the individual, they will reach out the Data Loss Prevention team.

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: Very Low. There is a risk that individuals will be unaware of how to correct any inaccurate information.

Mitigation: Users can correct AD information by submitting a SNOW ticket. All other information collected by connectors and APIs are log base information from VA assets.

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?

The same access policies that apply to the VA network apply to the MS-XDR system. Access to MS-XDR is requested via the ticketing system and approvals are received before a user's VA account is added to the appropriate security group(s) for access to the Azure portal or to the jump boxes. MS-XDR access requires elevated privilege access via ePAS and correct Security group assignment for the user to gain access.

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?

All users for MS-XDR will be VA employees or VA Contractors. This is a VA internal only system. VA establishes what PII can be shared for MS-XDR. The same access policies that apply to the VA network apply to the MS-XDR system. Access to MS-XDR is requested via the ticketing system and approvals are received before a user's VA account is added to the

appropriate security group(s) for access to the Azure portal or to the jump boxes. MS-XDR access requires elevated privilege access via ePAS and correct Security group assignment for the user to gain access.

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.

Read-only, Contributor, Owner, Security Administrator, Global Administrator.

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.

The same access policies that apply to the VA network apply to the MS-XDR system. Contractors follow the VA onboarding process, which includes signing a confidentiality agreement. Access to MS-XDR is requested via the ticketing system and approvals are received before a user's VA account is added to the appropriate security group(s) for access to the Azure portal or to the jump boxes. MS-XDR access requires elevated privilege access via ePAS and correct Security group assignment for the user to gain access.

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

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

All users that access the MS-XDR have gone through the VA Onboarding process, which includes the required Privacy and HIPAA Training.

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

NO

8.4a If Yes, provide:

1. *The Security Plan Status: <<ADD ANSWER HERE>>*
2. *The System Security Plan Status Date: <<ADD ANSWER HERE>>*

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

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.**
05/15/2024

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)

MS-XDR uses FedRAMP FISMA High Microsoft Azure Government and FedRAMP FISMA High Microsoft Azure Commercial Software as a Service (SaaS) Services

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.

The VA maintains ownership of the data, and selects which services can process, store, and host data. The CSP does not access or use the data for any purpose without agreement from the VA. VA determines where the data will be stored, including the type of storage and geographic region of that storage. VA manages access to its data, and access to services and resources through users, groups, permissions, and credentials that are internally controlled. VA chooses the secured state of the data. The CSP provides encryption features that protect data in transit and at rest and provides VA with the option to manage their encryption keys. VA Enterprise Contract, NNG15SD22B VA118-17-F-2284 for Microsoft Commercial and 47QTCA22D003G for Microsoft Azure Government.

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.

The CSP automatically collect metrics, such as offering usage, occurrences of technical errors, diagnostic reports, settings preferences, backup information, API calls, and other logs. VAEC is the owner of its data (customer data). The CSP does not use customer data and has anonymized metrics to help them measure, support, and improve their services. The CSP has ownership of these anonymized metrics.

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.

For all cloud deployment types, the customer owns their data and identities. The customer is responsible for protecting the security of their data and identities, on-premises resources, and the cloud components they control (which varies by service type). This is the Shared Responsibility Model for Security in the Cloud.

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).

MS-XDR is an endpoint detection and response tool that broadens the scope of protection by providing data analysis across the VA network. MS-XDR includes Microsoft Defender for Cloud, Microsoft Defender for Endpoint, Defender for Identity, Microsoft 365 Defender, Defender for Office 365, Defender for Cloud Apps, Azure AD Identity Protection, Microsoft Defender for IoT, and Microsoft Sentinel. MS-XDR provides analysis of endpoints, networks, servers, cloud workloads, SIEM and much more by sifting through thousands of information logs. MS-XDR leverages the power of artificial intelligence, machine learning and automation. The goal of MS-XDR is to provide accurate, context-rich alerts to security teams.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

Privacy Officer, Tonya Facemire

Information System Security Officer, Eric Abraham

Information System Owner, Gregory Watson

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

<https://www.govinfo.gov/content/pkg/FR-2022-07-01/pdf/2022-14118.pdf>

[2022-14118.pdf \(federalregister.gov\)](#)

Security Warning

This U.S. government system is intended to be used by authorized VA network users for viewing and retrieving information only except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA. All use is considered to be with an understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government Intranet or Extranet (non-public) networks or systems. All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring- recording- retrieving- copying- auditing – inspecting-investigating- restricting access- blocking-tracking- disclosing to authorized personnel or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms.

Unauthorized attempts or acts to either (1) access- upload- change- or delete information on this system (2) modify this system (3) deny access to this system or (4) accrue resources for unauthorized use on this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal civil or administrative penalties.

These words are followed by a checkbox where the use has to select “OK”

Automated Protection of VA Credentials/Secrets

Bulletin No.

August 25, 2024

Introduction

The Automated Protection of VA Credentials/Secrets project is a collaborative effort between The Data Loss Prevention (DLP) team and the Azure Information Protection (AIP) team. The project is deploying a new Sensitivity Label called **VA Credential-Secrets Protect** that protect VA Tokens, Keys, and Certificates within the VA network and being shared externally. **VA users may be impacted due to the automated enforcement of outbound communications that contain these data elements.** The Information Security Engineering (ISE) DLP team authored this bulletin.

Sponsor: Amber Pearson, Deputy Chief Information Security Officer, and Jason Miller, Director Collaboration Service are the sponsors of this project.

Background

The VA Credential-Secrets Protect Sensitivity Label tags and protects content containing VA credentials. This content will be automatically encrypted in these repositories and on internal email messages. In addition, email messages containing VA credentials will be restricted from external recipients. No action by VA users is required to apply the VA Credential-Secrets Protect Sensitivity Label. However, if a VA user is attempting to send content containing VA credentials to an external recipient, the content will be blocked, and the user will receive the following automated notification message:

This action is being taken to mitigate cybersecurity incidents associated with the disclosure of credentials in 3rd-party environments. This action bolsters VA's progress in addressing Executive Order (EO) 14028 [Improving the Nation's Cybersecurity](#) requirements.

Project Schedule

Enterprise-wide enforcement of this Sensitivity Label will begin on August XX, 2024.

Access the following links for additional resources:

- [Data Loss Prevention](#)
- [VA Azure Information Protection \(AIP\)](#)

Points of Contact

Connectivity and Collaboration Services

Ahmed-Daha Hassan, AIP Team Lead
oitccsaip@va.gov

Office of Information Security

Niles Kirchoffer, DLP Program Manager
oisdatalosspreventionsupport@va.gov

HELPFUL LINKS:

General Records Schedule

<https://www.archives.gov/records-mgmt/grs.html>

National Archives (Federal Records Management):

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

VA Publications:

<https://www.va.gov/vapubs/>

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

[VHA Notice of Privacy Practices](#)

[VHA Handbook 1605.04: Notice of Privacy Practices](#)