Privacy Impact Assessment for the VA IT System called:

Box Enterprise Cloud Content Collaboration Platform-I

Office of Information and Technology

Office of General Counsel (OGC)

eMASS ID #1787

Date PIA submitted for review:

10/29/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.Drake@va.gov OITPrivacy@va.gov	202-632-8431
Information System Security Officer (ISSO)	Anna Johnson	Anna.Johnson3@va.gov	520-629-4930
Information System Owner	Kary Storms	Kary.Storms@va.gov	531-247-9026

Abstract

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

Box is an enterprise content management platform that solves simple and complex challenges, from sharing and accessing files on approved devices to sophisticated business processes like data governance and retention. The Box enterprise content management platform enables business to easily share, manage and secure their content. In today's cloud-first world, providing employees with secure access to content at any time using approved devices is critical to creating a more productive, connected workforce and improved customer experiences. Beyond secure file sharing, Box enables easy access to content from approved devices with the security, scalability, and administrative controls that IT requires. In addition to Box's core content management platform offering, customers have more control over their content to meet security, compliance, and privacy requirements.

Overview

The overview is the most important section of the Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*

Box Enterprise Cloud Content Collaboration Platform-I enables easy access to content from approved devices with the security, scalability, and administrative controls that IT requires. The purpose of information being shared is so VA OGC staff can exchange large files with other Federal Agencies, the Courts, and parties in litigation. These documents are sensitive and would allow bad actors to discover vulnerabilities in these systems and possibly steal sensitive VA Data or disrupt VA operations. OGC needs to securely send and receive this information to and from stakeholders to maintain the highest level of cybersecurity possible. Box has a Moderate VA ATO, and an approved FedRAMP Moderate ATO. Box will not be utilizing MuleSoft to generate automatic password for shared folders.

B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

Unified Communications and Product Engineering Service

2. Information Collection and Sharing

C. *Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*

The expected number of individuals impacted is approximately 500. This environment currently has 59 Box account holders. The typical client are lawyers that represent cases on behalf of the VA. They use Box to temporarily store information related to cases.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☒	VA Employees
☒	Clinical Trainees
☒	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

D. *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 types within the IT system are names, SSN, dob, personal mailing address, financial account information, health insurance beneficiary numbers, certificates/licenses, current medications, previous medications, medical record number, personal email address, personal phone number, Retirement Disability data, Benefits management information, Labor rights management, Survivor Compensation Information, Public Resources and Infrastructure Information , Direct Transfers to Individuals, Judicial Hearings, Legal Defense Information, Legal Investigation Information, Legal Prosecution and Litigation Information, Resolution Facilitation Information, Office of Resolution Management. The purpose of collecting this information is solely for addressing business owners need for a secure tool that can collect sensitive data for research.

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

There are 2 components to the system which are Switch, Nevada-Primary and Vantage, California Alternate Data Center.

F. Are the modules/subsystems only applicable if information is shared?

Yes, the modules/subsystems are only applicable if information is shared.

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

The system is hosted on a commercial cloud. Google Cloud Platform and Amazon Web Services is the Cloud Service Provider (CSP).

3. Legal Authority and System of Record Notices (SORN)

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

VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B).

H. What is the SORN?

145VA005Q3-Department of Veterans Affairs Personnel Security File System (VAPSFS) (7/1/2022)
https://www.govinfo.gov/content/pkg/FR-2022-07-01/pdf/2022-14118.pdf

146VA005Q3/73 FR 16093 Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008)
https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pd

150VA10, Enterprise Identify and Demographics Records-VA (11/2/2023)
https://www.govinfo.gov/content/pkg/FR-2023-11-02/pdf/2023-24193.pdf

23VA10NB3, Non-VA Care (Fee) Records-VA (7/30/2015)
https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

24VA10A7, Patient Medical Records-VA (10/2/2020)
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pd

79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (12/23/2020) https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pd

121VA10, National Patient Databases-VA (4/12/2023)
https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

I. SORN revisions/modification

There are no revision/modification necessary.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

Currently, no additional amendment or revision to the system and the SORN will not require amendment or revision.

4. System Changes

J. Will the business processes change due to the information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

K. Will the technology changes impact information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

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 Information collected, used, disseminated, created, or maintained in the system.

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

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

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

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

☒ Name
☒ **Full** Social Security Number
☒ **Partial** 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[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☒ Medical Record Number
☐ Gender/Sex
☐ Integrated Control Number (ICN)
☒ Military History/Service Connection
☒ Next of Kin
☐ Date of Death
☒ Business Email Address
☐ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (list below)

Other PII/PHI data elements: • *Criminal record,* • *SEC ID (Unique identifier)*

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

1.2 List the sources of the information in the system

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

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

The information is provided directly from Veterans/ Dependents, VA Employees, VA Contractors, and Clinical Trainees.

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.

Information from other sources other than an individual is not required for Box.

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

Box does have the ability to generate a report based on user activity.

1.3 Methods of information collection

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 information is collected from individuals. The information is not collected on a form.

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?

Not applicable. The information is not collected on a Form.

1.4 Information checks for accuracy, and 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.

Box does not check for accuracy. It is the Box account holder's responsibility to determine if data is accurate prior to upload.

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?

The system does not use a commercial aggregator to check information for accuracy.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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

VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B).

145VA005Q3-Department of Veterans Affairs Personnel Security File System (VAPSFS) (7/1/2022)
https://www.govinfo.gov/content/pkg/FR-2022-07-01/pdf/2022-14118.pdf

146VA005Q3/73 FR 16093 Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008)
https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pd

150VA10, Enterprise Identify and Demographics Records-VA (11/2/2023)
https://www.govinfo.gov/content/pkg/FR-2023-11-02/pdf/2023-24193.pdf

23VA10NB3, Non-VA Care (Fee) Records-VA (7/30/2015)
https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

24VA10A7, Patient Medical Records-VA (10/2/2020)
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pd

79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (12/23/2020) https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pd

121VA10, National Patient Databases-VA (4/12/2023)
https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.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:

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

<u>Principle of Minimization:</u> The information is directly relevant and necessary to accomplish the specific purposes of the program.

<u>Principle of Individual Participation:</u> The program, to the extent possible and practical, collects information directly from the individual.

<u>Principle of Data Quality and Integrity:</u> VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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:

<u>Privacy Risk:</u> There is a risk that the information collected in the system is not accurate.

<u>Mitigation:</u> Data is collected from the individual; the individuals have opportunity to correct their information. It is the responsibility of the user to determine if data is accurate. They have the ability to remove data from Box if they believe it is not accurate, since the user is responsible for uploading data into Box.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	File Identification purposes	Not authorized for external use.
SSN	used to identify the hearing recording for purposes on transcription and ensuring accuracy.	Not authorized for external use.
DOB	Used to determine age. Will be included on certain court related documents	Not authorized for external use.
Personal mailing address	Will be used as a secondary method of contact. Will be	Not authorized for external use.

	included on certain court related documents	
Personal phone number	Will be used to contact inviduals related to court hearings.	Not authorized for external use.
Personal email address	Will be used to follow up and contact individuals associated with a court case.	Not authorized for external use.
Emergency Contact Information (Name, Phone Number, etc. of a different individual)	Will be used to reach out to list the emergency contact.	Not authorized for external use.
Financial account information	Will be used to highlight information related to financial accounts. Will be included on certain court related documents	Not authorized for external use.
Health Insurance Beneficiary Number Account Numbers	Will be used to highlight information related to health insurance beneficiary accounts.	Not authorized for external use.
Certificate/License Numbers	Will be used to highlight information related to certification and licenses.	Not authorized for external use.
Medications	Will be used to highlight information related to current prescriptions/medications.	Not authorized for external use.
Medical Records	Will be used to highlight information related to medical records.	Not authorized for external use.
Medical Record Number	Will be used to identify medical records.	Not authorized for external use.
Military History/ Service Connection	Will be used to highlight information related to military service/history.	Not authorized for external use.
Next of Kin	Will be used to identify relatives.	Not authorized for external use.
Business Email Address	Will be used as a secondary method to contact business	Not authorized for external use.
Criminal record	Will be used to highlight criminal records	Not authorized for external use.
SEC ID (Unique identifier)	Will be used to help identify/verify individual trying to sign in to Box account.	Not authorized for external use.

2.2 Describe the types of tools 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?

Box can be used to generate user activity reports.

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.

New records are created by the system after the data is altered. The user has the ability to revert the changes or addition of new records. With new information a new record is created, but the information is only accessible to individuals who have obtained a license and been provisioned at root level to have access to that folder.

2.3 How the information in the system is 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 data is protected by 256 bit encryption at rest and in transit. TLS 1.3: The standard protocol for encrypting content uploaded to Box in transit.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

The data stored at rest and in transit within Box is protected by end to end 256 Advanced Encryption Standard bit encryption.

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

Box is compliant with the OMB Memorandum. This instance of Box does not interface or share PII or PHI with an external system.

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?*

<u>Principle of Use Limitation:</u> Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

The access to PII is determined by the SSOi. Each OGC personnel/ OIT employees would need to verify their identity through PIV card to access their Box account. They would access Box by using the Box-OGC sign in page. Then they would just select continue, select PIV card option, and type in PIV pin. Box has a moderate ATO, which allows for both PII and PHI

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Yes, there are several SOPs, criteria, controls, and responsibilities are being documented and stored within Box.

2.4c Does access require manager approval?

Yes, manager approval is required. Each user would first need to be verified from the OGC point of contact to obtain a license.

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

Box system allows for PHI and PII and logins are tracked/monitored regularly.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

Information System Owner

Section 3. Retention of Information

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

3.1 What information is retained?

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

The PII/PHI that can be uploaded to Box are:

- Name
- SSN
- DOB
- Personal mailing address
- Personal phone number
- Personal email address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)

- Financial account information
- Health Insurance Beneficiary Numbers Account Numbers
- Certificate/License numbers
- Medications
- Medical Records
- Medical record number
- Military History/ Service Connection
- Next of Kin
- Business Email Address
- Criminal record
- SEC ID (Unique identifier)

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

Records received via Box are maintained for up to 14 days, program records are moved and take on the record retention of the program office. The records maintained in this system fall under transitory and Intermediary records.

3.3 The retention schedule 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. Please work with the system 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?

Yes, GENERAL RECORDS SCHEDULE 5.2

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

GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records, section 20-Intermediary records. Disposition Authority:

Temporary. Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later.

DAA-GRS-2022-0009-0002. Box Records are maintained in accordance with the General Record Schedule 5.2: Transitory and Intermediary Record

The retention scheduled has been approved by the VA. Yes, all records that are stored within the system are approved on disposition authority. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFDP records are retained according to Record Control Schedule 10-1 Section 4. (Disposition of Records). Due to OGC's unique use case, the data cannot be stored within Box for more than 14 days.

<< Box Admins can generate report on the creation, editing, and retiring of a policy (administrative actions). Admins can also report on the application of policy to files as part of an end-of-policy Disposition Action. The default retention policy for Box use within the VA is 7 years. When retention policies are configured with an end of policy Disposition Action, content is queued for deletion after its applicable retention period expires. While files identified for deletion are often deleted the same day the retention period ends, disposition timeframes may vary and cannot be guaranteed. Additionally, for enterprises with extremely large volumes of content, delays in disposition may occur in some cases. Lastly, Box Governance's disposition identification process can affect disposition timing in the following rare scenarios:

Scenario: As part of a customer sandbox experiment, you apply a retention policy of one day to a file.

Result: The disposition identification process is run on customer sandboxes daily, so the file is now eligible for deletion after one day elapses.

Scenario: Given a file that is under an Event-Based Retention (EBR) policy of three years, you set the retention start date to exactly three years ago.

Result: The disposition status will be recognized in the next disposition identification process. and the file will be eligible for immediate deletion when the process runs.

Scenario: Given a file that was uploaded to Box five years ago, you apply a retention policy of three years to the file's parent folder.

Result: The disposition status will be recognized in the next disposition identification process. and the file will be eligible for immediate deletion when the process runs.>>

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.

Users can delete retained files by sending them to Trash. However, users cannot purge files from Trash until the files' retention period has ended. Before that time, users can also restore files from Trash to their original location. If the original location has been deleted, users can choose a new folder in which to restore the files. When a file is governed by a retention policy, an indicator displays under the Details section in the righthand navigation. You also see this information by clicking the More options arrow to the right of the file name and then selecting Properties > General Info.

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.*

The system does not use PII for research, testing, or training. This system is specifically catered to OGC personnel use case. Each individual must have an OGC Box account to access the environment. They also have to verify their identity through their PIV card/pin.

Box does not directly use PII for testing new applications or information systems prior to deployment. Box serves as temporary repository for data that has both PII and PHI.

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 Privacy Officer (PO) 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: *The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

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

Follow the format below:

Privacy Risk: There is a risk that data may still be stored within Box due to user not removing data. The data may be sensitive and need to be removed as soon as possible

Mitigation: The Group Admin has the ability to remove the data on behalf of the user.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a **Box Enterprise Cloud Content Collaboration Platform-I** consists of **2** key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Box Enterprise Cloud Content Collaboration Platform-I** 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 3.9a 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**
Switch, Nevada-Primary	**Yes**	**Yes**	Name, SEC ID	Verification of user signing into Box	identity through SSOi (PIV card). Has to approved by Group Admin to obtain an account
Vantage, California Alternate Data Center	**Yes**	**Yes**	SEC ID	Verification of user signing into Box	identity through SSOi (PIV card). Has to approved by Group Admin to obtain an account

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
OGC Personnel	The purpose of information being shared is so VA OGC staff can exchange large files with other Federal Agencies, the Courts, and parties in litigation.	• Name • SSN • DOB • Personal mailing address • Personal phone number • Personal email address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Financial account information • Health Insurance Beneficiary Numbers Account Numbers • Certificate/License numbers • Medications • Medical Records • Medical record number • Military History/ Service Connection • Next of Kin • Business Email Address • Criminal record • SEC ID (Unique identifier)	Data is shared from a Veteran/ Dependent via secured email and temporarily uploaded to Box. TLS 1.3 is used to encrypt content uploaded to Box in transit

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

Privacy Risk: There is always an inherent risk that data stored within Box can be intentionally leaked (human error).

Mitigation: To mitigate this issue, Box only allows access to users who have been specifically requested by the OGC point of contact. This environment is restrictive to OGC's unique use case and only allows individuals to temporarily upload content. System admins routinely run user activity/ monitoring reports that show account logins and actions.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office	***List the purpose of information***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as:***	***List the method of transmission***

information is shared/received with	***being shared / received / transmitted***		***Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***and the measures in place to secure data***
N/A				

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.

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:

<u>Privacy Risk:</u> Not applicable. This instance of Box does not support or permit external sharing of content.

<u>Mitigation:</u> Not applicable. This instance of Box does not support or permit external sharing of content.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

Yes, notice is provided upon usage of Box. The notice is comprehensive and can be found in its entirety at https://www.box.com/legal/privacypolicy

Each SORN published in the Federal Register provides notice to individuals on the collection, purpose, use and disclosure of PII/PHI.

6.1b If notice was not provided, explain why.
Notice was provided

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.
The notice at the entry point, prior to the entering of any information, the privacy notice provides the purpose of system.

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, but no penalty is attached.

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

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.
Yes, each SORN provides individual rights as well as the Box Privacy notice. The individual does have the right to consent to certain uses of information. Please see the privacy page for information below. https://www.box.com/legal/privacypolicy.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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 Privacy Officer (PO) 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: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: *The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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: Risk that user did not thoroughly read consent notice before obtaining a Box account.

Mitigation: Box has a requirement that users read consent form before accessing the Box environment for the first time. This prevents users from accessing tool until they have agreed that they have read the terms and conditions.

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 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

The Box user uploads their own documents. If users have access to Box, they will have access to any content that they have uploaded to Box. Procedures to access individually identifiable information are addressed in the Box Privacy Policy under the Personal Information Choices section: Users can update, access, and delete account information and exercise data protection and privacy rights at any time by logging into their Box account or they can contact Box at privacy@box.com.

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)?

If customers have access to Box they will have access to any content that they have uploaded to Box. Information would be attained by veteran names, and other identifiers, so they can request through the Privacy Act Request. Under VHA, veterans can request under HIPPA.

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?

This system stores information collected from individuals. Individuals have a Box user account and upload their own documents. Users can update, delete account information, and exercise data protection and privacy rights at any time by logging into their Box account and updating their preferences or by contacting Box at privacy@box.com.

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.

Box users provide their own data/information via account creation and documentation upload. The Box privacy policy does provide a process for users to update, delete account information. Users can log into their Box account and update their preferences or can contact privacy@box.com

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.

Box users control their Box account and documents that are uploaded to their file. Box users can update, delete account information, and exercise data protection and privacy rights at any time by logging into their Box account or by contacting privacy@box.com. The Box privacy notice is comprehensive and can be found in its entirety at https://www.box.com/legal/privacypolicy.

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.

Box users control the information they store within their account. The user can directly access their account to correct/update their information at any time by logging into their Box account or by contacting privacy@box.com. The Box privacy notice is comprehensive and can be found in its entirety at https://www.box.com/legal/privacypolicy.

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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

Privacy Risk: There is Privacy Risk that individuals whose records contain incorrect information may not receive notification on how to redress or correct their information.

Mitigation: This risk is partially mitigated by the Box user being in control of the information that is uploaded to the account. Individuals can reach out to the local admin for correction purposes. Users may also go to Box's support link for assistance 24/7 to correct information. https://support.box.com/hc/en-us.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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?

To receive access to this instance of Box, an account would need to be requested from our dedicated OGC point of contact (Group Admin for OGC Box environment). Once requested, the new user will need to sign an acceptable use policy. Once the signed acceptable use policy has been received, the user will receive a link that allows them access to Box.

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?

The system is restricted for OGC personnel. The OGC personnel will have roles of Group Admin or Co-Owners. Co-Owners are provided their own folder.

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.

The role within the environment is Co-owner. The permission set described below are utilized as part of the waterfall security design. Permissions are assigned at the top and flow to folders and content down the hierarchy. Group Admins essentially have the top-level access of co-owners and can control the level of access other have within their group. Please reference this provided chart as well as this link for a more in depth look at the different permission levels.

• Co-owner – A Co-owner has all functional read/write access that an editor does. This permission level has the added ability of being able to change some advanced folder settings. Co-owners cannot change the owner of a folder.

8.2a. Will VA contractors have access to the system and the PII? VA contractors will not have direct access to the system. However, they will be referenced and included on some of the documentation that is temporarily stored.

8.2b. What involvement will contractors have with the design and maintenance of the system?

Contractors do not have any involvement with design and maintenance of the system. The system is for OGC personnel use only.

8.2c. Does the contractor have a signed confidentiality agreement?

All Box System Admins must sign a confidentially agreement, business associate agreement. And non-disclosure agreement. The contracts are reviewed annually by our Security SME, COR. and ISSO. For additional information about the roles, please see 8.1.c.

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

Contractors that have been provisioned to the external box environment and verified their identity through id.me will have access to PII related to use case and data elements. Contractors with VA emails will be able to login to the environment through SSOi. All requests will use PII and PHI need go through the process of obtaining a Data Security Categorization, where the data elements are reviewed by and ISSE team member. The contractor also must complete an Acceptable Use Policy.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?

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.

Contractors also must sign a non-disclosure agreement in place.

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

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

VA 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 must complete the following VA Training: VA Privacy and Information Security Awareness and Rules of Behavior (WBT) (VA 10176) VA Privacy and HIPPA Training (VA 10203).

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 03/06/2023
3. *The Authorization Status:* Authority to Operate (ATO)
4. *The Authorization Date:* 05/15/2023
5. *The Authorization Termination Date:* 08/28/2025
6. *The Risk Review Completion Date:* 04/27/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

Not applicable

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.* ***(Refer to question 1.8 of the PTA)***

Yes, users connect to the Box Enterprise Cloud Content Collaboration Platform using a Web Browser. No application or client is required to use Box. The connection path and mechanisms for each (Browser, Mobile Client, Sync Client or Box APIs) is the same and Box Official Applications are considered part of this Authorization boundary. Allowing users to exchange various moderate impact level information through this SaaS.

9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)* *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes, VA has ownership of VA data (including PII/PHI).

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.

No, the CSP will not collect 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.

Yes, responsibilities are described within contract language between cloud provider and organization.

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).

Not applicable- The system is not utilizing Robotics Process Animation.

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

ID	Privacy Controls
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.

JULIE DRAKE Digitally signed by JULIE DRAKE
Date: 2024.11.08 11:58:00 -07'00'

Privacy Officer, Julie Drake

ANNA JOHNSON Digitally signed by ANNA JOHNSON
Date: 2024.11.12 09:51:38 -07'00'

Information System Security Officer, Anna Johnson

KARY STORMS Digitally signed by KARY STORMS
Date: 2024.11.13 14:11:27 -05'00'

Information System Owner, Kary Storms

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).

Link to Privacy Act Notice

The Box privacy notice is comprehensive and can be found in its entirety at

https://www.box.com/legal/privacypolicy

Please see below for applicable SORNs:

145VA005Q3-Department of Veterans Affairs Personnel Security File System (VAPSFS)

(7/1/2022) https://www.federalregister.gov/documents/2022/07/01/2022-14118/privacy-act-of

1974-system-of-records

146VA005Q3-Department of Veterans Affairs Identity Management System (VAIDMS)

VA (3/26/2008)

https://www.govinfo.gov/content/pkg/FR-2008-03-25/pdf/E8-5969.pdf

150VA10 / 88 FR 75387 Enterprise Identity and Demographics Records-VA 11/2/2023

https://www.govinfo.gov/content/pkg/FR-2023-11-02/pdf/2023-24193.pdf

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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 Directive 1605.04
IB 10-163p (va.gov)