



Privacy Impact Assessment for the VA IT System called:

OGC-Box Enterprise Cloud Content Collaboration Platform

Office of General Counsel (OGC)

Date PIA submitted for review:

09/10/2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.Grewal@va.gov	202-632-7861
Information System Security Officer (ISSO)	Anna Johnson	Anna.Johnson3@va.gov	520-629-4930
Information System Owner	Herbert Ackermann	Herbert.ackermann@va.gov	202-461-0543

Abstract

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

Box is an enterprise content management platform that solves simple and complex challenges, from sharing and accessing files on mobile 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 mobile-first, cloud-first world, providing employees with secure access to content at any time using any device is critical to creating a more productive, connected workforce and improved customer experiences. Beyond secure file sharing, Box enables easy access to content and collaboration tools from any device 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 PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

**List sites here “info varies depending on documents being shared.” Internal and external sharing needs to be listed, and shared across the board. Include contract for VACO- BVA is external.

- Box Enterprise Cloud Content Collaboration Platform, will be owned by Project Special Forces (PSF). The purpose of this system is to allow collaboration between different groups within VA by providing a solution to easily share, manage and secure their content.
- The Box Enterprise Cloud Content Collaboration Platform is owned by Box, Inc and is provided to VA customers in its SaaS model. In this service delivery model, Box, Inc. is responsible for all service delivery layers, including: infrastructure; data security; and service management process. Users connect to the Box Enterprise Cloud Content Collaboration Platform using a Web Browser, Mobile Application on their Mobile Device, the Box Sync Client, custom applications or through Application Programming Interfaces (API). 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.
- The list of VA approved sites who will be using Box are the following:

1. A Office of General Counsel -- The mission of the OGC is to identify and meet the legal needs of the Department of Veterans Affairs (VA). As part of our legal representation of VA, the OGC needs to send and receive sensitive files which are too large for email. The solution will be used by VA OGC staff to exchange large files with other Federal Agencies, the Courts, and parties in litigation
 - VA site submitted an SaaS intake, and completed the SaaS Request Process, thus receiving an approval to procure, through Project Special Forces, will be able to use Box.
 - This system does use cloud technology and has a FedRAMP authorization at Moderate.
 - If privacy related data is disclosed, it should only have a moderate impact level, as only Moderate level information can pass through the system.
 - Box's key management system uses a FIPS 140-2 validated module (Cryptographic Module Validation Program CMVP #2583. <https://csrc.nist.gov/Projects/cryptographic-modulevalidation-program/Certificate/2583>. Through this FIPS 140-2 validation process Box demonstrates compliance with NIST 800-57, 'Recommendation for Key Management'. Additionally, Box leverages Amazons Key Management Service (KMS) which is FIPS 140-2 Validated (CMVP #3139) for KeySafe. Version Date: January 2, 2019 Page 5 of 31
 - The integrity impact level is based on the specific purpose to which personal identity and authentication information is put; and not on the time required to detect the modification or destruction of information. In the case of very large databases containing personal identity and authentication information relating to the general public, there is a significant probability that erroneous actions will be taken affecting benefits entitlements of or access to facilities by large numbers of individuals. In the case of benefits, this can result in at least short-term financial hardship for citizens. It can also be expected to result in very serious disruption of the agency operations due to large time and resource requirements for taking corrective actions.
 - Information that contains PII, should it become compromised, could potentially have serious impact on the reputation of the Veterans Affairs. This could also cause significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced. This could potentially also result in significant damage to organizational assets or result in significant

financial loss. The compromise of data could potentially also result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

- The Box.com SaaS solution will potentially be hosting data that will require protection at a minimum of moderate impact for availability.
- Box is FedRAMP Moderate compliant through the sponsorship of Department of Veteran Affairs. The link below where one may find this system is in compliance with FedRAMP: <https://marketplace.fedramp.gov/index.html#/product/box-enterprise-cloud-content-collaborationplatform?sort=productName&productNameSearch=box>
- All content uploaded to Box is encrypted with TLS 1.2 in transit and AES-256-bit at rest.

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 (II), 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.

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 checked="" type="checkbox"/> Name | Number, etc. of a different individual) | <input checked="" type="checkbox"/> Previous Medical Records |
| <input checked="" type="checkbox"/> Social Security Number | <input checked="" type="checkbox"/> Financial Account Information | <input type="checkbox"/> Race/Ethnicity |
| <input checked="" type="checkbox"/> Date of Birth | <input checked="" type="checkbox"/> Health Insurance Beneficiary Numbers | <input type="checkbox"/> Tax Identification Number |
| <input type="checkbox"/> Mother's Maiden Name | Account numbers | <input checked="" type="checkbox"/> Medical Record Number |
| <input checked="" type="checkbox"/> Personal Mailing Address | <input checked="" type="checkbox"/> Certificate/License numbers | <input checked="" type="checkbox"/> Other Unique Identifying Information (list below) |
| <input checked="" type="checkbox"/> Personal Phone Number(s) | <input type="checkbox"/> Vehicle License Plate Number | |
| <input checked="" type="checkbox"/> Personal Fax Number | <input type="checkbox"/> Internet Protocol (IP) Address Numbers | |
| <input checked="" type="checkbox"/> Personal Email Address | <input checked="" type="checkbox"/> Current Medications | |
| <input type="checkbox"/> Emergency Contact Information (Name, Phone | | |

- OGC —Retirement Disability data, Benefits management information, Labor rights management, Survivor Compensation Information, Public Resources and Infrastructure Information, Direct Transfers to Individuals, Judicial Hearings Information, Legal Defense Information, Legal Investigation Information, Legal Prosecution and Litigation Information, Resolution Facilitation Information Office of Resolution Management—Name, email

PII Mapping of Components

Box consists of 2 Nevada Primary and California Alternate Data Center (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Box** and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, Phone number, email address, personal address, financial account, and medical record)	Reason for Collection/ Storage of PII	Safeguards
Switch, Nevada – Primary	Yes	Yes	Name/unique identifier	Registration	Stored encrypted, subject to very strict guidelines compliant to our various government certifications like FedRAMP Moderate
Vantage, California – Alternate Data Center	Yes	Yes	Name/unique identifier	Registration	Stored encrypted, subject to very strict guidelines compliant to our various

					government certifications like FedRAMP Moderate
--	--	--	--	--	---

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

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

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

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The information obtained from Box is not collected for data aggregators or analysis.
 145VA005Q3 - Department of Veterans Affairs Personnel Security File System (VAPSFS) - VA
 146VA005Q3 - Department of Veterans Affairs Identity Management System (VAIDMS) - VA
 150VA19 - Administrative Data Repository - VA 121VA10P2 - National Patient Databases (Formerly known as 121VA19) - VA
https://www.oprm.va.gov/docs/Current_SORN_List_08_17_2021.pdf

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

HTTPS transfer (upload and download) over port 443. The information is collected from individuals, received via electronic transmission from another system, and created by the system itself.

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Name: To clarify responsible parties on a project. The purpose of name and email address being entered in Slack by the VA Account Manager is to establish a user account for accessing Slack to communicate with other users.

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

Customers can check the integrity of a file using hashes. Please see <https://developer.box.com/reference#files> for more details on checking the hash for the upload. In order to perform this check, you will need to utilize Box API to make the call for the file's hash (Sha1). Admin will verify the information is correct before individual can receive credentials to use Box.

Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a). VHA clinical operations, WRIISC (War Related Illness and Injury Study Center, Washington DC VAMC). The SSN serves to collect and verify further information on veterans from other data systems, such as CPRS (Computerized Patient Record System), Vista (Veterans Health Information System Architecture), and CDW (Corporate Data Warehouse). Privacy Act

(5 U.S.C. 552a) and in accordance with 5 U.S.C. 552a(b)(3) of the Privacy Act adding Routine Use #27. The Veteran's social security number (SSN) is used to identify the hearing recording for purposes on transcription and ensuring accuracy when returning transcribed hearings for correlation to the Veteran's appeal. The SSN is used to verify the identity of the Veteran that is requesting the hearing. The SSN is part of the Veteran information available to the Board of Veterans' Appeals under Title 38, United States Code, Section 5106. SORNs: 79VA10P2, 23VA10NB3, 121VA10P2, and 24VA10P2

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.

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: Due to the sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, personal, professional, or financial harm may result for the individuals affected.

Mitigation: The CSP will follow the FedRAMP and VA approved Incident Response Plans (IRP). This includes:

a. Preparation: Box conducts proactive investigation of potential issues, runs tabletop drills, and completes proactive identification of tooling/monitoring

b. Detection: Box NOC/Ops becomes aware of an incident and initiates the Incident Process described here. The focus during this phase is to develop a clear problem statement and engage the correct parties to work the issue.

c. Analysis: Security Incident Response, Network Operations Center (NOC), and Crisis Management Teams, work to identify the problem causing the incident and the appropriate restoration path. The focus during this phase is to identify the problem causing the incident,

identify the proper restoration path, determine if there is a security exposure resulting from the incident, and determine if there is potential data loss or corruption resulting from the incident.

d. Reporting: Box will report the Incident to the Enterprise Administrators and other designated POCs listed for that account as well as the US-CERT for civilian customers and the assigned MCND/DIBS for DoD customers.

e. Containment: Responders take action to restore service and mitigate the problem causing the incident. The focus during this phase is to restore normal operations and restore the customer experience.

f. Eradication: Responders work to address urgent problems that could allow the issue to repeat. The focus during this phase is to prevent an immediate recurrence of the issue and put emergency stop gaps in place as needed. Version Date: January 2, 2019 Page 11 of 31

g. Recovery: Normal service operation is restored and risk of recurrence is mitigated. The focus during this phase is documenting the issue, collecting forensic data for the Post Mortem, and communicating the "All Clear" to stakeholders.

h. Post-incident activities: A postmortem is an after the fact analysis of failure. The goal of a postmortem is not only to deeply understand the causes and identify the problems that lead to the incident, but also to recognize the successes that prevented an even worse reality. We believe that through thoughtful postmortem analysis we can build a better culture and process.

Once the incident is resolved, CSP will update all engaged VA stakeholders, including VA ISSO.

Section 2. Uses of the Information

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

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

Identify and list each use (both internal and external to VA) of the information collected or maintained.

This question is related to privacy control AP-2, Purpose Specification.

Identify and list each use (both internal and external to VA) of the information collected or maintained.

This question is related to privacy control AP-2, Purpose Specification.

Name and VA email are used to appropriate accounts for use, and as an identifier. Social Security Number is used to identify the hearing recording for purposes on transcription and ensuring accuracy. The last four digits may show in payroll records. SSN, may also be

collected for quality improvement projects where Electronic Health Record reviews are required to facilitate and monitor quality improvement efforts.

Date of Birth may be included in a file.

Personal Mailing Address may be included in a file in a general manner.

Personal Phone Number(s) may be used for identifying and contacting user(s)

Personal Fax Number may be used for contacting user(s)

Personal Email Address may be used to verify user(s) and as primary contact info.

Financial Account Information – Financial status information, but no bank account numbers or the like, discussed within the case documentation.

Health Insurance Beneficiary Numbers is used to directly identify the Veteran and/or Veteran's representative appealing the case

Certificate/License numbers may be used for identifying purposes

Current Medications is used to directly identify the Veteran and/or Veteran's representative appealing the case. It is within their medical records and discussed as part of the case file.

Previous Medical Records is used to directly identify the Veteran and/or Veteran's representative appealing the case

Medical Record Number is used to directly identify the Veteran and/or Veteran's representative appealing the case. Part of the file and a search field.

Other Unique Identifying Number (list below) – Yes, their VA-assigned number if they don't have a social security number, used as an identifier and as a search parameter.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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

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

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

Box does not use any tools to analyze data.

2.3 How is the information in the system secured?

Data within the system is encrypted.

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

The data is protected by encryption

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

The SSN are encrypted

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

Principle of Transparency: *Is the PIA and SORN, if applicable, clear about the uses of the information?*

Principle of Use Limitation: *Is the use of information contained in the system relevant to the mission of the project?*

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Add answer here:

VA users of Box.com do not have access to information about other users other than name and role. VA Account Admins have access to name and email address in order to provision and manage accounts according to VA Enterprise Box.com Onboarding Procedures and at the direction of user managers. A unique identifier is used for SSO is not accessible to other users or VA Account Admins. Box.com and the VA are responsible for safeguarding PII, depending on how the responsibility for a given security control has been assigned in the VA GRC tool.

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

VA can set their own retention on documentation- Retention Policies are available through the Governance feature.

If Governance Retention Policies are not enabled Content is retained on our servers until a customer either a) permanently deletes it or b) cancels their account. When either of these happen the content (primary and backup copies), the corresponding metadata (such as comments), and the associated data encryption keys are deleted. The length of retention post contract termination is dependent on the agreement between the customer and Box.

Upon termination or expiration of the Agreement, and subject to the Customer's prior written request, Box will grant Customer's Administrator limited access to the Box Service solely for purposes of Customer's retrieval of the Content for up to 30 days (dependent on contract terms) following the expiration or the termination of the Agreement and/or applicable Subscription Period.

For specific details around the timeline for deletion of Content, Box can provide a deletion whitepaper upon request.

Box Sales info that contains PII- so e.g. emails to set up meeting invites for contract reviews

Box will retain personal information for the period necessary to fulfill the legitimate business purposes outlined in our Privacy Notice. Please refer to Box's Privacy Notice for further details: <https://www.box.com/legal/privacypolicy>

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. This question is related to privacy control DM-2, Data Retention and Disposal.

If Governance Retention Policies are not enabled Content is retained on Box servers until a customer either a) permanently deletes it or b) cancels their account. When either of these

happen the content (primary and backup copies), the corresponding metadata (such as comments), and the associated data encryption keys are deleted. The length of retention post contract termination is dependent on the agreement between the customer and Box.

Upon termination or expiration of the Agreement, and subject to the Customer's prior written request, Box will grant Customer's Administrator limited access to the Box Service solely for purposes of Customer's retrieval of the Content for up to 30 days (dependent on contract terms) following the expiration or the termination of the Agreement and/or applicable Subscription Period.

For specific details around the timeline for deletion of Content, Box can provide a deletion whitepaper upon request.

Box Sales info that contains PII- so e.g. emails to set up meeting invites for contract reviews Box will retain personal information for the period necessary to fulfill the legitimate business purposes outlined in our Privacy Notice. Please refer to Box's Privacy Notice for further details: <https://www.box.com/legal/privacypolicy>

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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

If Governance Retention Policies are not enabled Content is retained on Box servers until a customer either a) permanently deletes it or b) cancels their account. When either of these happen the content (primary and backup copies), the corresponding metadata (such as comments), and the associated data encryption keys are deleted. The length of retention post contract termination is dependent on the agreement between the customer and Box.

The retention has been approved by the National Archives and Records Administration (NARA). The guidance for retention of records is found in the RCS 10-1, and the National Archives and Records Administration. The RCS 10-1 can be found at: <https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf>

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?

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

Box will follow electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA Handbook 6500 Electronic Media Sanitization.

According to VA Handbook 6500, once records are entered into the system they remain as part of the protected system information. System logs are maintained for one year and then flagged for deletion by their automated processes. System logs are not retained after one year and any SPI containing them will be overwritten as part of the process for audit management. When virtual machines are no longer required to support the system they are wiped clean and the data overwritten.

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014),

https://www.va.gov/digitalstrategy/docs/VA_Directive_6500_24_Jan_2019.pdf

In addition, any equipment that is decommissioned and is leaving the controlled data center will be sanitized (e.g., degaussing) or destroyed in accordance with VA Handbook 6500 and the Veterans Affairs Dedicated Cloud Media Sanitization Procedure. VA Dedicated Cloud Media Sanitization policy outlines the VA Dedicated Cloud policy and procedure for tracking, documentation and disposal of storage media within the environment and their return to the VA, in accordance with VA Handbook 6500.

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

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

Box will not be using PII for research testing or training however we have security controls in place to minimize risk related to security. All content uploaded to Box is encrypted. However, Box monitors the success/failure of events through logs and tools to enable and improve their product.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that PII gets released outside of specified purpose.

Mitigation: Box will not be using PII for research testing or training however they have security controls in place to minimize risk related to security. All content uploaded to Box is encrypted. However, Box monitors the success/failure of events through logs and tools to enable and improve our product.

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 3.10 (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

<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 shared/received with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

Section 5. External Sharing/Receiving and Disclosure

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

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

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

NOTE: Question 3.11 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 shared/received 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>

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

Box does not interface or share PII or PHI with an external system.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

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

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

Section 6. Notice

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

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

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

145VA005Q3 - Department of Veterans Affairs Personnel Security File System (VAPSFS) - VA
146VA005Q3 - Department of Veterans Affairs Identity Management System (VAIDMS) - VA
150VA19 - Administrative Data Repository - VA 121VA10P2 - National Patient Databases
(Formerly known as 121VA19) - VA
https://www.oprm.va.gov/docs/Current_SORN_List_08_17_2021.pdf

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 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*

Individuals would need to read the PIA for the system that stored the information at the time of collection to determine whether they have a right to consent to uses of the information.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

Privacy Risk: Risk that individual is unaware that their information is being collected by the system.

Mitigation: Box is only being used for individuals to file share. User information will not be collected or stored by Box.

Section 7. Access, Redress, and Correction

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

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

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

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

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

This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

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.

7.2 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.

Veterans Health Administration (VHA) Directive 2012-036, Identity Authentication for Health Care Services, provides policy and procedures to authenticate the identity of individuals requesting VA medical care, treatment, or services in person and provides administrative correction procedures to correct information previously captured by, or in, error. AUTHORITY: Privacy Act of 1974, Title 5 United States Code (U.S.C.) 552a, Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, Title 45 Code of Federal Regulations (CFR) Part 160 and 164.

The VA website provide numerous avenues that notify individuals of the procedures for updating their information. Individuals seeking to make changes to their records may use VA Form 10-10EZ, Instructions for Completing Health Benefits Update Form. Individuals wishing to obtain more information about access, redress and record correction of the Master Patient Index, should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) "National Patient Databases-VA" 121VA10P2. This SORN can be found online at: https://www.oprm.va.gov/docs/Current_SORN_List_08_17_2021.pdf

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

The VA, Veterans Service Organizations, and other Veteran advocate organizations also support the education of and notification process for Veterans. Individuals wishing to obtain more information about access, redress and record correction of the Master Patient Index, should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) "National Patient Databases-VA" 121VA10P2. This SORN can be found online at: https://www.oprm.va.gov/docs/CurrentSORNList_7_24_20.pdf 145VA005Q3 146VA005Q3 150VA19 121VA10P2

For further information on the listed SORNs please visit link:
https://www.oprm.va.gov/privacy/systems_of_records.aspx

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.

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

Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.

This applies to limited subset of VA users because Box does not collect PII on all customers typically only for the purpose of the sale and to keep in contact regarding product updates, etc.

Yes, Box is able to comply with the requirements applicable to Box, including providing the relevant personal data as requested in a data subject access request (DSAR) in 30 days. Additionally, customers using the Box Cloud Content Management platform are responsible for Version Date: January 2, 2019 Page 24 of 31 fulfilling their own FOIA/DSAR requirements, such as determining the appropriate retention periods of personal data as well as identifying the content stored which contains personal data.

Redress is also provided through VA policy. VA Handbook 6300.4-Procedures for Processing Requests for Records Subject to the Privacy Act.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.

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

Principle of Individual Participation: *Is the individual provided with the ability to find out whether a project maintains a record relating to him?*

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

This question is related to privacy control IP-3, Redress.

Follow the format below:

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

Mitigation: Individuals are immediately able to 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.

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

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

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

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

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Individuals receive access to the Box system by being awarded an approval from Project Special Forces (PSF) that then provides access to Box system upon contract and training. Upon contract, PSF opens network access accounts as determined by information submitted during SaaS intake process and Critical Decision 1. Veterans Health Administration (VHA) Supervisors are required to review and approve an individual's initial and additional requests for access. Approval process is documented and maintained by PSF and the Information Security Officer (ISO). PTA and PIA will be updated to reflect any added sites or changes to use case.

Furthermore, Box will be using 2-FA authentication mechanism to allow users internal to the VA to access the system (e.g., using Personal Identity Verification PIV). Server-level access will be

Version Date: May 1, 2021

Page 23 of 31

managed and granted to users on an as-needed basis through approved processes using established VA OIT Systems.

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.

Yes, the target user population for Box is any system user accessing a secured VA application available on the public Internet, potentially the entire Veteran population, their dependents, VA's customers and business partners including but not limited to contractors and other users to the information system.

Contractors are required to complete the same provisioning, onboarding and training requirements as all VA users prior to access to VA Information Systems. VA COR review and manage contracts and non-disclosure agreements approved by VA. The COR oversees the contracts awarded to contract personnel. No Contractor access to information system is granted without VA COR approval.

No contractor, volunteer, or employee has any access to VA information systems and PII until they have been fully on boarded. Contractors as well as VA employees receive annual training regarding their roles on the system and sign a "Rules of Behavior for EP" that prevents VA contractors from using PII in any manner not consistent with business needs. Administrators ensure screening is conducted for all contract personnel and federal employees and all other appointed workforce members. The onboarding process consists of screening, as defined by VA Directive and Handbook 0710 Personnel Suitability and Security Program, of federal employees and contract personnel who participate in the design, development, operation, or maintenance of sensitive applications and sensitive systems, as well as those individuals having access to VA sensitive information or information is required.

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 of the Box system are required to complete annual Privacy Security Training, as well as VA Rules of Behavior training and VA mandated privacy HIPAA training

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date, .*
6. *The Risk Review Completion Date*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

Box was able to obtain a full ATO. This system ATO will go through 06/25/2023. The FIPS 199 Classification of the system is Moderate.

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, 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.

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Yes, users connect to the Box Enterprise Cloud Content Collaboration Platform using a Web Browser, Mobile Application on their Mobile Device, the Box Sync Client, custom applications or through Application Programming Interfaces (API). 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 Identify the cloud model being utilized.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Software as a Service (SaaS)

9.3 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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Box.com and the VA are responsible for safeguarding PII, depending on how the responsibility for a given security control has been assigned in the VA GRC tool.

9.4 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.

9.5 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. The onboarding process consists of screening, as defined by VA Directive and Handbook 0710 Personnel Suitability and Security Program, of federal employees and contract personnel who participate in the design, development, operation, or maintenance of sensitive applications and sensitive systems, as well as those individuals having access to VA sensitive information or information is required.

9.6 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).

Box is not using RPA. Box is currently utilizing box relay, which uses automation to trigger specific actions.

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Privacy Officer, Rita Grewal

Information Systems Security Officer, Anna Johnson

System Owner, Herbert Ackermann

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). [Link for Privacy Act Notice](#)