SPLASH PAGE LANGUAGE

The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements
under the Federal Information Security Management Act (FISMA).

VA HANDBOOK 6508: "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 2014, http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=767&FType=2

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Privacy Impact Assessment for the VA IT System called:

DOCUSIGN CONTRACT LIFECYCLE MANAGEMENT (CLM)

ENTERPRISE PROGRAM MANAGEMENT OFFICE (EPMO)

Date PIA submitted for review:

MARCH 24, 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)	Thomas J. Orler	Thomas.Orler@va.gov	708-938-1247
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595-7291

Abstract

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

DocuSign Contract Lifecycle Management (CLM) (hereafter referred to as "DocuSign CLM") is business process automation software delivered through a cloud platform. DocuSign CLM can manage metadata, unstructured content, routine business documents such as Microsoft Office content, and workflow processes. DocuSign CLM is a FedRAMP-approved system hosted by Equinix and Switch Communications Group's SUPERNAP in secure, state-of-the-art data centers in the Chicago, Ashburn, and Las Vegas metropolitan areas.

DocuSign CLM serves as a document repository for two Salesforce Development Platform (SFDP) modules: (1) Government Accountability Office (GAO) Module and Veterans Health Administration (VHA) Integrity.

For the GAO Module, DocuSign CLM also serves as a workflow automation tool for processing files in the document repository. Data transmitted to or from DocuSign CLM includes the folder location information and the files (document attachments) contained therein. These files can contain any and all types of data, including Personally Identifiable Information (PII).

The GAO Module is used to manage VA's response to inquiries from the General Accountability Office. This is done by assigning subject matter experts to provide information, obtaining the needed information, and submitting the requested information in the form of a final report to the GAO. The final report and the other artifacts that are necessary to support the response to the GAO inquiry are created and sourced from outside of the system and are uploaded to the DocuSign CLM repository for storage. All GAO Module users have access to DocuSign CLM. However, access to specific files in the repository may be limited, depending on the user's role or access permissions on the case.

Overview

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

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

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

The subject of this Privacy Impact Assessment is the product named DocuSign Contract Lifecycle Management which is also referred to as DocuSign CLM. The Enterprise Program Management Office (EPMO), Project Special Forces (PSF) organization is the DocuSign CLM system owner. This product is a GAO Module sub-system. The GAO Module is classified as a Support System and which is recorded in the VA System Inventory (VASI) as system number 2623. It is used primarily at the VA Central Office (VACO), several VA Program Offices, and by the Office of Congressional and Legislative Affairs (OCLA). It is not used by any region, hospital, or medical center.

The Office of Congressional and Legislative Affairs (OCLA) uses the GAO Module to processes GAO-originated inquiries by identifying the subject matter experts, obtaining the requested information, and submitting a final report to GAO. This requires tracking GAO correspondence, data requests, reports and recommendations. The DocuSign CLM product enabled within the GAO Module provides the document repository, document versioning, security and workflow capabilities to manage artifacts, data files, and business process documents in support of OCLA's response to GAO inquiries.

The U.S. Government Accountability Office is an independent, nonpartisan agency that examines how taxpayer dollars are spent and provides Congress, the public, and federal agencies with objective, reliable information to help the government save money and work more efficiently. GAO evaluations, audits, investigations, and analyses are done at the request of congressional committees or subcommittees or is statutorily required by public laws or committee reports, per GAO's Congressional Protocols (GAO-17-767G). The VA's OCLA is the lead office with statutory responsibility for Department management and coordination of all matters involving Congress, including GAO inquiries (U.S.C. Title 38 Part I Chapter 3).

DocuSign CLM stores information on Veterans and other persons only if they are persons who are the subject of, or associated with, a GAO audit, investigation or request for information. Consequently, there is no 'typical client or affected individual'.

Documents stored in the DocuSign CLM system support the following business processes in response to GAO requests: Request for Information, Response, Concurrence, Edits, Review,

Signature, Actions, and Case Closure. Related artifacts stored in DocuSign CLM include the following: Notification Letter, Entrance Conference, Data Requests, Statement of Facts, Exit Conference, Draft and Final Reports, Recommendation Updates, Interim Briefings, and Hearing Preparation. The GAO Module may share documents and files within DocuSign CLM using Case Task functionality. However, this sharing is only among licensed users and is not shared outside the system.
DocuSign-CLM is operated at VACO in several Washington, DC locations. System users may also log in remotely. PII is managed identically at all locations by user controls built into the system. All users are required to participate in Cybersecurity and Privacy training and to sign 'Rules of Behavior' and to complete GAO Module training before gaining access to the system. DocuSign employees and contractors are not granted access to the data.
The DocuSign CLM product is a Salesforce Cloud App Exchange product (eMASS System ID# 980) and is FedRAMP Authorized. DocuSign CLM (F1605027893) has an agency authorization date of 05/27/2020. The FIPS 199 classification is Moderate and Authority to Operate was granted on November 19, 2020 and expires May 18, 2021.
The DocuSign CLM contract establishes that all content, including PII stored in the Salesforce cloud is owned by the VA. In order to clearly identify the organization that is accountable to protect the data, the DocuSign CLM contract identifies the VA the organization that is ultimately accountable for the security and privacy of the data held in DocuSign CLM.
Completion of this PIA is not expected to require changes to the technology or business process.
If privacy related data is disclosed, intentionally or unintentionally, VA would incur significant harm to its reputation and those responsible may be held responsible with potential civil or criminal liabilities. In addition, VA could be compelled to provide credit monitoring services and other compensation to any customers who were thus harmed. Depending on the circumstances and root cause of a privacy disclosure incident, the Cloud Service Provider's reputation could be substantially impacted.

Section 1. Characterization of the Information

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

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

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

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

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

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

GAO inquires may include sensitive data in documents or files that are uploaded to DocuSign CLM. Documents containing certain kinds of sensitive data are stored in specially configured secure folders.
Because DocuSign CLM serves as a file management system to the GAO Module, it will house all attachments required to respond to the GAO inquiry and consequently can contain PII from the various program offices. These attachments will contain detailed information for the GAO cases and the parties involved, including names, work addresses, work emails, work phone numbers and anything else that might be related to the case. Other examples of potential data could include health records and pharmacy pricing data, depending on the nature of the inquiry.

PII Mapping of Components

DocuSign CLM consists of five key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by DocuSign CLM and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Swift API	No	Yes	Potentially all PII listed above	No personal data is collected directly from	All seven safeguards listed

				individuals. Information in documents loaded to DocuSign CLM may contain PII which was gathered by system users from other systems.	immediately following this table are environment level controls and apply to each of the 5 components in this table.
Network Attached Storage (NAS)	No	No	Not applicable. No VA data is stored on this component. It is not a Privacy sensitive component.	No personal data is collected directly from individuals. Information in documents loaded to DocuSign CLM may contain PII which was gathered by system users from other systems.	All seven safeguards listed immediately following this table are environment level controls and apply to each of the 5 components in this table.
SQL Server	No	Yes	Potentially all PII listed above	No personal data is collected directly from individuals. Information in documents loaded to DocuSign CLM may contain PII which was gathered by system users from other systems.	All seven safeguards listed immediately following this table are environment level controls and apply to each of the 5 components in this table.
Apache Cassandra	No	Yes	Potentially all PII listed above	No personal data is collected directly from individuals. Information in documents loaded to DocuSign CLM	All seven safeguards listed immediately following this table are environment level controls

				may contain PII which was gathered by system users from other systems.	and apply to each of the 5 components in this table.
ElasticSearch API	No	Yes	Potentially all PII listed above	No personal data is collected directly from individuals. Information in documents loaded to DocuSign CLM may contain PII which was gathered by system users from other systems.	All seven safeguards listed immediately following this table are environment level controls and apply to each of the 5 components in this table.

Safeguards: All safeguards detailed as follows are environmental level safeguards and apply to each of the components defined in the table above:

1. Transport Layer Security (TLS) with FIPS 140-2 compliant encryption for data in transit.
2. AES-256 cryptographic keys are generated using SQL Server and Cassandra Transparent Data Encryption (TDE) to encrypt information at rest.
3. Administrative access via IPsec or SSL VPN tunnel using Duo or Google authenticator soft tokens to accomplish multi-factor authentication.
4. AlienVault Unified Security Management (USM), which includes security information and event management (SIEM) tools and intrusion detection and prevention capabilities
5. Palo Alto Networks software running on Layer 7 next-generation firewalls.
6. Nessus and BurpSuite vulnerability and compliance scanning software.
7. Zabbix software used for network monitoring and alerting regarding server and application availability and capacity.

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.

In response to a GAO investigation, request for information, or other correspondence, VA Program Offices may store sensitive information in the form of documents or standard office productivity files or as text-based data. This data may be sourced from any other systems such as SharePoint or office productivity software throughout the VA. Information collected may be shared with the GAO, but this is accomplished outside the system. There are no GAO agency users of the DocuSign CLM system.
The information stored in DocuSign CLM comes from OCLA and VA program office users. There is no information collected directly from an individual. This system is a document repository and does not create any type of information including any scores, analysis or reports.

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.

Information is collected through standard office software and is uploaded into DocuSign CLM by GAO Module users. No information in the system is transmitted electronically from another system or to another system. And no information is collected on a paper form to populate DocuSign CLM.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose.
This question is related to privacy control AP-2, Purpose Specification.

Sensitive Personal Information is collected only if required in response to a GAO investigation, audit, or request for information. DocuSign CLM is used as a document repository, and documents may be retrieved by licensed users of the GAO Module.
DocuSign CLM does not collect any commercial data, however, in response to a GAO investigation, audit, or request for information, a user may upload commercial data into the system. DocuSign CLM is used as a document repository, and documents may be retrieved via the GAO Module.

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

The information stored in DocuSign CLM may be checked for accuracy by the systems or users from which the information was originally sourced. The information is not checked for accuracy at the time of uploading to DocuSign CLM, unless end users do so prior to uploading.

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

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

1. 5 U.S.C. § 552a - Records maintained on individuals No. 104---231, 110 Stat. 3048
2. Public Law 100--503, Computer Matching and Privacy Act of 1988
3. E---Government Act of 2002 § 208
4. Federal Trade Commission Act § 5
5. 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33
6. Title 35, Code of Federal Regulations, Chapter XII, Subchapter B

7. OMB Circular A---130, Management of Federal Information Resources, 1996
8. OMB Memo M---10---23, Guidance for Agency Use of Third---Party Websites
9. OMB Memo M---99---18, Privacy Policies on Federal Web Sites
10. OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions
11. OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
12. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
13. Various state privacy laws
14. SORN: 75VA001B -Department of Veteran's Affairs Secretary's Official Correspondence Records-VA (expired but an update is in progress during Q2-Q3 2021)

The legal authority is 38 U.S.C. 7601-7604 and U.S.C 7681-7683 and Executive Order 9397

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:
Privacy Risk: Sensitive Personal Information (SPI) including any type of personal contact information, SSN and medical information may be released to unauthorized individuals.

Mitigation: Profile based permissions govern what users have access to. The profiles are reviewed on a regular basis to ensure that appropriate information is shared with appropriate users. All employees with access to Veteran's information are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior annually. All VA, VHA staff, business associates, affiliates and business partners who have, or will request access to electronic protected health information (EPHI) must complete all the VA's annual security,

privacy, and HIPAA privacy related awareness courses as required by Department and VHA policies.
Access to the Document Management Portion of GAO containing sensitive information is controlled by OCLA. Only case team members are permitted to view or add sensitive content and OCLA strictly controls who is added to the case team, providing access on a need to know basis. Existing case team members are permitted to add another case team member. Furthermore, visibility to secure content is limited. Only the office that uploaded the sensitive information can view it. No office has access to another office's sensitive information. The only exception to this rule is OCLA which oversees the case and the Office of the Executive Secretary which provides additional oversight. Both of these offices can see all sensitive information that has been uploaded into the GAO Module. However, one must be provisioned as a GOA Module user to view system content if not a case team member.

Privacy Risk: Data breach at the facilities level.

Mitigation: To ensure the utmost privacy and security at the facility level, authorized personnel must pass through multiple levels of biometric and/or badge scanning to reach the Salesforce system rooms/cages. All buildings are completely anonymous, with bullet resistant exterior walls and embassy grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of a suspected intrusion. Data is backed up. Backups do not physically leave the data center.

Privacy Risk: Data breach at the network level.

Mitigation: Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only https traffic on specific ports, along with Internet Control Message Protocol (ICMP) traffic. Switches ensure that the network complies with the Request for Comment (RFC) 1918 standard, and address translation technologies further enhance network security. Intrusion Detection Sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry.

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.

The Office for Congressional and Legislative Affairs serves as the Department of Veteran's Affairs liaison with the Government Accountability Office (GAO). OCLA's use of DocuSign CLM is to store and manage artifacts and business process documents in response to GAO investigations and audits within the Government Accountability Office (GAO) Module. The GAO Module is used to track GAO correspondence, investigation artifacts, data requests, reports and recommendations.

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

Data analysis and data processing is not performed by the DocuSign CLM system on any of the document content stored in DocuSign CLM.

2.3 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> 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. <u>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.</u>

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

<u>Principle of Transparency:</u> 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.

Controls have been implemented to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data, including mandatory training completion for all employees, volunteers, and contractors. These include acknowledgement of the Rules of Behavior by all users; and drive encryption or Transparent Data Encryption (TDE). All DocuSign CLM data is encrypted in transit and at rest. User access is controlled through the GAO Module.
All changes to documents in the DocuSign CLM repository are logged. The system does not log changes to the actual content within the documents. Log functionality tracks actions on the document such as whether a new version of a document has been uploaded. It is not possible for DocuSign CLM to be aware of precisely what was edited in any document since that data is contained in the document itself, which is encrypted and under the control of the VA. Logs merely contain metadata about an action on the document. DocuSign CLM does not collect a customer's document data and does not store sensitive document data outside of the document itself. The VA owns and controls the data within the documents. The contract between the VA and DocuSign (Contract Number NNG15SD37B) requires that DocuSign abide by VA data security and privacy rules.
Users must complete instructor led, web-based GAO Module training. Users must provide their certificate of VIEWS training completion to their assigned VIEWS Office Coordinator (VOC) member. Once your VIEWS training certificate is provided a user can be provisioned to enable login and access the GAO Module. Inactive user accounts are deactivated after 90 days.
DocuSign CLM applies the same safeguards to documents regardless of whether or not the documents contain PII. Consequently, control over PII access is managed within the GAO Module using secure folders. A user must be on a case team to access PII. If not on a case team, users wouldn't know that PII exists in a document or have access. When a user wants to upload PII, they must create a secure folder which is only visible to the office of the user that owns the case. Only members of the same office or case team can see the case associated secure folders. However, OCLA and the Executive Secretariat (ExecSec) acting in oversight capacity has oversight of all case documents, regardless of case or PII contents.
DocuSign is contractually responsible for safeguarding PII and their staff may only gain access to a document at the request of the VA to troubleshoot an issue.
The GAO Module User Guide details access controls to secure folders in DocuSign CLM. DocuSign CLM users have the ability see who has access to secure folders. DocuSign CLM inherently tracks actions in the documents and can also produce audit logs on request that satisfy FedRAMP Web App requirements including: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.
To ensure that information is handled in accordance with the uses described above, users can not email documents containing PII directly from a module or assign them to a case task. Email and case task functionality do not display secure folder contents.
With cases containing sensitive but not classified information, no documents are visible to anyone unless they are on the respective case team that is responsible for the GAO inquiry. Then, access is limited to the entire case, not just on a folder-by-folder basis. Sensitive but not

classified content depends on the use case and could contain PII but does not necessarily. OCLA and the Executive Secretariat acting in oversight roles have unlimited access to sensitive but not classified folders.
User access audits are performed to ensure information is accessed and retrieved appropriately. Before new accounts are added to the GAO Module, they must be approved by a GAO Module manager. The VA and Salesforce have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the Acting Assistant Secretary for Information Technology [the VA Authorizing Official].
Salesforce's Master Subscription Agreement also addresses the protection of Customer Data. A sample Master Subscription Agreement can be viewed here:
http://www.salesforce.com/assets/pdf/misc/salesforce_MSA.pdf .

In addition to the Master Subscription Agreement, Salesforce has documented a System Security Plan that identifies the security controls that salesforce has documented to protect the environment in which Customer Data is stored. Additionally, their privacy and security statements can be viewed here:
http://www.salesforce.com/company/privacy.

Salesforce has a Global Privacy Team who oversees privacy for salesforce. Protecting the security and privacy of user data is a shared responsibility between Salesforce and VA that provision user accounts (See VA118-16-F-1530).

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

Depending on the type of document that is being uploaded, any type of PII/PHI may be included: Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address Personal Phone Number(s), Personal Fax Number , Personal Email Address, Emergency Contact Information (Name, Phone Number, etc. of a different individual), Financial Account Information, Health Insurance Beneficiary Numbers, Account numbers, Certificate/License numbers, Vehicle License Plate Number, Internet Protocol (IP) Address Numbers, Current Medications, Previous Medical Record, Race/Ethnicity, Tax Identification Number, Medical Record Number, or other Unique Identifying Numbers.

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.

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

All of the information that is collected in DocuSign CLM will be retained throughout the lifecycle of the GAO investigation.
The DocuSign CLM system does not create documents. The documents that are loaded into DocuSign CLM are sourced from other systems and fall outside definition of a record as specified in Title 44, Section 3301, of the United States (U.S.) Code. The documents loaded to DocuSign CLM are copies and therefore are regarded to be non-record materials. The documents may be disposed of as soon as the final report responding to the GAO inquiry is delivered to GAO. However, the documents will not be kept beyond the disposition period. It is the responsibility of the OCLA Records Steward to determine at what point in time within the disposition period, the documents stored in the system will be destroyed. The disposition period depends on the contents of each document.

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.

The GAO Module complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the Salesforce FedRAMP cloud will be retained as long as the information is needed in accordance with a NARA-approved retention period. 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).
The determination of VA Records Office is that the documents that are uploaded to the DocuSign CLM system are copies and therefore are non-record material. However, the documents will not be kept beyond the disposition date. It is the responsibility of the OCLA Records Steward to determine at what point in time prior to the disposition date, the documents

stored in the system will be destroyed. The disposition date depends on the contents of each document.

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

The OCLA sets the disposition date for documents stored in DocuSign CLM. The OCLA stores SPI in secure folders within the DocuSign CLM repository and will dispose of DocuSign content on a case-by-case basis, according to the disposition date specified.
All documents are uniquely associated with the GAO Module user accounts and are deleted across all storage nodes in compliance with the disposition date. DocuSign CLM leverages Iron Mountain or equivalent asset destruction services for the disposal of retired hard drives. DocuSign CLM adheres to NIST 800-88 for all sanitization of media. DocuSign is not retaining information. The systems using DocuSign 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.

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

PII data is only stored on the production, production mirror and staging environments. Access to these systems is protected using the Single Sign On (SSO) technology to verify the user and provides access only to data based on permissions set up for that user. All other environments, including the development and training environments, use lower level environments that do not host PII data.

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

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

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains

information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

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: The risk to maintaining data within the GAO Module is that longer retention times increase the risk that information may be compromised or breached.

Mitigation: To mitigate the risk posed by information retention, the OCLA may dispose of the non-record content as soon as the final report is delivered to GAO. Any documents that contain SPI are easily identified and are stored in secure folders. It is the responsibility of the OCLA Records Steward to determine at what point in time prior to the disposition date, the documents stored in the system will be destroyed. The disposition date depends on the contents of each document. The OCLA Records Steward will dispose of the data by the determined method as described in question 3.4. All electronic storage media used to store, process, or access DocuSign CLM records will be disposed of in adherence with the latest version of VA Handbook 6500.1, Electronic Media Sanitization.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Active Directory Federated Service (ADFS)	Validate the user	The ADFS servers pass a token to the SFDP that validates a VA internal user, via their federated ID, as a current credentialed user of VA systems.	Access credentials via login credentials along with integrating with the PIV card and eToken security FOB's.
VA - Office of Legislative Affairs (OCLA)	Internal use: Coordination of collection and approval of data to be shared with GAO	Names, emails, phone numbers, offices of those that are part of the case team and any type of PII including: Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address Personal Phone Number(s), Personal Fax Number , Personal Email Address, Emergency Contact Information (Name, Phone Number, etc. of a	Viewable in GAO Module Two-way secure socket layer / Transport layer Security (SSL/TLS) encryption. The data from Salesforce traverses through the Equinix (TIC) gateway to VA Salesforce Development Platform (SFDP)

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
		different individual), Financial Account Information, Health Insurance Beneficiary Numbers, Account numbers, Certificate/License numbers, Vehicle License Plate Number, Internet Protocol (IP) Address Numbers, Current Medications, Previous Medical Record, Race/Ethnicity, Tax Identification Number, Medical Record Number, Other Unique Identifying Numbers..	
Executive Secretary's office (ExecSec)	Internal use: Approval, concurrence of data to be shared with GAO	Any type of PII to include: Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Phone Number(s), Personal Fax Number1 Personal Email Address, Emergency Contact Information (Name, Phone Number, etc. of a different individual), Financial Account Information, Health Insurance Beneficiary Numbers	Viewable in GAO Module

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
		Account numbers, Certificate/License numbers, Vehicle License Plate Number, Internet Protocol (IP) Address Numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Tax Identification Number, Medical Record Number, Other Unique Identifying Number (list below) that is required to respond to a GAO investigation, request for information, or audit **Note**: PII is not stored in fields in the system but rather may be included with any attachments of documents, data, or other related files.	
Any VA Program Office relevant to GAO investigation or request	Internal use: Coordination of collection of data to be shared with GAO	Any type of PII to include: Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Phone Number(s), Personal Fax Number1 Personal Email Address, Emergency	Viewable in GAO Module

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
		Contact Information (Name, Phone Number, etc. of a different individual), Financial Account Information, Health Insurance Beneficiary Numbers Account numbers, Certificate/License numbers, Vehicle License Plate Number, Internet Protocol (IP) Address Numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Tax Identification Number, Medical Record Number, Other Unique Identifying Number (list below) that is required to respond to a GAO investigation, request for information, or audit **Note**: PII is not stored in fields in the system but rather may be included with any attachments of documents, data, or other related files.	

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: There is a risk that information may be shared with unauthorized VA personnel.

Mitigation: Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized for the system.
The document management functionality has a secure folder feature to ensure that data is not shared inappropriately outside of case teams and across other program offices within the VA.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

Note: This question is #7 in the Privacy Threshold Analysis.

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

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

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

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

Data Shared with External Organizations

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

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

No specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16. However, remote users must connect to the VA network and use a Personal Identity Verification (PIV) to access system content. A timeout policy applies to all users, whether remote or not as a platform level setting. The standard timeout is 15 minutes but can vary depending on the organization users are associated with.
The metadata logging of actions on DocuSign CLM as detailed in Section 2.3 occur whether a user is remote or not.

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: There is no data being shared outside of the Department. If there is data being shared outside of the department in the future access controls will be implemented based on MOUs, contracts or agreements. If data was maintained outside of the Department, there is a risk that information may be accessed by an external organization or agency that does not have a need or legal authority to access VA data.

Mitigation: VA has contracted Salesforce Inc. to deliver services that include maintaining VA data. A contract is in place that clearly articulates Salesforce's roles and responsibilities. Authorized Salesforce personnel access data on users to provision and provide the Salesforce service. Access is controlled by authentication and is restricted to authorized individuals. Salesforce's security policies address the required security controls that must be followed in order to protect PII. Salesforce Development Platform Assessing will be connected to Equinix for data transfer purposes. Equinix will provide details of the security event, the potential risk to VA owned sensitive information, and the actions that have been or are being taken to remediate the issue. Activities that will be reported include event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. Equinix will also provide VA with a written closing action report once the security event or incident has been resolved. VA will follow this same notification process should a security event occur within the VA boundary involving Equinix's provided data. Designated POCs will follow established incident response and reporting procedures, determine whether the incident warrants escalation, and comply with established escalation requirement for responding to security incidents.

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.

No direct notice is provided to end users of DocuSign CLM. Data stored in this system is collected in other systems and aggregated within the system in response to the GAO request for information, investigation, or audit.

The GAO may request any type of data which may contain PII and the Customer continues to have access to such information. VA does not otherwise share this information except if required by law to do so. VA has sole ownership of the information and data located in Salesforce's Data Center. The VA is the only entity that has access to the data.
No personal data is collected directly from individuals. Information in documents loaded to DocuSign CLM may contain PII which was gathered by system users from other systems. Privacy Impact Assessments of other systems are available to be referenced as needed. The opportunity and right to provide or decline personal information requests would be covered in the PIA of the system where data was originally aggregated from. The DocuSign PIA will be published. Both the SORN (75VA001B) and PIA serves as a form of public notice.

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

No personal data is collected directly from individuals. Information in documents loaded to DocuSign CLM may contain PII which was gathered by system users from other systems. Privacy Impact Assessments of other systems are available to be referenced as needed. The opportunity and right to provide or decline personal information requests would be covered in the PIA of the system where data was originally aggregated from. The DocuSign PIA will be published. Both the SORN (75VA001B) and PIA serves as a form of public notice.

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

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

No personal data is collected directly from individuals. Information in documents loaded to DocuSign CLM may contain PII which was gathered by system users from other systems. Privacy Impact Assessments of other systems are available to be referenced as needed. The opportunity and right to consent to particular uses of the information would be covered in the PIA of the system where data was originally aggregated from. The DocuSign PIA will be published. Both the SORN (75VA001B) and PIA serves as a form of public notice.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that VA employees and Veterans will not know that the DocuSign CLM repository collects, maintains, and/or disseminates PII and other SPI about them.

Mitigation: No personal data is collected directly from individuals. Information in documents loaded to DocuSign CLM may contain PII which was gathered by system users from other systems. Privacy Impact Assessments of other systems are available to be referenced as needed. The opportunity and right to provide or decline personal information requests would be covered in the PIA of the system where data was originally aggregated from. The DocuSign PIA will be published. Both the SORN (75VA001B) and PIA serves as a form of public notice.

Section 7. Access, Redress, and Correction

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

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

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may

also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

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

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

No personal data is collected directly from individuals. Information in documents loaded to DocuSign CLM may contain PII which was gathered by system users from other systems. Privacy Impact Assessments of other systems are available to be referenced as needed. The procedures that allow individuals to gain access to their information would be covered in the PIA of the system where data was originally captured by the respective document creator. The DocuSign PIA will be published. Both the SORN and PIA serves as a form of public notice.

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.

No personal data is collected directly from individuals. Information in documents loaded to DocuSign CLM may contain PII which was gathered by system users from other systems. Privacy Impact Assessments of other systems are available to be referenced as needed. The procedures for correcting inaccurate or erroneous information would be covered in the PIA of the system where data was originally aggregated from. The DocuSign PIA will be published. Both the SORN (75VA001B) and PIA serves as a form of public notice.

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.

No personal data is collected directly from individuals. Information in documents loaded to DocuSign CLM may contain PII which was gathered by system users from other systems. Privacy Impact Assessments of other systems are available to be referenced as needed. The notification to individuals on the procedures for correcting their information would be covered in the PIA of the system where data was originally aggregated from. The DocuSign PIA will be published. Both the SORN (75VA001B) and PIA serves as a form of public notice.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

If the GAO Module User discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the documentation they are now providing supersedes that previously provided.
No personal data is collected directly from individuals. Information in documents loaded to DocuSign CLM may contain PII which was gathered by system users from other systems. Privacy Impact Assessments of other systems are available to be referenced as needed. If no formal redress is provided, the alternatives available to the individual would be covered in the PIA of the system where data was originally aggregated from. The DocuSign PIA will be published. Both the SORN (75VA001B) and PIA serves as a form of public notice.

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 Veterans whose records contain incorrect information may not receive notification of any changes. Furthermore, incorrect information in a Veteran's record may result in improper identification.

Mitigation: Privileged users such as Providers and Operation Managers will access and update online records other than their own, consistent with their authority and organizational affiliations using PIV.

No personal data is collected directly from individuals. Information in documents loaded to DocuSign CLM may contain PII which was gathered by system users from other systems. Privacy Impact Assessments of other systems are available to be referenced as needed. The opportunity for access, redress and correction would be covered in the PIA of the system where data was originally captured by the respective document creator. The DocuSign PIA will be published. Both the SORN and PIA serves as a form of public notice.

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.

Neither the GAO nor any agencies other than the VA have access to this system. Procedures explaining which users may access the system are fully documented in the training materials that are provided with the required system training.
There are two user roles:

1. OCLA User – OCLA and ExecSec users have read and write access to all sensitive documents.
2. Program Office User – Program Office users have read and write access to their respective Program Office sensitive documents.

The GAO Module uses VA Identity and Access Management (IAM) services to validate user login information. The validation of VA employees is done through Active Directory Federated Services (ADFS). The GAO Module is hosted in a Salesforce environment within a FedRAMP government certified cloud.

DocuSign CLM uses Salesforce to authenticate users. Access to Salesforce is regulated through Single Sign On (SSO) with ADFS. As a result, access to DocuSign CLM is also governed by ADFS. Users without GAO Module access will not have access to DocuSign CLM.

In order to obtain access to the GAO Module application, the request is submitted must have authorization from their VA manager. Authorized GAO Module users log into the GAO Module application using their proper Org ID though the Single Sign On (SSO) interface. The system will reject anyone who attempts to log in that hasn't been officially authorized prior to the attempt. These users then have the ability to create and modify cases and tasks within cases as it relates to their case work. Cases and tasks are terms used within the application. When a new correspondence is received, a case is created to track it and tasks may be created and assigned to obtain the answer(s) needed to answer the correspondence.

All VA employees use their PIV to sign into GAO Module using ADFS. This IAM VA service checks the presented VA credentials from their PIV card against VA's Active Directory. If an employee is not a user in the Active Directory, then they will not have access to GAO Module.

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

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

Some VA contractors may have access to PII. All contractors have Non-Disclosure Agreements and have completed the appropriate background investigations for their respective roles. Contractors who are involved with system data migration must pass a Tier 4 Background Investigation.

The Lead System Administrator is a contractor for VA and maintains governing authority over all GAO Module environments. The System Administrator maintains users, updates applications, introduces new functionality, governs deployment activity and ensures user operability. The System Administrator is not a primary user of any application on the GAO Module. The System Administrator will monitor and review contracts monthly. System Owner and Contracting

Officer Representative (COR) is the individual to accept and amend any incoming or outgoing contracts involving Salesforce Development Platform VA Assessing.
The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior and HIPAA training via the VA's Talent Management System (TMS). The office of Contract Review operates under a reimbursable agreement with VA's Office of Acquisition, Logistics and Construction (OALC) to provide pre-award, post-award, and other requested reviews of vendors' proposals and contracts. After award, contractors are then reviewed and provisioned into the Salesforce environment by VA's Digital Transformation Center (DTC) system administrators on an ad hoc basis and upon approval of the System Owner.

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.

Initial and annual Cybersecurity Training, Privacy and Rules of Behavior training is required of all users. Upon completion of training, personnel must complete a security and privacy quiz with a passing score. All required VA privacy training must be completed in TMS prior to the user being provisioned. All VA, VHA staff, business associates, affiliates and business partners who have, or will request access to electronic protected health information (EPHI) must complete all the VA's annual security, privacy, and HIPAA privacy related awareness courses as required by Department and VHA policies. Training is also required on GAO Module functionality related to access to secure folders.
Training content details who can access what content. For example:
1. When adding documents to the case, the GAO Module allows for users to generate secure folders within any of the related parent folders. Secure folders are designed for OCLA and Administrator and Staff Offices (AD/SO) to upload sensitive and classified documents, such as those containing personally identifiable information (PII). Secure folders can only be generated by the case owner and the case team.
2. When OCLA generates a secure folder, only users assigned to the OCLA office in the GAO Module will have permissions to view and access an OCLA secure folder. When Administrations or Staff Offices within the Department of Veterans Affairs (AD/SO) generate a secure folder, only users assigned to the OCLA office and users assigned to the AD/SO that generated the secure folder will have permissions to view and access that AD/SO secure folder. All offices under a parent office, such as VHA, will have access to the same secure folder. No AD/SO will be able to view another AD/SO's folder.

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

If Yes, provide:

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

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

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

The DocuSign CLM product (eMASS System ID# 980) is FedRAMP Authorized and is categorized as a Moderate Impact system. Authority to Operate (ATO) was granted November 19, 2020 and expires May 18, 2021.

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2021.04.06 20:15:49 -04'00'

Privacy Officer, Rita Grewal

Thomas J. Orler 178546

Digitally signed by Thomas J. Orler 178546
Date: 2021.04.05 12:38:24 -05'00'

Information Security Systems Officer, Thomas Orler

Michael S. Domanski 326889

Digitally signed by Michael S. Domanski 326889
Date: 2021.04.05 09:13:51 -04'00'

Information System Owner, Michael Domanski

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 to the Privacy Policy found here.