Privacy Impact Assessment for the VA IT System called:

Government Accountability Office Module

Enterprise Program Management Office (EPMO)

Date PIA submitted for review:

12/21/20

System Contacts:

Role	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.Grewal@va.gov	202-632-7861
Information System Security Officer (ISSO)	Joseph Facciolli for James Boring	james.boring@va.gov Joseph.Facciolli@va.gov	215-842-2000, 4613 215-842-2000, 2012
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.

The U.S. Government Accountability Office (GAO) 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 are statutorily required by public laws or committee reports, per GAO's Congressional Protocols (GAO-17-767G). VA's Office of Congressional and Legislative Affairs (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). OCLA uses the GAO Module to process inquires by determining the proper subject matter experts to provide information, obtaining the needed information and submitting the requested information in the form of a final report to GAO.

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 Demand Management Division (formerly known as "Project Special Forces"), a component of the Enterprise Program Management Office (EPMO), is the GAO Module system owner. OCLA uses the GAO Module to manage VA responses to GAO audits and investigations. This work requires tracking GAO correspondence, data requests, reports and recommendations. The system is built using the Salesforce Development Platform (SFDP). The SFDP is Federal Risk and Authorization Management Program (FedRAMP) Moderate approved. It is hosted on the U.S. Government Cloud Plus (FedRAMP High), built on Amazon Web Services (AWS) GovCloud (U.S.). It is classified as a Minor application that augments the Major Application SFDP. DocuSign Contract Lifecycle Management (CLM) is a GAO Module sub-system, providing document management and workflow functionality. The DocuSign CLM datacenter is a FedRAMP Moderate system hosted on the Salesforce Government Cloud.

The GAO Module stores information on system users and other persons who have initiated, or are involved in, processing GAO audits and investigations. There are approximately 300 GAO Module users. These users are identified within the system indicating their respective role(s) in GAO Module case processing. Overall, potentially thousands of individuals could have their information stored in the GAO Module.

OCLA creates a new GAO Module case in response to each new GAO notification letter. This involves tasking case liaisons, organizing an entrance conference, assigning subject matter experts to provide information, completing a final report, holding an exit conference, tracking recommendations, related tasks and updates, and closing the recommendations and the case.

The GAO Module stores and processes the following information: VA offices, VA staff, GAO Module users, associated committees, case emails, case queue ownership, case tasks, case task summaries, case attachments, case notes, case teams, associated contacts, contact roles, functional queues, functional queue members, meetings, meeting attendees, recommendations, recommendation updates, related cases and case-related documents. The DocuSign CLM sub-system provides the following document management functionality: document storage, document version control, security and workflow automation. Additional privacy information associated with this sub-system is addressed in the DocuSign CLM Privacy Impact Assessment (PIA).

Documents stored in the DocuSign CLM sub-system support the following business processes in response to GAO requests: requests for information, responses, concurrences, reviews, signatures, actions and case closure. Related artifacts stored in DocuSign CLM include the following: notification letters, entrance conferences, data requests, statements of facts, exit conferences, 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 GAO Module users and not outside the system.

Case attachments may contain any type of data including Personally Identifiable Information (PII). Case attachments are created and sourced from outside of the system and uploaded through the GAO Module to the DocuSign CLM repository. GAO Module users have access to DocuSign CLM attachments based on their user role or access permissions.

KnowWho is a Salesforce App Exchange product providing a directory of contact and biographical data on Members of Congress, Capitol Hill staffers, and Congressional committees and caucuses. The directory delivers daily updates of committee information and members to the GAO Module as a commercial service. KnowWho uses Salesforce standard objects for loading publicly available PII.

The GAO Module uses GridBuddy to create and manage conference information associated with GAO cases. It provides a form with the ability to perform bulk edits of meeting attendees.

OCLA and several Administration and Staff Offices (AD/SO) use the GAO Module primarily at the VA Central Office (VACO). No regions, hospitals, medical centers or other agencies use the system. System users may also log in remotely. User controls built into the system to manage PII identically at all locations. All users are required to complete mandatory cybersecurity and privacy training, sign VA Rules of Behavior and complete GAO Module training before gaining system access. DocuSign employees and contractors are not granted data access.

The GAO Module limits data access to the case team, which OCLA, the case creator, assigns. Managers review and approve requests for access to the system before new user accounts are created. Once access is granted, users must log into Salesforce via Single Sign-On (SSO) to validate access. OCLA, and Office of the Executive Secretariat (EXECSEC) have access to view all GAO Module cases. AD/SO users provide supporting detail for responses to GAO audits and investigations and have access only to data associated with their assigned cases.

The GAO Module, identified as VA System ID (VASI) #2623, is a child system of the parent Salesforce Application (VASI ID 2104). Salesforce is built in the Salesforce Government Cloud rated FedRAMP Moderate and has an agency authorization date of November 2, 2020. The Federal Information Processing Standards (FIPS) 199 classification is Moderate, and Authority to Operate (ATO) was granted on December 17, 2020 and expires December 17, 2023.The Salesforce and DocuSign CLM contracts establish VA ownership rights of all data. The VA Salesforce contract stipulates that the contractor shall not retain any copies of data, in full or in part, at the completion of the performance period. The data shall contain no proprietary elements that would preclude the VA from migrating the data to a different hosting environment or from using a different case management system in the future.

The Salesforce and DocuSign contracts address the National Institute of Standards (NIST) 800-144 principle that states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf."

If privacy-related data is disclosed, intentionally or unintentionally, VA would incur significant harm to its reputation, and those at fault 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 damaged.

Completion of this PIA is not expected to require changes to any technology or business processes. System of Record Notice (SORN): 75VA001B - Department of Veteran's Affairs Secretary's Official Correspondence Records - VA. (This SORN has expired but an update is in progress during Q3 2021.)

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 following text box:

☒ 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

Federal employee information/data which is publicly accessible.

NOTE: Federal employees' information is considered PII, however it is considered non-sensitive PII.

- GAO Module objects contain VA staff, GAO Module users, case emails, case queue ownership, case notes, case teams, associated contacts, contact roles, functional queue members, meeting attendees, recommendation updates and case-related attachments.

- Case attachments may contain names, work addresses, work emails, work phone numbers, health records and pharmacy pricing data or any other type of PII, depending on the nature of the inquiry.

- KnowWho contains biographical data on all Members of Congress, Capitol Hill staffers, committees and caucuses. The data received is publicly available PII, which may be sensitive.

PII Mapping of Components

The GAO Module consists of six key components. Each component has been analyzed to determine if any elements collect PII. The type of PII that the GAO Module collects, and the reasons for collection, are listed in the table below.

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
VA Salesforce Development Platform (SFDP)	Yes	Yes	Any of the following may be stored: name, DOB, email address, federation ID, associated contacts, contact role, functional queue member, personal address, personal email and personal phone number.	PII is gathered and stored to identify persons and parties involved in responding to or managing GAO cases. PII may also be included in case attachments because persons or parties are subject of a GAO case or are incidentally identified in a case.	Data is stored in a FedRAMP Moderate environment protected by Moderate-level security controls. SFDP uses cryptography that is compliant with federal laws and regulations (i.e., FIPS 140-2). All PII is encrypted in transport and at rest. Profile-based permissions govern access. User profiles are reviewed regularly to ensure appropriate access. VA employees and contractors are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
DocuSign, Swift Application Programming Interface (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 gathered by users from other systems.	All seven safeguards listed immediately following this table are environment-level controls and apply to each of the five DocuSign CLM components in this table.

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
DocuSign, Network Attached Storage (NAS)	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 gathered by users from other systems.	All seven safeguards listed immediately following this table are environment-level controls and apply to each of the five DocuSign CLM components in this table.
DocuSign, 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 gathered by users from other systems.	All seven safeguards listed immediately following this table are environment-level controls and apply to each of the five DocuSign CLM components in this table.
DocuSign, Apache Cassandra	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 gathered by users from other systems.	All seven safeguards listed immediately following this table are environment-level controls and apply to each of the five DocuSign CLM components in this table.
DocuSign, 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 gathered by users from other systems.	All seven safeguards listed immediately following this table are environment-level controls and apply to each of the five DocuSign CLM components in this table.

Safeguards: All seven safeguards detailed as follows are environmental-level safeguards and apply to each of the five DocuSign CLM 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 Burp Suite 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.

The VA Salesforce Development Platform (SFDP) provides names, emails and offices of case team users.

Incoming and outgoing case email originate with GAO, OCLA, liaison offices and AD/SOs. GAO provides recommendations, and system users load them into the GAO Module. OCLA, Liaison Office or AD/SO system users provide all other information in the system. KnowWho sources names of associated committees and members. This is necessary for reporting back to committee members and Congress on cases for which they are a stakeholder.

VA AD/SOs may attach sensitive information to a case in the form of standard office productivity files (Microsoft Word, and so on) or as text-based data. GAO Module users may source this data from any other systems, such as SharePoint or any other routine office productivity software throughout VA. Information collected may be shared with the GAO, but this is accomplished outside the system. There are no GAO agency system users.

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.

OCLA and AD/SOs enter data into data fields in the GAO Module. GAO Module users collect documents, reports and artifacts through standard office software and attach such repository content to the associated case. GAO Module users enter all the data in the system, except for SFDP and KnowWho-provided data.

No information is collected on paper to populate the system, other than meeting sign-in forms. These forms could be printed and used for maintaining a list of meeting attendees.

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.

Persons' names are identified and stored in the GAO Module to identify: persons with a role in executing a process on a GAO case; system users; a person associated with a case, such as a GAO or AD/SO contact; meeting attendees; signatories to a case resolution task; and Members of Congress. A GAO Module case record may also list the committees associated with a particular GOA investigation or audit.

SPI 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 only GAO Module licensed users may retrieve documents stored therein.

The GAO Module does not collect any commercial data; however, a user may upload commercial data into the system in response to a GAO investigation, audit or request for information. KnowWho information is provided in a daily integration to Salesforce for any applications built on the platform.

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.

Users of systems from which the information was originally sourced may check the information stored in the GAO Module for accuracy. End users must check information for accuracy before entry into the system.

The files and case attachment documents are not checked for accuracy unless end users do so prior to uploading documents to DocuSign CLM.

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. 552, "Freedom of Information Act," c. 1967
2. 5 U.S.C. 552a, "Privacy Act," c. 1974
3. 18 U.S.C. 1030 (a) (3), "Fraud and related activity in connection with computers"
4. 38 U.S.C. 218, "Security and law enforcement on property under the jurisdiction of the Veterans Administration"
5. OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems
6. Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
7. Federal Information Security Management Act (FISMA) of 2002
8. Executive Order 13103, Computer Software Privacy
9. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
10. FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
11. FIPS 201-1, Personal Identity Verification of Federal Employees and Contractors
12. FIPS 140-2, Security Requirements for Cryptographic Module
13. VA Handbook 6510, VA IDENTITY AND ACCESS MANAGEMENT, 2016
14. •VA Handbook 6500.2, Management of Data Breaches Involving Personal Information (SPI),2016
15. •VA Directive 6066, Protected Health Information (PHI) and Business Associate Agreements Management, 2014
16. No. 104---231, 110 Stat. 3048
17. Public Law 100--503, Computer Matching and Privacy Act of 1988
18. E---Government Act of 2002 § 208
19. Federal Trade Commission Act § 5
20. 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33

21. Title 35, Code of Federal Regulations, Chapter XII, Subchapter B

22. OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

23. OMB Circular A---130, Management of Federal Information Resources, 1996

24. OMB Memo M---10---23, Guidance for Agency Use of Third---Party Websites

25. OMB Memo M---99---18, Privacy Policies on Federal Web Sites

26. OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions

27. OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII

28. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

29. Various state privacy laws

30. SORN: 75VA001B -Department of Veteran's Affairs Secretary's Official Correspondence Records-VA

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.

Privacy Risk: SPI, including any type of personal contact information, SSN and medical information, may be released to unauthorized individuals.

Mitigation: Profile-based permissions govern user information access. Profiles are reviewed on a regular basis to ensure that information is shared only with appropriate users. All employees with access to Veterans' information are required to complete the VA Privacy and Information Security Awareness and Rules of Behavior training annually. All VA, Veterans Health Administration (VHA) staff, business associates, affiliates and business partners who have, or will request access to, Electronic Protected Health Information (EPHI), must complete VA's annual security, privacy and Health Insurance Portability and Accountability Act (HIPAA) privacy-related awareness courses as required by Department and VHA policies.

OCLA controls access to the GAO Module containing sensitive information. Only case team members are permitted to view or add sensitive content. OCLA strictly controls who is added to the case team, providing access on a need-to-know basis. Existing case team members can add additional case team members. 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 exceptions to this rule are OCLA, which oversees the case, and the EXECSEC, which provides additional oversight. Both offices can see all sensitive information uploaded into the GAO Module. However, one must be a GAO 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, 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: Multi-level security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only Hypertext Transfer Protocol Secure (https) traffic on ports 80 and 443, 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 (2FA), 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 data accuracy.

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.

Names are used to identify persons and parties involved in responding to or managing GAO cases. All system users are identified in the GAO Module.

Names and all other PII listed below may be used for persons who are a subject of a GAO case or are incidentally identified in a case:

- 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

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

The GAO Module does not perform analysis or processing on any stored data. The system functions as a business process workflow with database links to case attachments stored in the DocuSign CLM document repository. The system does not create any information such as scores, analysis or reports.

2.3 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.

Implemented controls ensure data is used and protected in accordance with legal requirements, VA policies and VA's stated purpose for data usage. Controls include mandatory training completion for all employees, volunteers and contractors. Audits are also performed to ensure information is accessed and retrieved appropriately. 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. All controls are per Acting Assistant Secretary for Information and Technology [Designated Accrediting Authority (DAA)] approval.

The Salesforce FedRAMP Moderate Authority to Operate (ATO) package employs security controls in the respective baselines unless specific exceptions have been allowed. Exceptions are based on the tailoring guidance provided in the VA Moderate ATO for Salesforce, NIST Special Publication 800-53 and specific VA directives. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how Veterans' information is used, stored and protected.

The GAO Module is accessible only to OCLA, Liaison Office and AD/SO users who require logical access to the system. The GAO Module controls access to DocuSign CLM case attachments. Users must access the system through VA via 2FA Personal Identity Verification (PIV) card.

Identity and Access Management (IAM) systems verify credentials and collect audit logs based on access requested and may contain PII captured to authenticate to the resource.

Before new users are provisioned for GAO Module access, they must be approved by a VIEWS Office Coordinator (VOC) member and must complete instructor-led, web-based training. Users must provide their certificate of training completion to their assigned VOC member. Once a user provides the GAO Module training certificate, GAO Module login credentials and access can be granted. The VOC member will not grant login credentials to individuals who do not require access, have not been approved or have not provided the training certificate. Inactive user accounts are deactivated after 90 days.

The system applies the same safeguards to documents regardless of whether documents contain PII. Secure folders within the GAO Module manage control over PII access. Users needing to upload PII must create a secure folder that is only visible to the case owner office. Users must be assigned to a case team to see the case-associated secure folders and PII. If not on a case team, users would not know of or have access to PII in a document. Cases containing sensitive but not classified information have restricted access to the entire case, not just to specific folders. Sensitive but not classified content depends on the use case and could, but does not necessarily, contain PII. Users cannot email documents containing PII directly from a module or assign such

documents to a case task. Email and case tasks do not display secure folder contents. OCLA and the EXECSEC have oversight and access to all case documents, regardless of case or PII contents.

The Salesforce 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 to protect the environment in which customer data is stored. Additionally, Salesforce privacy and security statements can be viewed here:

http://www.salesforce.com/company/privacy

Salesforce has a global privacy team that oversees privacy. Salesforce, DocuSign and the VA share responsibility for protecting the security and privacy of user data.

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

All information collected in the GAO Module will be retained throughout the GAO investigation lifecycle, 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, and so on, 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.

GAO Module record disposition period is "Temporary," meaning, "Destroy six years after report submission or oversight entity notice of approval, as appropriate, but longer retention is authorized if required for business use."

All information collected in the GAO Module will be retained throughout the GAO investigation lifecycle.

The DocuSign CLM system does not create documents. The documents 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 as 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. The OCLA records steward determines 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 VA Records Office determined that the data stored in the GAO Module should be retained according to the General Records Schedule 5.7-050: Mandatory reports to external Federal entities regarding administrative matters.

The VA Records Office determined that the documents 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. The OCLA records steward determines 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 document contents.

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 Moderate Government Cloud will be retained according to the NARA-approved retention period.

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

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

What is the procedure for elimination of the records and Sensitive Personal Information that may be captured in the GAO module?

Paper documents are destroyed six years after the final report is issued. Paper records are boxed, and OIT Records Management is contacted for disposition. For electronic documents, the present disposition is six years after the final report is issued.

The OCLA sets the disposition date for documents stored in the GAO Module and 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 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 does not retain information. The systems using DocuSign will follow electronic media sanitization when the records are authorized for destruction (or upon system decommission). Electronic media sanitation will be carried out in accordance with VA Handbook 6500.1, Electronic Media Sanitization.

The GAO Module business owner and product owner have engaged with EPMO Records Management and OCLA records officer to configure the EPMO Records Management-MetaKnowledge Repository (RM-MKR) tool to manage the disposition schedule and process going forward.

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. SSO technology protects access to these systems by verifying the user and providing access only to data based on user permissions. All other environments, including development and training, use lower-level servers that do not host PII data.

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.

Privacy Risk: Longer retention times within the GAO Module increase the risk that information may be compromised or breached.

Mitigation: The OCLA may dispose of the non-record content after the final report is delivered to GAO. Any documents that contain SPI are easily identified and are stored in secure folders. The OCLA records steward is responsible for determining 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 document contents. 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
DocuSign CLM	GAO Module case attachments must be accessible to the GAO Module for users to respond GAO audits and investigations. Case attachments may contain PII.	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 account numbers, certificate/license numbers,	Connection between DocuSign CLM and the VA is through Salesforce, which is bi-directional. Two-way secure socket layer/Transport layer Security (SSL/TLS) encryption. The data from Salesforce traverses through the Equinix (TIC) gateway to VA Salesforce Application.

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
		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 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.

Privacy Risk: Information may be shared with unauthorized VA personnel.

Mitigation: Implemented safeguards ensure data is not sent to unauthorized VA employees, including employee security and privacy training and required reporting of suspicious activity. The system uses secure passwords, access on a need-to-know basis, PIV cards, PIN, encryption and access authorization.

Document management functionality uses a secure folder feature to ensure that data is not shared inappropriately outside of case teams and across other VA AD/SOs.

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
VA Salesforce Development Platform (SFDP)	To access a single common lookup source of VA offices, staff and related data	Names, emails, phone numbers, offices of case team members and any type of PII including: name,	ISA/MOU	Content is accessible within GAO Module Graphical User Interface (GUI)

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
	necessary to process GAO audits and investigations	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, other unique identifying numbers.		depending on user role.

If specific measures have been taken to meet the requirements of OMB Memoranda M-0615 and M-06-16, note them here.

This is not applicable. No specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16.

The GAO Module does not share data with third parties. The system configures and implements administrative and physical safeguards to deny users from accessing data outside of role and

organizational assignments. Technical controls implemented include encrypting data at rest and in transit to prevent data exposure, and 2FA is the only means for access. The system includes a timeout feature that automatically logs off a user after a specified period of inactivity. For internal users, AC-12 Session Termination control is inherited from the VA IAM and Active Directory Federation Services (ADFS) for all PIV-enabled users listed in the Global Address List (GAL). IAM implements a PowerShell script that automatically disables accounts where the password has not been changed in 90 days or if the account was not accessed within 90 days. OCLA can configure the timeout feature.

The metadata logging of actions performed with DocuSign CLM, as detailed in Section 2.3, occur whether a user is remote.

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

Privacy Risk: With the exception of application data stored in Salesforce Government Cloud, data is not shared outside of the VA. If data is being shared outside of the Department in the future, access controls will be implemented based on Memoranda of Understanding (MOU), 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 for or legal authority to access VA data.

Mitigation: VA has contracted Salesforce to deliver services that include maintaining VA data. A contract in place clearly articulates Salesforce's roles and responsibilities. Authorized Salesforce personnel access data on users to provision and provide the Salesforce service. Authentication controls access, which is restricted to authorized individuals. Salesforce's security policies address the required security controls to protect PII. SFDP 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. Reported activities 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 requirements 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.

GAO Module users receive no direct notice. Other systems collect and aggregate data stored in this system in response to the GAO request for information, investigation or audit.

No personal data is collected directly from individuals. Information in documents loaded to DocuSign CLM may contain PII gathered by users from other systems. PIAs of other systems are available to be referenced as needed. The PIA of the system from which data was originally aggregated would cover the opportunity and right to provide or decline personal information requests. The GAO Module PIA and the DocuSign PIA will be published. Both the SORN (75VA001B) and PIAs serve 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 gathered by users from other systems. PIAs of other systems are available to be referenced as needed. The PIA of the system from which data was originally aggregated would cover the opportunity and right to provide or decline personal information requests. The GAO Module PIA and the DocuSign PIA will be published. Both the SORN (75VA001B) and PIAs serve 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 gathered by users from other systems. PIAs of other systems are available to be referenced as needed. The PIA of the system from which data was originally aggregated would cover the opportunity and right to consent to particular information uses. The GAO Module PIA and the DocuSign PIA will be published. Both the SORN (75VA001B) and PIAs serve 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

Privacy Risk: VA employees and Veterans will not know that the GAO Module 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 that was gathered by users from other systems. PIAs of other systems are available to be referenced as needed. The PIA of the system from which data was originally aggregated would cover the opportunity and right to provide or decline personal information requests. 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 the GAO Module may contain PII gathered by users from other systems. PIAs of other systems are available to be referenced as needed. The PIA of the system from which the document creator originally captured the data would cover the information access procedures. The GAO Module PIA and the DocuSign PIA will be published. Both the SORN (75VA001B) and PIAs serve 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 the GAO Module may contain PII gathered by users from other systems. PIAs of other systems are available to be referenced as needed. The PIA of the system from which data was originally aggregated would cover the procedures for correcting inaccurate or erroneous information. The GAO Module PIA and the DocuSign PIA will be published. Both the SORN (75VA001B) and PIAs serve 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 the GAO Module may contain PII gathered by users from other systems. PIAs of other systems are available to be referenced as needed. The PIA of the system from which data was originally aggregated would cover the notification to individuals on information correcting procedures. The GAO Module PIA and the DocuSign PIA will be published. Both the SORN (75VA001B) and PIAs serve 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.

Is there formal redress for inaccurate information? Are there specific procedures for addressing errors? Describe:

Before conducting an investigation or audit, the GAO decides whether a data reliability assessment is necessary. This decision depends on whether the data would materially support findings, recommendations or conclusions, and whether the data presents risks including data sensitivity. If necessary, the GAO uses a risk-based framework to assess the data quality as a required investigation or audit component. The framework considers three factors for assessing the data under consideration for audit purposes: the data applicability, completeness and accuracy. Whatever the outcome, auditors are responsible for ensuring the data reliability. The GAO document titled "Assessing Data Reliability," published December 2019, details the entire process.

If information provided during intake is discovered to be incorrect, the GAO Module user records corrections with a statement that the updated documentation supersedes the previous.

No personal data is collected directly from individuals. Information in documents loaded to the GAO Module may contain PII gathered by users from other systems. PIAs of other systems are available to be referenced as needed. If no formal redress is provided, the PIA of the system from which data was originally aggregated would cover the alternatives available to the individual. The GAO Module PIA and the DocuSign PIA will be published. Both the SORN (75VA001B) and PIAs serve 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.

Privacy Risk: 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 the GAO Module may contain PII gathered by users from other systems. PIAs of other systems are available to be referenced as needed. The PIA of the system from which the respective document creator originally captured the data would cover the opportunity for access, redress and correction. The GAO Module PIA and the DocuSign PIA will be published. Both the SORN (75VA001B) and PIAs serve 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. The materials provided with the required system training fully document procedures explaining which users may access the system.

There are two user roles:

1. OCLA User – OCLA and EXECSEC users have read and write access to all sensitive documents.

2. AD/SO User – AD/SO users have read and write access to their respective sensitive documents.

The GAO Module uses VA IAM services to validate user login information. ADFS performs the validation of VA employees. The GAO Module is hosted in a Salesforce environment within a FedRAMP Moderate Government Cloud.

DocuSign CLM uses Salesforce to authenticate users. SSO with ADFS regulates access to Salesforce. As a result, ADFS also governs access to DocuSign CLM. Users without GAO Module access will not have access to DocuSign CLM.

To access the GAO Module application, users must obtain VA manager authorization and submit a request. Authorized GAO Module users log into the GAO Module application using their proper organization ID though the SSO interface. The system will reject any non-authorized users who attempt to log in. These users can then create and modify cases and tasks related to their 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 address the correspondence.

All VA employees use their PIV card to sign into GAO Module using ADFS. The VA IAM service checks the presented VA credentials from their PIV card against VA's Active Directory (AD). Users not in the AD will not have access to the 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 NDAs and have completed the appropriate background investigations for their respective roles. Contractors involved with system data migration must pass a Tier 4 background investigation.

The lead system administrator (SA), a VA contractor, maintains governing authority over all GAO Module environments. The SA maintains users, updates applications, introduces new functionality, governs deployment activity and ensures user operability. The SA is not a primary user of any application in the GAO Module. The SA monitors and reviews contracts monthly. System owner and Contracting Officer Representative (COR) accept and amend any incoming or outgoing contracts involving SFDP VA Assessing.

Contractors who provide system support are required to complete annual VA Privacy and Information Security and Rules of Behavior and HIPAA training via 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, VA's Digital Transformation Center (DTC) system administrators review and provision contractors into the Salesforce environment on an ad hoc basis and upon system owner approval.

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 must complete initial and annual Cybersecurity, VA Privacy and Information Security Awareness and Rules of Behavior training in TMS before being provisioned. Upon completion of training, personnel must complete a security and privacy quiz with a passing score. All VA, VHA staff, business associates, affiliates and business partners who have, or will request access to, EPHI must complete all the VA's annual security, privacy and HIPAA privacy-related awareness courses as required by Department and VHA policies.

GAO Module-specific training is required for both user roles: OCLA and AD/SO. Training details content access. For example:

1. When adding documents to the case, the GAO Module allows users to generate secure folders within any related parent folders. Secure folders are designed for OCLA and AD/SO to upload sensitive and classified documents, such as those containing PII. Only the case owner and case team can generate secure folders.

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 that folder. When VA AD/SO generate a secure folder, only users assigned to the OCLA office and to the AD/SO that generated the secure folder will have view and access permissions. 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 is MODERATE.*

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 GAO Module (VASI ID 2623) is a child system of the parent Salesforce Application (VASI ID 2104), which is built in the Salesforce Government Cloud and has an agency authorization date of November 2, 2020. The FIPS 199 classification is Moderate. The ATO was granted on December 17, 2020 and expires December 17, 2023.

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: 2021.06.24 10:46:16 -04'00'

Privacy Officer, Rita Grewal

Joseph Facciolli 148552

Digitally signed by Joseph Facciolli 148552
Date: 2021.06.14 11:30:32 -04'00'

Information System Security Officer, Joseph Facciolli for James Boring

Michael S. Domanski 326889

Digitally signed by Michael S. Domanski 326889
Date: 2021.06.22 15:46:29 -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).

No personal data is collected directly from individuals. Information in documents loaded to DocuSign CLM may contain PII that was gathered by 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 serve as a form of public notice.