Contents

No.	Tab	Description
1	Definitions	Definitions to assist Suppliers with responses
2	Standard Agreement	Contains requirements that are part of VITA's Standard Agreement
3	General	General requirements that all Suppliers must answer
4	Security Requirements	Security requirements that all Suppliers must answer
5	Identity Proofing	Identity Proofing Capability Requirements
6	T2 ID Proofing Tech Support	Tier 2 Identity Proofing Technical Support Requirements
7	T3 ID Proofing Tech Support	Tier 3 Identity Proofing Technical Support Requirements
8	Implementation	Implementation Requirements
9	Reporting	Reporting Requirements
10	Training	Training Requirements
11	Communication	Communication Requirements
12	Perfomance Measures & Reports	Perfomance Measures and Reports Requirements
13	On Premise Responsibility Matrix	On Premise Responsibility Matrix
14	Cloud Responsibility Matrix	Cloud Responsibility Matrix

Definitions	
Authorized User	All public bodies, including VITA, as defined by Code § 2.2-4301 and referenced by Code §§ 2.2-4304 and 2.2-2012, authorized to participate in the procurement of information technology under this Contract. Authorized Users include private institutions of higher education that are listed at: https://cicv.org/Our-Colleges/Profiles.aspx.html Pursuant to Code § 2.2-4304, "Authorized Users" also includes those public bodies,
End User	An individual who utilizes the identity verification solution.
Supplier	Any entity that submits a proposal in response to this RFP.
For the purposes of answering the questions in this document, please refer to the following definitions for Identity Assurance Levels, as documented in NIST 800-63-4, which is currently in draft form.	
IAL0 (No identity verification)	There is no requirement to link the End User to a specific, real-life identity. Any attributes provided in conjunction with the End User's activities are self-asserted and are treated as self-asserted. Self-asserted attributes at IAL0 are neither validated nor verified by an independent third party.
IAL1	This identity verification process supports the real-world existence of an End User's claimed identity. Core attributes are obtained from identity evidence or asserted by the End User. All core attributes are validated against authoritative or credible sources and steps are taken to link the attributes to the person undergoing the identity verification process.
IAL2	IAL2 requires the collection of stronger types of evidence and a more rigorous
IAL3	IAL3 adds the requirement for a trained Credential Service Provider (CSP)
For the purposes of answering the questions in this document, the following definitions for Tiers of Support are as follows:	
Tier 0	Tools and resources that allow End Users to resolve issues independently. This is a self-service capability that includes options such as knowledge-based articles, frequently asked questions, job aids and how-to videos.
Tier 2	In-depth technical support for the identity verification solution. Support personnel with deep knowledge of the product or service, but not necessarily the engineers or programmers who designed and created the product. Support would resolve issues that cannot be resolved by Tier 1 staff or process issues resulting in unacceptable error levels, decreased throughput, or security concerns.
Tier 3	Expert product and service support. Tier 3 technicians attempt to duplicate problems and define root causes, using product designs, code, or specifications. Generally, technicians are the most highly skilled specialists, and may include the product developers, architects, and software and hardware engineers. These technicians work with the Authorized User to determine the root cause of the problem and the steps needed to fix it. Tier 3 also focuses on capacity planning and product improvements.

Req. No.	Category	Requirement	Yes (Y) Future (F) No (N)	Provide an explanation of how the Solution fulfills the requirement. The Supplier's detailed explanation should not simply be an affirmative reiteration of the question, but should describe the manner in which the requirement is met. Where possible and beneficial, please provide screenshots or graphics to help illustrate your response. Where your response is described as a future release or update as the provision, please provide a timeline for that provision. Supplier may also use this column to cross-reference a detailed explanation included as an attachment to its
Standard Agreement Requirements				
The Supplier's responsibilities include:				
SA01	Data Protection	Supplier agrees to comply with all applicable state and federal laws, regulations, and standards concerning the protection of Commonwealth and Authorized User data. Please describe how Supplier will comply.	Y	Socure will comply with all applicable state and federal laws, regulations and standards. Further, SocureGov was architected to protect personal information submitted by the Commonwealth for processing by storing and processing. The SocureGov platform has been designed, built, and assessed against FedRAMP Moderate control requirements by a FedRAMP-approved Third Party Assessment Organization (3PAO). Our fully hosted (AWS) cloud platform has been assessed against and currently complies with the following industry security standards: StateRAMP Moderate (Authorized), TX-RAMP Moderate (Authorized), System and Organization Controls (SOC) 2 Type 2, International Organization for Standardization (ISO) 27001, 27017, 27018, 27701, Web Content Accessibility Guidelines (WCAG) 2.1 Level AA, and NIST Identity Assurance Level 2 (IAL2). Socure is compliant with FedRAMP requirements and has been assessed by a FedRAMP-approved third-party assessor (3PAO) as compliant with FedRAMP security controls. All traffic is encrypted using FIPS 140-2 validated modules at the edge and within our system boundary, both in transit (with TLS 1.2+) and at rest (AES-256 in GCM mode). As a result, Commonwealth and Authorized User data is protected in accordance with the most stringent security and compliance requirements of U.S. federal agencies. As such, our customers generally find that our security standards meet or exceed their security policies.
SA02	Data Standards	Supplier's Solution's interface to Commonwealth systems must comply with or have https://www.vita.virginia.gov/media/vitavirginiagov/it- Describe how Supplier's Solution will comply.	Y	As part of Socure's continuing commitment to our PS customer mission & expectations, the SocureGov Platform services, processes & infrastructure have been assessed against multiple identity & technology industry standards. We have assumed these asssessment and accredidations will meet
SA03	508 Compliance	Supplier's Solution, training material, and communications plans must provide https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/domain-amp- (Refer to www.section508.gov and www.access-board.gov for further information). https://www.itic.org/policy/accessibility/vpat	Y	All aspects of the Solution with which the State and its consumers will interact have been evaluated by a third-party and found to be in alignment with applicable WCAG 2.1 AA standards. We have assumed that this level of compliance will meet Commonwealth standards and Socure would be glad to discuss any requirements of the Commonwealth beyond such WCAG compliance. Socure maintains
SA04	Homeland Security Standards	Supplier's Solution or any of Supplier's subcontractors' components must not include any hardware, software, or services that are prohibited by the U.S. Department of Homeland Security for use on federal systems as defined in Code of VA §2.2-5514. If no, describe how Supplier will ensure these standards are met.	Y	The SocureGov platform has been evaluated against the most stringent of requirements and is in process for FedRAMP Authorization. All hardware, software and services have been assessed by our auditor to ensure compliance with Department of Homeland Security requirements.
SA05	WCAG Standards	Supplier's Solution, training material, and communications plans must comply with https://www.w3.org/TR/WCAG21/	Y	All aspects of the Solution with which the State and its consumers will interact have been evaluated by a third-party and found to be in alignment with applicable WCAG 2.1 AA standards as required by

SA06	Kaspersky Standards	Supplier's Solution or any of Supplier's subcontractors' components include Kaspersky-branded products. See definition below. If yes, please describe. “Kaspersky-branded products” means information security products, Solutions, and services supplied, directly or indirectly, by AO Kaspersky Lab or any of its predecessors, successors, parents, subsidiaries, or affiliates, including Kaspersky Lab North America, Kaspersky Lab, Inc., and Kaspersky Government Security Solutions, Inc. (collectively, “Kaspersky”), including those identified below: Kaspersky-branded products currently known to Department of Homeland Security are: Kaspersky Anti- Virus; Kaspersky Internet Security; Kaspersky Total Security; Kaspersky Small Office Security; Kaspersky Anti Targeted Attack; Kaspersky Endpoint Security; Kaspersky Cloud Security (Enterprise); Kaspersky Cybersecurity Services; Kaspersky Private Security Network; and Kaspersky Embedded Systems Security.	N	The SocureGov Platform does not utilize Kaspersky-branded products.
SA07	Data Consent Lifecycle	Supplier's Solution must inform End Users how their data is used and obtain their permission initially to store or share their data (if applicable) and whenever changes are made to the storage or sharing of their data. If no, explain any alternative Solutions.	Y	Socure empowers our customers to themselves provide any required notices, and obtain any required consents, necessary to process PII through our Passive SocureGov modules (Socure Verify, Sigma Fraud products, RiskScores & Global Watchlist functions). This allow customers to customize and streamline their user experience. However, to comply with applicable law, Socure will need to obtain its own consent from users of its Predictive Document Verification product. Socure's GRC & Legal functions continuously monitor the biometric & applicable legal landscapes in order to ensure adherence to the regulatory environment. Socure is happy to discuss any specific concerns the state may have.
SA08	Data Standards	Supplier agrees to provide information about standards the solution adheres to (e.g., GDPR, CCPA, HIPAA, etc.) to protect the End Users’ personal data (PII and PHI) from those who should not have access to it.	Y	Socure employs a robust data compliance framework, including user access administration protocols to limit access to End User personal data. We welcome the opportunity to discuss these processes with the state.
SA09	Data Standards	Supplier agrees to provide a solution that complies with the Virginia Consumer Data Protection Act as so far as it is applicable. See link below. https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/	Y	Socure complies with applicable privacy and data protection laws, including the Virginia Consumer Data Protection Act, in numerous ways, including the following: • Implementing and enforcing Fair Information Practice Principles throughout the product development lifecycle; • Maintaining a public-facing privacy statement that provides the requisite notice and description of our privacy and data handling practices; This privacy notice describes how we collect, use, and disclose data. • Processing data only for the business purposes and pursuant to the disclosed lawful bases for collection; • Conducting third party assessments and maintaining security certifications for SOC 2 Type 2, ISO 27001, ISO 27701 (Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management) and 27018 (Information technology tection Officer. — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors); • Maintaining a solution that is compliant with Federal Risk and Authorization Management Program (FedRAMP), which requires a Privacy Impact Assessment (PIA) and several controls designed to

SA10	Artificial Intelligence	Supplier agrees to provide a solution that complies with the Commonwealth of Commonwealth of Virginia 1.17.2024 1 Policy Standards for the Utilization of Artificial Intelligence by the Commonwealth of Virginia Overview Virginia is	Y	Socure has documentation and processes to support any department, agency, or office's compliance needs with regards to these standards. We can support your responsibilities with regards to the ethical use of AI, business use case assessment, approval processes, and drafting of mandated disclaimers. Socure is accustomed to supporting regulated financial institutions with model risk management and fair lending documentation, as well as is able to support your AI transparency needs.

General				
Req. No.	**Category**	**Requirement**	**Yes (Y)**	**Provide an explanation of how the Solution fulfills the requirement. *The Supplier's detailed***
General Requirements				
The Supplier's responsibilities include:				
G01	Platform	Does the Supplier agree to propose a solution that is cloud-based/SaaS or an on-premise solution? Please provide diagrams that detail the hardware, software, infrastructure, etc., that are used to support either solution.	Y	Socure will provide a cloud-based/SaaS solution. Please find the attached the attached diagram which shows where how our proposed solution would integrate with the Identity Solution for the Commonwealth. See Tab "G01 - Diagram of Solution"
G02	Migration of On-Premise Solution	If Supplier is required by the Authorized User at a future date to migrate its on-premise solution (if applicable) to a cloud-based solution, describe how Supplier would accomplish this migration and the timeline for it.	Y	Post adoption migration to the cloud would not be necessary. The SocureGov platform offering is a fully hosted, cloud-based (SaaS) solution.
G03	Business Continuity and Disaster Recovery	Provide a business continuity and/or disaster recovery process. If yes, describe these processes.	Y	Socure has a dedicated team across Governance, Risk, Compliance, Legal, Tech and Product to ensure Business Continuity across all lines of business and corporate functions. Socure's FedRAMP-compliant Contingency Plan is designed to secure the resilience and continuity of operations in the event of significant disruptions, such as natural disasters or other unforeseen incidents. The plan includes strategies for data backup, rapid adaptation and recovery to maintain critical business processes and IT services. It encompasses the development and implementation of a detailed BCP and Disaster Recovery Plan (DRP), regular testing and review of these plans, and training for all relevant parties on their roles and responsibilities during an incident. The Socure Contingency Plan aims to minimize operational disruptions and facilitate a quick restoration of services, with specific procedures and resources outlined to assist in recovery. It also includes measures for maintaining the availability of business-critical information and resources. The plan is regularly reviewed and updated to reflect current business requirements and to manage any changes effectively. Additional details & definition around Socure's Contingency Plan can be shared upon request.
G04	On-Premise Disaster Recovery Plans	If Supplier's solution is on-premise, provide a Disaster Recovery plan. Supplier's disaster recovery plan must meet a recovery time objective (RTO) of 24 hours and a recovery point objective (RPO) of 1 hour.	Y	SocureGov is fully SaaS based, N/A.
G10	Demo Availability	Provide a weblink for a demo of the proposed solution/software. This weblink should be available throughout the life of the contract.	Y	Socure has created a self-service Demo environment where the Commonwealth can explore Socure's fully integrated fraud risk, compliance, and document verification solutions for multiple use cases. https://www.socure.com/demo. The opening screen asks you to to create an account, however, it is self guided from there on out. This link is always avalaible and will continue to evolve as use cases are developed.
G06	General	If requested by the Authorized User, Supplier staff will submit to background checks conducted and paid for by the Authorized User.	Y	Socure conducts background checks on all employees as part of its hiring process. The background investigation includes the following screening criteria: - Employment history verification - Criminal background check - Residency history verification - Social security number trace - Sex offender registry check We have assumed additional background checks will therefore be unecessary. Socure welcomes the conversation to discuss what additional checks the Commonwealth would advise.
G07	Encryption Standards	Provide a solution that uses encryption standards to protect data at rest and in transit. Describe these standards.	Y	Socure's data security posture enforces encryption standards in both data at rest & in transit. We leverage the following industry best practices: For data at rest, Socure uses AES-256 encryption to secure personal data, including biometric data. This encryption standard is applied across Socure's systems to protect the confidentiality and integrity of stored data. Additionally, Socure emphasizes data minimization, purpose limitation, and conducts regular privacy risk assessments to manage and mitigate privacy risks effectively. These practices are part of Socure's broader governance and privacy program aimed at maintaining high standards of data protection and privacy compliance. During data transit, Socure ensures the security of data through the use of TLS 1.2 encryption, providing a secure channel for data transmission. Specifically, for Socure's public endpoints, Socure supports one-way TLS1.2+ at the TCP layer and/or combined with two-way payload signature and encryption at the application layer. For Socure's private endpoints, Socure supports mutual TLS1.2+ at the TCP layer.
G08	Account Management	Provide a dedicated account manager and support team for questions and concerns from Authorized Users and End Users. Describe your plans to support the Authorized User(s).	Y	Socure adopts a comprehensive and client-focused methodology. After the contract award, Socure designates the Account Management Team, which is pivotal in guiding both product implementation and post-production release account management. The Strategic Account Manager assumes the role of the implementation project manager, supported by additional team members including the Account Executive, Solutions Consultant, and Technical Account Manager. This team structure is designed to ensure a smooth transition of customer objectives, with each role having specific responsibilities: • **Account Executive**: Manages client relationships and communicates priorities and timelines to ensure a smooth transition of customer objectives. • **Solutions Consultant**: Accountable for overall project implementation, works closely with the Technical Account Manager and Strategic Account Manager to define pre-go-live calibrations, and coordinates preliminary kickoff meetings. • **Technical Account Manager**: Acts as the Socure solutions implementation specialist, providing training on solutions, guidance on SocureGov calibration settings, and expertise on technical aspects of integrating into the client environment. • **Strategic Account Manager**: Once the contract has been signed, the Strategic account manager (SAM) is the lead account manager for the customer. SAMs help customers build successful, long-lasting journeys with Socure by helping them customize, scale and adopt technological changes and proactively links customers to Socure resources when needed.

G09	Ongoing Operation	Propose a structure/framework for providing jurisdiction and management over the operation of services. The proposed structure/framework should describe roles, responsibilities and forums for decision making. Include descriptions of the identification process for issues, the resolution process for issues, and the process for escalations of issues into the governance structure.	Y	Socure's empowers our customers to take the primary role in jurisdiction and management over the operation of services.
G10	Demo Availability	Provide a weblink for a demo of the proposed solution/software. This weblink should be available throughout the life of the contract.	Y	Socure can create a demo meeting the requirements of this RFP and make it available for anytime retrieval. Demos and Data Studies are important practices that Socure engages in to prove our value over other solutions with a 90% success rate. Socure is ready to engage with VITA and provide the type of demo or study that provides the most value to your procurement effort. We find that collaborating with you to prove our performance for your populations using a data study is incredibly effective. This approach results in real outcomes that quantify the hours saved, reveal Ux impacts (such as rates for no friction, some friction, or transaction declined), and fraud detection that escapes the current process. Socure would gladly create a demo and do a data study to prove our value.
G11	Additional Capabilities	Propose additional services that are not referenced in the RFP requirements that will provide additional value to the Authorized Users and End Users. Describe any additional services.	Y	**Digital Intelligence and Entity Profiler** - Socure's Digital Intelligence Suite brings together cutting-edge solutions to protect your organization from sophisticated fraud attacks by combining device intelligence, behavioral analytics, and an entity profiler that provides an online digital footprint of user activity. Digital Intelligence uses information about the device and the connection to provide threat signals that cannot be detected analyzing PII alone. **Alert List** - Socure's contributory and proprietary service built to notify clients of the confirmed and declined identities that are reported by thousands of other customers across the Socure consortium. Alert List is continually refined using hundreds of millions of known outcomes processed by our platform each month. **Negative Positive List** - The Negative/Positive List module enables your organization to establish personalized lists of unique data elements known to be linked with either positive, negative or suspected negative identities, and utilize them for decision-making purposes. **Deceased Check** - Enables a check on a consumer's identity details to receive vital status information, such as whether the provided PII corresponds to a deceased individual. This module facilitates real-time and batch deceased checks beyond standard Customer Identification Program (CIP) verification, leveraging Socure's top-tier identity resolution techniques and the most precise deceased data in the market. **Progressive Onboarding** - The modular nature of the SocureGov platform easily supports multi-check identity proofing use cases. Many times it is critical to support the resident population by making it easy to create an account using minimal PII (such as full name, email address and date of birth). When the resident then applies for a benefit that has financial implications a more stringent identity verification check can be performed. **SocureID** - A persistent unique identifier that allows you to easily deduplicate identities across your existing customer base, ensuring smooth onboarding regardless of potential identity manipulations. **Call Center: Admin Dashboard** - The Socure Administrative Dashboard provides a role-based user interface which can be used for call center operations. Agents can search for and view

Security Requirements					
Req. No.	**Category**	**Requirement**	**Yes (Y) Future (F) No (N)**	**Provide an explanation of how the Solution fulfills the requirement. The Supplier's detailed explanation should not simply be an affirmative reiteration of the question, but should describe the manner in which the requirement is met. Where possible and beneficial, please provide screenshots or graphics to help illustrate your response. Where your response is described as a future release or update as the provision, please provide a timeline for that provision. Supplier may also use this column to cross-reference a detailed explanation included as an attachment to its proposal.**	Redaction Rationale
General Security Requirements					
The Supplier's responsibilities include:					
SEC01	Security	Ensure the Solution complies with Commonwealth security policies and standards, VITA Rules, and all Customers' individual Information Security Policies and applicable Federal standards (e.g., FedRAMP moderate or high, SEC530, CJIS, FISMA, PCI, ISO27001, FERPA, FTI (IRS PUB-1075), SSA, HIPAA-HITECH and any updates to these listed standards.)	Y	The SocureGov platform has been designed, built, and assessed against FedRAMP Moderate control requirements by a FedRAMP-approved Third Party Assessment Organization (3PAO). Our fully hosted (AWS) cloud platform has been assessed against and currently complies with the following industry security standards: StateRAMP Moderate (Authorized), TX-RAMP Moderate (Authorized), System and Organization Controls (SOC) 2 Type 2, International Organization for Standardization (ISO) 27001, 27017, 27018, 27701, Web Content Accessibility Guidelines (WCAG) 2.1 Level AA, and NIST Identity Assurance Level 2 (IAL2). Socure is compliant with FedRAMP requirements and has been assessed by a FedRAMP-approved third-party assessor (3PAO) as compliant with FedRAMP security controls. As a result, Socure has been listed on the FedRAMP website as "In Process" for FedRAMP Authorization. Therefore, Socure has taken all the necessary steps to be FedRAMP Authorized and is currently awaiting final approval from the Federal government.	
SEC02	Security	Grant access to specified systems, services, and/or other technologies to the Chief Information Officer and the Chief Information Security Officer for the Commonwealth of Virginia, or an identified designee with credentials upon request.	Y	The CIO and CISO can be provided access by a VITA resource who has user management permissions for the VITA account. Socure empowers our customers to manage application, risk & user access through the SocureGov Administrative Dashboard. This dashboard serves as a centralized location to view details related to past transaction analysis, manage the onboarding solution calibration, provide self-service tools for development & integration, and manage user & role access and permissions.	
SEC03	Security	Ensure the Solution is supported and maintained by US Citizens or those legally allowed to work in the US.	Y	Access to the SocureGov environment and system resources is restricted to only U.S. persons (Permanent Resident or citizen as defined by the U.S. Department of State).	
SEC04	Security	Ensure the Solution is housed within a container reserved for the exclusive use of the Commonwealth. All storage, backups, and replication, must remain within the US. See PE-18-COV within SEC530.	Y	SocureGov is hosted on AWS Govcloud, comprised of two physically and logically isolated U.S. sovereign regions. It is verified for use by U.S. government agencies and entities. Only U.S. persons (Permanent Resident or citizen as defined by the U.S. Department of State) have access to the environment. Because SocureGov is a SaaS offering, it is not designed to be completely containerized for the exclusive use of the Commonwealth. Socure employs logical separation with separate encryption keys for each customer and a suite of other controls to segment data provided by our customers on the platform. We would love to discuss our approach with the Commonwealth further.	
SEC05	Security	Ensure all User activity and System administration activity is logged.	Y	[redacted]	Sensitive Security Information

SEC06	Security	Ensure all logged Events are provided to the VITA Managed Security Service Provider for analysis in a VITA approved format utilizing a VITA approved automated method. Ensure VITA Agencies logged events are provide for Agencies view and use.	Y	Socure stores all logs related to dashboard events and utilizes this information internally to identify security related issues. Socure will work with VITA to determine the best mechanism to support transparency in the ongoing administration of the dashboard, and how best to partner with the Commonwealth on this requirement.	
SEC07	Security	Ensure that all Commonwealth Data remains in the United States and all Sensitive Data remains encrypted at rest and while in transit.	Y	[redacted]	Sensitive Security Information
SEC08	Security	Ensure a Commonwealth Security and Risk Management approved key management solution is used within the solution in accordance with VITA Rules.	Y		Sensitive Security Information
SEC09	Security	Ensure that encryption allows for Time-based revocation of access/encryption keys based on the schedule defined by VITA and VITA Customers.	Y		Sensitive Security Information
SEC10	Security	Ensure that Encryption allows for User-based revocation of access/encryption keys.	N	Access to encryption keys is managed through SSO group membership. Users' access can be revoked by removing them from the SSO group.	
SEC11	Security	Ensure that all data associated with the Solution is encrypted in transit and at rest between services and Systems.	Y	[redacted]	Sensitive Security Information
SEC12	Security	Ensure that all encryption mechanisms in use by the solution are compliant with FIPS 140-3.	Y	Encryption mechanisms are accordance with our FedRAMP Moderate control requirements. Socure currently uses FIPS 140-2 validated modules certified at FIPS 140-2 Level 3 and will develop a migration plan to upgrade to FIPS 140-3 validated versions when available.	
SEC13	Security	Establish and maintain mechanisms and notifications to safeguard against the unauthorized access, destruction, loss or alteration of Customer's data per VITA Standards.	Y	The SocureGov platform has been designed, built, and assessed against FedRAMP Moderate control requirements to protect customer data. The solution is StateRAMP Authorized and is currently In Process for FedRAMP Authorization. As such, our customers generally find that our security standards meet or exceed their security policies.	
SEC14	Security	Utilize controls and processes such that the Services are compliant with all VITA Rules for the processing, storage, and transmission of information based on its classification and impact categorization, and ensure that Authorized User(s) is able to gain assurance and evidence that such compliance is being maintained upon request.	Y	The SocureGov platform has been designed, built, and assessed against FedRAMP Moderate control requirements. The solution is StateRAMP Authorized and is currently In Process for FedRAMP Authorization. As such, our customers generally find that our security standards meet or exceed their security policies.	
SEC15	Security	Disable or delete accounts in accordance with VITA Rules for standard expiration (e.g., 90 days without use) or promptly as requested.	Y	Socure disables Customer Dashboard accounts that have been inactive for 90 days. For the Scoure production environment, accounts are disabled after 90 days of inactivity.	
SEC16	Security	Ensure that Solution logs all access attempts (successful / unsuccessful) by an administrative user or by personnel supporting the solution from any service provider associated with the Solution and that the logs are automatically forwarded to the VITA Managed Security Services Provider for analysis.	N	As part of our FedRAMP Authorization, Socure cannot provide data feeds to VITA unless it is to a FedRAMP authorized system. Socure auditing functions are documented and compliant with FedRAMP Moderate requirements. Socure continuously aggregates logs from all components within the authorization boundary and logs all access attempts (successful / unsuccessful) by an administrative user or by personnel supporting the solution. Socure does not automatically forward logs to its customers. FedRAMP security restrictions prohibit direct interface with outside systems. Socure would like to discuss with VITA what methods would be available to satisfy this requirement.	

SEC17	Security	Ensure that Solution logs all actions taken by an administrative user or by personnel supporting the solution from any service provider associated with the Solution and that the logs are automatically forwarded to the VITA Managed Security Services Provider for analysis.	F	User activity logs can be viewed and downloaded from the Admin Dashboard. Integration to forward event logs is not currently available but could be added to the roadmap. Socure would like to discuss with VITA what methods would be available to satisfy this requirement. Socure anticipates it could work with VITA to satisfy this requirement by Q1 of CY 2025 depending on VITA's availability and guidance.
SEC18	Security	Ensure that no personnel supporting or administrating the Solution can alter or	Y	Log files cannot be altered or deleted anywhere in the SocureGov environment. The
SEC19	Security	Ensure that no personnel supporting or administrating the Solution can alter or	Y	The SocureGov platform has been designed, built, and assessed against FedRAMP Moderate
SEC20	Security	Ensure there are no shared accounts and that each account (human or service) is	Y	Socure does not use shared credentials in the SocureGov environment requires unique
SEC21	Security	Supplier's Solution is approved through the VITA COV Ramp process. https://www.vita.virginia.gov/cov-ramp/	F	Socure assumes that VITA will sponsor the solution for the VITA COV RAMP process as part of the onboarding process for this contract. SocureGov has been designed, built, and assessed
		Incident Response Security Requirements		
		The Supplier's responsibilities include:		
SEC22	Security	Participate in the incident response process as required by VITA and its	Y	Socure has teams in place to provide customer support, handle incidents, and participate in
SEC23	Security	Report status of the incident and mitigation activities to VITA once every 24-hours	Y	All incidents impacting customers are posted and maintained on Socure's Status Page,
SEC24	Security	Provide data feeds or reports to VITA's Security Incident and Event Correlation Systems for purposes of deep analytics in accordance with VITA Rules to support VITA's analysis as requested.	N	As part of our FedRAMP Authorization, Socure cannot provide data feeds to VITA unless it is to a FedRAMP authorized system. Additionaly, SocureGov is a multi-tenant cloud service. As such as we cannot share all the security events and logs with external parties. VITA specific transactions and user activity logs are available for download from the Socure Administrative Dashboard. Socure would like to discuss how we can satisfy this requirement with the Commonwealth through scheduled reporting.
		Security Integration		
		The Supplier's responsibilities include:		
SEC25	Security	Perform or Integrate with current and future COV Enterprise Cyber Security services, including those of which are managed by VITA or other Service Tower Suppliers. This includes but is not limited to:	Y	Socure provides a SaaS offering within a FedRAMP environment that is accessed through an API gateway. As part of our FedRAMP Authorization, Socure cannot provide data feeds to VITA unless it is to a FedRAMP authorized system. Socure can provide information to satisfy requirements associated with some of the services below. Socure would like to discuss how
SEC25.1	Security	Event Log Management services (including incident management)	F	Socure provides a SaaS offering within a FedRAMP environment that is accessed through an API gateway. As part of our FedRAMP Authorization, Socure cannot provide data feeds to VITA unless it is to a FedRAMP authorized system. Socure would like to discuss how we can support the COV Enterprise Cyber Security services activites related to Event Log Management services (including incident management). Socure anticipates it could work with VITA to satisfy this requirement by Q1 of CY 2025 depending on VITA's availability and guidance.
SEC25.2	Security	Event Management System (SIEM service)	F	Socure provides a SaaS offering within a FedRAMP environment that is accessed through an API gateway. As part of our FedRAMP Authorization, Socure cannot provide data feeds to VITA unless it is to a FedRAMP authorized system. Socure would like to discuss how we can support the COV Enterprise Cyber Security services activites related to Event Management System (SIEM service). Socure anticipates it could work with VITA to satisfy this requirement by Q1 of CY 2025 depending on VITA's availability and guidance.

SEC25.3	Security	Security Orchestration, Automation, and Response (SOAR) service	F	Socure provides a SaaS offering within a FedRAMP environment that is accessed through an API gateway. As part of our FedRAMP Authorization, Socure cannot provide data feeds to VITA unless it is to a FedRAMP authorized system. Socure would like to discuss how we can support the COV Enterprise Cyber Security services activites related to Security Orchestration, Automation, and Response (SOAR) service. Socure anticipates it could work with VITA to satisfy this requirement by Q1 of CY 2025 depending on VITA's availability and guidance.	
SEC25.4	Security	Single Sign-on	Y	[redacted]	Sensitive Competitive Information
SEC25.5	Security	Identity Access Management Services	Y	Administratively, Socure supports SAML Single Sign-On with enterprise IAM solutions. Socure assumes that VITA will leverage the Commonwealth's SSO solution to seamlessly integrate user access to the Administrative Dashboard via SAML. With that design, VITA's Identity Governance protocols would be leveraged to identify issues and risks.	
SEC25.6	Security	Identity Governance services	Y		
SEC25.7	Security	Privileged Access Management (PAM)	Y	Socure empowers our clients to manage system user and role definitions through our self service Adminstrative Dashboard, including providing priviledged access management.	
SEC25.8	Security	Directory Services	Y	[redacted]	Sensitive Competitive Information
SEC25.9	Security	Vulnerability Management Service	Y	As part of our FedRAMP Authorization, Socure provides vulnerability reporting and other reports on a monthly basis to meet StateRAMP/FedRAMP Authorization requirements. Socure can provide the same reports to VITA to provide insight on our vulnerability management program and status.	
SEC25.10	Security	Key Management	Y	Socure empowers our customer to create their Client Keys via the Administrative Dashboard. Client keys can be managed autonomously through the dashboard to ensure the Commonwealth has full control over their API keys.	
SEC26	Security	Communicate and report any intrusion detected in the environment in accordance with VITA Rules.	Y	Socure will support VITA response to security incidents related to the operation of our service and provide logs or alert and event information as appropriate to support investigation of those incidents.	
SEC27	Security	Solution ensures all events required by VITA Rules be logged and forwarded to the VITA SIEM for review and analysis.	F	Socure provides a SaaS offering within a FedRAMP environment that is accessed through an API gateway. As part of our FedRAMP Authorization, Socure cannot provide data feeds to VITA unless it is to a FedRAMP authorized system. Socure would like to discuss how we can support the COV Enterprise Cyber Security services activites related to the VITA SIEM. Socure anticipates it could work with VITA to satisfy this requirement by Q1 of CY 2025 depending on VITA's availability and guidance.	
SEC28	Security	Solution will provide documented API integration with all VITA security tools.	F	Socure provides a SaaS offering within a FedRAMP environment that is accessed through an API gateway. As part of our FedRAMP Authorization, Socure cannot provide data feeds to VITA unless it is to a FedRAMP authorized system. Socure would like to discuss what VITA security tools require integration and how we can satisfy this requirement. Socure anticipates it could work with VITA to satisfy this requirement by Q1 of CY 2025 depending on VITA's availability and guidance.	
		Audit and Compliance			
		The Supplier's responsibilities include:			

SEC29	Security	Provide the non-redacted SOC 1 audit results to VITA and VITA Customers at least once every 12-months.	Y	SSAE 16 Type II (SOC 1) assessments are not relevant to the services Socure provides to its customers. Socure's financials are assessed by a third party auditor annually against US Generally Accepted Accounting Principles (US GAAP). In addition, the SocureGov platform has been designed, built, and assessed against FedRAMP Moderate control requirements by a FedRAMP-approved Third Party Assessment Organization (3PAO). Our fully hosted (AWS) cloud platform has been assessed against and currently complies with the following industry security standards: StateRAMP Moderate (Authorized), TX-RAMP Moderate (Authorized), System and Organization Controls (SOC) 2 Type 2, International Organization for Standardization (ISO) 27001, 27017, 27018, 27701, Web Content Accessibility Guidelines (WCAG) 2.1 Level AA, and NIST Identity Assurance Level 2 (IAL2). Socure is compliant with FedRAMP requirements and has been assessed by a FedRAMP-approved third-party assessor (3PAO) as compliant with FedRAMP security controls. As a result, Socure has been listed on the FedRAMP website as "In Process" for FedRAMP Authorization. Therefore, Socure has taken all the necessary steps to be FedRAMP Authorized and is currently awaiting final approval from the Federal government	
SEC30	Security	Provide the non-redacted SOC 2, Type II audit results to VITA and VITA Customers at least once every 12-months.	Y	Attached please find the latest SOC report attached separately in 8 Appendices Documents, Section 8.0 Additional Supplier Documents in Attachment SEC30 -Socure_-_2023_Type_2_SOC_2_-_Report	
SEC31	Security	Provide quarterly updates to Commonwealth Security on remediation steps taken for SOC1 and SOC2 Exceptions.	Y	SOC 1 is not applicable to Socure. If any exceptions are noted in SOC 2 are addressed during the ISMS committee meetings. Socure can provide updates on SOC 2 exception remediation activies upon request.	
		User Authentication			
		The Supplier's responsibilities include:			
SEC32	Security	Ensure that Solution provides single sign-on functionality.	Y	Yes, Socure supports federated SSO configuration. For instance, once user is redirected to the Federated SSO service (like Okta) they'll need to enter their Federated SSO/Okta credentials. A successful authentication request will redirect the user back to the Socure Dashboard Assertion Consumer Service (ACS) URL with an embedded SAML response from the Federated SSO/Okta.	
SEC33	Security	Ensure that Solution's authentication process integrates into COV Directory Service and tools.	Y	[redacted]	Sensitive Competitive Information
SEC34	Security	Ensure that the Solution can federate with the VITA approved single sign-on authority (e.g.; OKTA).	Y		Sensitive Competitive Information
SEC35	Security	Ensure that the Solution enforces interactive re-authentication at regular intervals as defined by VITA and its Customers.	Y	Socure's intuitive administrative dashboard provides a configurable User Interface (UI) to customize SP Session timeout for both Idle Session Sign-Out and Auto Sign-Out durations. VITA and its customers will have full control of sign-out configurations for each administrative account. Idle Session Sign-Out is triggered when the administrator is inactive inside of the account dashboard for the specified duration of time. Auto Sign-Out is the maximum session duration. Administrators will be logged out and forced to re-authenticate at the expiration of the Auto Sign-Out period.	

SEC36	Security	Ensure that the Solution will log and provide audit Events for all authentication attempts.	Y	Socure Dashboard provides an Account Activity Report which includes logged in user, IP address, timestamp and action performed, which can be downloaded as a csv/xls/tsv file by users with permissions	
SEC37	Security	Ensure that all logs are forwarded to a centralized repository of VITA choosing (SIEM).	F	Socure does not currently support log forwarding to a centralized repository for all transaction events. Audit events are stored and extractable via download from the Admin Dashboard. Transaction events for Document Verification and Monitoring Services are published via webhooks. SocureGov transaction responses to identity verification requests return with the full data payload supporting the transaction outcome. VITA can log this these responses as well.	
SEC38	Security	Utilize security clearance and access control processes to administer tools and environments used to support Authorize User's services for all staff.	Y	Socure offers a broad set of default User Roles that cover common use cases and the ability to create custom User Roles to meet your specific requirements. All default roles conform to limited access privileges and distinct controls for PII visibility. Socure supports username/password access and SAML SSO leveraging Okta, Salesforce, Google Workspace and Azure AD.	
SEC39	Security	Ensure that access privileges for Supplier Personnel are promptly removed upon departure in accordance with VITA Rules.	Y	Federated account actions can be accomplished through SAML SSO integration. VITA will also have full control over user access privileges at a fine-grained level from the Admin Dashboard.	
		Encryption at Rest			
		The Supplier's responsibilities include:			
SEC40	Security	Implement encryption at rest as required by VITA Rules.	Y	[redacted]	Sensitive Security
SEC41	Security	Provide the ability to perform a forensic analysis of the encrypted data.	N	Socure's FedRAMP certification restricts outside system access to our system.	
SEC42	Security	Ensure that the Device can be decrypted with the forensic software to support	N	Socure's FedRAMP certification restricts outside system access to our system.	
		Security Approach			
		The Supplier's responsibilities include:			
SEC43	Security	Security, compliance, encryption, auditing, and other InfoSec concerns should be	Y	Socure is dedicated to providing a secure SaaS offering to our clients. Socure takes	
SEC44	Security	Codify and implement security policies to enforce compliance and operational	Y	Socure has architected our system with a focus on automation and operational efficiency.	
		Security Management			
		Supplier's responsibilities include:			
SEC45	Security	Establish and maintain mechanisms to safeguard against the unauthorized access, destruction, loss or alteration of Customers' data.	Y	Socure data access is provided based on the principles of least privilege - only employees with a business need to know are provided access to customer data.	
		Security Assessment by Third Parties			
		Supplier's responsibilities include:			

SEC46	Security	Twice annually, participate in an independent SSAE 16 Type II assessment from a VITA approved firm, covering all aspects of the Managed Environment.	Y	SSAE 16 Type II (SOC 1) assessments are not relevant to the services Socure provides to its customers. As part of our FedRAMP conformance, Socure is assessed annually by a FedRAMP-approved Third Party Assessment Organization (3PAO). The 3PAO produces a Security Assessment Report (SAR) to describe their findings. We assume this assessment report will meet the requirements set forth herein. In addition, the SocureGov platform has been designed, built, and assessed against FedRAMP Moderate control requirements. Our fully hosted (AWS) cloud platform has been assessed against and currently complies with the following industry security standards: StateRAMP Moderate (Authorized), TX-RAMP Moderate (Authorized), System and Organization Controls (SOC) 2 Type 2, International Organization for Standardization (ISO) 27001, 27017, 27018, 27701, Web Content Accessibility Guidelines (WCAG) 2.1 Level AA, and NIST Identity Assurance Level 2 (IAL2). Socure is compliant with FedRAMP requirements and has been assessed by a FedRAMP-approved third-party assessor (3PAO) as compliant with FedRAMP security controls. As a result, Socure has been listed on the FedRAMP website as “In Process” for FedRAMP Authorization. Therefore, Socure has taken all the necessary steps to be FedRAMP Authorized and is currently awaiting final approval from the Federal government.
SEC47	Security	Assessments or audits of the Managed Environment may be conducted by VITA, Customers, the Auditor of Public Accounts, the Managed Security Service Tower Supplier, or by federal agencies with oversight responsibilities. Such assessments may include risk assessments, forensic analysis or audits (e.g., AICPA’s SOC 2, U.S. Internal Revenue Service 1075 audits, or risk assessments following NIST Special Pub 800-30 “Guide for Conducting Risk Assessments”) of the Services being provided by Supplier. These organizations reserve the right to define their own processes and methodologies to achieve their statutory goals. In such instances the Supplier shall:	Y	As part of our FedRAMP conformance, Socure is assessed annually by a FedRAMP-approved Third Party Assessment Organization (3PAO). The 3PAO produces a Security Assessment Report (SAR) to describe their findings. We assume this assessment report will meet the requirements set forth herein.
SEC47.1	Security	Participate in assessments of the Security Program and Services provided by the Suppliers.	Y	As part of our FedRAMP conformance, Socure is assessed annually by a FedRAMP-approved Third Party Assessment Organization (3PAO). The 3PAO produces a Security Assessment Report (SAR) to describe their findings. We assume this assessment report will meet the requirements set forth herein. Socure can provide additional evidence of compliance should the Commonwealth have additional questions about Socure's security program and services.
SEC47.2	Security	Cooperate fully with and provide any assistance required by VITA and the assessment organization in support of these assessments or audits.	Y	As part of our FedRAMP conformance, Socure is assessed annually by a FedRAMP-approved Third Party Assessment Organization (3PAO). The 3PAO produces a Security Assessment Report (SAR) to describe their findings. We assume this assessment report will meet the requirements set forth herein. Socure can provide additional evidence of compliance should the Commonwealth have additional questions about Socure's security program and services.

SEC47.3	Security	Provide access to any premises, equipment, personnel, documents, etc., as directed by VITA or any other entity conducting such assessments or audits.	Y	As part of our FedRAMP conformance, Socure is assessed annually by a FedRAMP-approved Third Party Assessment Organization (3PAO). The 3PAO produces a Security Assessment Report (SAR) to describe their findings. We assume this assessment report will meet the requirements set forth herein. Socure can provide additional evidence of compliance should the Commonwealth have additional questions about Socure's security program and services.
SEC47.4	Security	Recognize that VITA has sole discretion regarding acceptance or disputing any findings documented by such an assessment or audit.	Y	As part of our FedRAMP conformance, Socure is assessed annually by a FedRAMP-approved Third Party Assessment Organization (3PAO). The 3PAO produces a Security Assessment Report (SAR) to describe their findings. We assume this assessment report will meet the requirements set forth herein. Socure can provide additional evidence of compliance should the Commonwealth have additional questions about Socure's security program and services. Socure can also discuss and work with the Commonwealth to address any findings about which the Commonwealth has concerns.
SEC48	Security	If the report concludes that the Security Program does not meet or exceed the VITA Rules, then the affected Suppliers shall develop and agree upon an Action Plan to promptly address and resolve any deficiencies, vulnerabilities, concerns and recommendations identified in such report.	Y	Should the Commonwealth determine that Socure's Security Program does not meet the VITA Rules, Socure will work with the Commonwealth to develop an Action Plan to address and resolve any deficiencies, vulnerabilities, concerns.
SEC49	Security	Under no circumstances will Supplier attempt to persuade or control or otherwise influence the party conducting the Security Assessment.	Y	As part of our FedRAMP conformance, Socure is assessed annually by a FedRAMP-approved Third Party Assessment Organization (3PAO). Socure agrees that under no circumstances will Socure attempt to persuade or control or othrewise influence that 3PAO assessor.
SEC50	Security	Supplier acknowledges that VITA views the right to conduct assessments as a critical inducement to VITA's agreement to many of the terms of this Agreement, including the Term and termination rights provided for in the Agreement, and therefore Supplier agrees that it will cooperate in good faith to accomplish the objectives contemplated for the benefit of the Commonwealth.	Y	Socure acknowledges the importance for VITA to understand the security controls implemented in the SocureGov environment and the importance of independent assessment of those controls to confirm continued compliance. As part of our FedRAMP conformance, Socure is assessed annually by a FedRAMP-approved Third Party Assessment Organization (3PAO). The 3PAO produces a Security Assessment Report (SAR) to describe their findings. We assume this assessment report will meet the requirements set forth herein. Socure can provide additional evidence of compliance should the Commonwealth have additional questions about Socure's security program and services. Socure can also discuss and work with the Commonwealth to address any findings about which the Commonwealth has concerns.
		Security Incident Management		
		Supplier's responsibilities include:		
SEC51	Security	Security Incidents must be treated as Severity 1 Incidents.	Y	Any VITA security incidents that meet the definition of a Severity 1 Incident will be handled in accordance with the FedRAMP Incident Response Plan. Socure has a documented Incident Response Plan compliant with FedRAMP Moderate requirements. The SocureGov environment is continuously monitored and alerts are configured to automatically trigger if suspicious events or thresholds are detected. Alerts are investigated by the on-call Security Engineer who follows the Socure incident response process.

SEC52	Security	Upon identification of a Security Incident, or potential Security Incident, follow the escalation notification processes in accordance with VITA Rules.	Y	Socure will follow the escalation notification processes documented in Socure's Incident Response Plan, which is compliant with FedRAMP Moderate Incident Response requirements. Socure will notify VITA and provide information on incidents in accordance with our Incident Response communications requirements. Socure can discuss any delta between Socure's Incident Response Plan and VITA Rules.
SEC53	Security	Participate with designated parties to conduct a forensic investigation to determine what Systems, data and information have been affected by the Security Incident.	Y	Socure will support VITA investigations of incidents related to the operation of our service.
SEC54	Security	Provide any logs or alert and event information required to respond to Security Incidents.	Y	Socure will support VITA response to security incidents related to the operation of our service. SocureGov is a multi-tenant cloud service. As such as we cannot share all the security events and logs with external parties. Socure will work with the Commonwealth to provide the information necessary to respond to security incidents. In addition, VITA specific transactions and user activity logs are available for download from the Socure Administrative Dashboard.
SEC55	Security	Do not serve any notice or otherwise publicize a Security Incident without the prior written consent of VITA.	Y	Socure only provides notice to customers impacted by security incidents. Socure will not publicize information related to VITA about a Security Incident related to without the prior written consent of VITA.
SEC56	Security	Do not provide any information to outside sources (e.g., public, media, VITA or Supplier Personnel) of any Security Incidents without the prior written consent of VITA.	Y	Socure only provides notice to customers impacted by security incidents. Socure will not provide any information related to VITA to outside sources about a Security Incident related to without the prior written consent of VITA.
SEC57	Security	Cooperate with any law enforcement officials, regulatory officials, agencies or associations, where directed by VITA and with the consent of VITA.	Y	Socure's Security and GRC teams are responsible for coordinating and cooperating with external entities, including law enforcement officials, regulatory officials, agencies or associations, where directed by VITA and with the consent of VITA, during incident response activities. The procedures ensure timely and appropriate interaction with these officials to comply with legal and regulatory requirements.
SEC58	Security	Provide a summary of all Security Incidents related to the Services and Commonwealth Data to VITA, upon the request of VITA, for all Security Incidents since Commencement.	Y	If necessary, Socure can provide a summary of security incidents related to Commonwealth Data and the Services provided to VITA

Identity Verification					
Req. No.	**Category**	**Requirement**	**Yes (Y) Future (F) No (N)**	**Provide an explanation of how the Solution fulfills the requirement. The Supplier's detailed explanation should not simply be an affirmative reiteration of the question, but should describe the manner in which the requirement is met. Where possible and beneficial, please provide screenshots or graphics to help illustrate your response. Where your response is described as a future release or update as the provision, please provide a timeline for that provision. Supplier may also use this column to cross-reference a detailed explanation included as an attachment to its proposal.**	
Identity Verification Requirements					
The Supplier's responsibilities include:					
IDP01	Identity Verification Methods	Verify and validate the End User's identity. Please describe the entire process, including any relevant diagrams to illustrate it.	Y	There is more response than is viewable. The SocureGov platform is built upon a best-in-class approach that analyzes and correlates facets of an individual's PII, to verify and validate the end users digital identity, eanbling equitable and inclusive access to public programs. End Users input PII to be validated and assessed by SocureGov's fraud detection models. If an elevated risk of fraud is detected, or if an IAL2 process is required, Socure will present the End User with the opportunity to verify their identity via Document Capture and Liveness detection. The End User will user their smart phone device to capture images of identity evidence, along with a selfie for submission to our DocV solution. If needed, Socure will provide remediation processes for End Users who do not possess the necessary identity evidence, or are unable to provide it at this time. Remediation could include Trusted Referee services both virtually and in-person. Our comprehensive identity verification platform that combines advanced machine learning and artificial intelligence with analytics and unrivaled data coverage to deliver the industry's most accurate and inclusive solution for validating qualified applicants. Socure's Decision Module provides a seamless way to orchestrate the breadth of Socure risk scores and reason codes to a client following an identity proofing transaction. Socure hosts the decision module and uses a client's set risk threshold to help automate decisions to accept, reject, review, resubmit, or refer individuals in an identity proofing workflow. Socure's Sub-accounts provide the capability to manage multiple Decision Modules to use different levels of verification based on the identity assurance level assigned, and the application that triggered the request as defined in this RFP. Socure's solutions are fully automated—accessible via a single, RESTful API and can be implemented to serve online, call center, and in-person use cases. Once fully integrated, the customer will have access to the following product modules: • Socure Verify/Identity Verification – purpose-built IDV module that searches and correlates data ingested from authoritative sources such as Credit Bureau, Mobile Network Operators, Mobile Virtual Network Operators, Utility Data, Higher-Education, Socure's proprietary database of known good and bad identities, Banking data, Payroll Data, Student data, Device and IP geolocation and Tax Records to return the best-matched identity. Our proprietary set of U.S. data sources enables us to uniquely resolve more than 90% of the U.S. population. Socure's platform provides comprehensive population coverage with 9 billion records, using complementary and redundant data sources.	Please see Tab "IDP01 - Verification Process" for Diagram
IDP02	Unique Identifier	Return information to the Authorized User when the Solution verifies the End User's identity. If yes, describe the information returned to the Authorized User.	Y	The information returned when an end user's identity has been verified include an overall decision, scores, risk and information codes, and correlation scores in a JSON format depending on the SocureGov platform modules requested. If further verification is required after the risk decision, the automated Document Verification of the End User will also result in a JSON response including a decision and results from the validation of the identity documentation evidence provided. SocureGov platform offers over 700+ unique reason codes to inform the Authorized User of the factors which informed the risk scores and decisions delivered.	

IDP03	Claimed Identity Data	Associate and pass back to the Authorized User the claimed identity of the End User. Provide details about the metadata that is shared with the identity management solution about the Identity Verification event. (The metadata should include the date when Identity Verification was completed, the identity assurance level assigned, the name of the application that triggered the request for Identity Verification, a description of the document(s) used for Identity Verification, whether the Identity Verification was satisfactorily completed or not, and if disapproved, the reasons for disapproval.)	Y	[redacted]	
IDP04	Identity Assurance Levels (IAL)	Employ methods to prove the End User's identity to Assurance Level 1 as defined in the Definitions tab of this workbook. Please explain those methods.	Y	Socure takes a disciplined approach to validating identity information at each IAL level. For all IAL levels, Socure applies a uniquely layered approach to validating the PII provided in any transaction. The data entered by the applicant is used as an indicator to records held by Socure that confirm the data provided is all associated with the claimed identity. Our first step to validating an identity. The Verify module is used to resolve a best matched entity from our data inventory that aligns with the PII provided. These continuously updated data sources are aggregated from a broad array of authoritative data sources across the applicant's entire identity, including consumer records (e.g., utilities, financial institution records, etc.), along with traditional sources, such as offline credit header and insurance data. These records are continuously refreshed to provide data accuracy and recency. By using data from multiple authoritative sources consolidated, Socure has high confidence in the best matched entity and can validate the PII attributes. Once the Verify module has determined the identity exists, the platform performs analyses of the data entered by the applicant and collected during the transaction (e.g., name, address, SSN, DOB, phone, geolocation data, IP address) and correlates that data to evaluate if it belongs together and indicates the strength of the relationship between the various data elements. Any anomalies are flagged as potential risks. In addition, the platform performs an analysis to determine if any data associated with the claimed identity has been used in a fraudulent transaction. This analysis helps uncover whether the claimed identity has been involved in identity theft, demonstrates indicators of a fraudulent transaction, or is likely a synthetic identity. See Tab “IDP04 - Account Creation” for diagram.	See Tab “IDP04 - Account Creation” for diagram.

IDP04.2		Employ methods to prove the End User's identity to Assurance Level 2 as defined in the Definitions tab of this workbook. Please explain those methods.	Y	There is more response than is viewable. Socure's entirely automated risk-based IAL2 onboarding process is listed as an approved component service on the Kantara Trust Status List (https://kantarainitiative.org/trust-status-list/). It leverages passive verification of an applicant's PII, matched with an easy-to-use document verification. This process has allowed similar public programs to disposition 100% of applications without employee intervention. Socure's Kantara-certified NIST SP 800-63 IAL2 remote unsupervised proofing process involves passive / active identity and fraud analytics to verify the identity of the individual. As a RESTful API that can analyze information and provide responses in under 400ms for passive checks, agencies will own onboarding/application process design and administration. This allows agencies to build trust with constituents that PII being collected is being done so in line with agency policy, the autonomy to update the experience without implication to the identity and fraud program and efficiency from a technology management operations perspective. Once an agency collects consent and the core PII elements (name, address, social security number, phone number, date of birth and/or email address, the agency will transmit the information to Socure with the information for the SocureGov platform to begin the process. Socure meets the requirements of NIST SP 800-63 IAL2 for remote unsupervised identity proofing as evidenced by our Kantara IAL2 certification. Additionally, the Socure team has engaged extensively with NIST to inform the upcoming requirements in the NIST SP 800-63-4 update. During remote unsupervised proofing, the applicant provides a First Name, Last Name, DOB, SSN, Phone, and Address and provides their consent for Socure to use the data. The SocureGov platform confirms the identity associated with the phone number or other data and sends a link to the number associated with the mobile device, which is then used to collect images of identity documents (e.g., driver's license or passport) and perform liveness checks of a selfie photograph. The platform also conducts a number of identity document authenticity checks. This link expires within 10 minutes. Only the minimum data necessary to uniquely resolve an identity is requested of the applicant. Once the platform has verified both the authenticity of the identity and the identity document, it analyzes the liveness checks to confirm that the individual in possession of the device matches the photo on the identity document, binding the identity to the individual to the device. An agency will own onboarding/application process design and administration. This allows the government to build trust with
IDP04.3		Employ methods to prove the End User's identity to Assurance Level 3 as defined in the Definitions tab of this workbook. Please explain those methods.	Y	Socure assumes that providing remote supervised identity proofing conformant to IAL3 through trusted referees is sufficient to VITA's requirements. For IAL3 required use cases, or in the event that an end user is unable to complete the automated IAL2 process, Socure provides a seamless digital Trusted Referee workflow in which users can join a waiting room to be met with a qualified person immediately. If more time is needed, users can schedule appointments for a digital meeting with the qualified trusted referee. If the government does require an in-person IAL3 flow, Socure has existing case management capabilities to support in-person verification activities.

IDP05	Concurrent sessions	Provide the number of concurrent sessions and/or End Users that Supplier's Solution supports.	Y	SocureGov is built on AWS GovCloud and is designed for high availability and scalability and can support an increasing number of concurrent identity proofing transactions. The solution can be integrated with other solutions to provide support for an increasing number of concurrent authentication transactions. Socure can scale up or down to meet each customer's needs and has a proven track record of supporting the largest companies with the highest volumes in the world. Our customers range from thousands of transactions a year, to tens of millions. For example, we supported a number of existing customers this year during Superbowl LVII to support spikes in identity proofing and account changes. Generally, we require at least 2 weeks advance notice to confirm the infrastructure is ready to support unplanned spikes in identity verification transactions - this is best done by working regularly with our customers to understand their use cases and changes resulting from seasonality or other compelling events.

IDP06	Handling of PII	Supplier's Solution does **not** store End Users' personally identifiable information (PII) (e.g., name, date of birth, image of face from document/chip, selfie image, biometric data) beyond the lifetime of the validation workflow. If no, describe how the data is stored and the security controls in place to protect it.	Y	[redacted]
IDP07	Data Consent for Minor Child	Allow a parent to provide consent for a minor child to process the child's data consistant with Virginia FERPA laws. https://www.doe.virginia.gov/programs-services/student-	Y	Socure's services have the benefit of not requiring the use of FERPA data. We have assumed this requirement is therefore not applicable.
IDP08	Data Minimization	Adhere to the principle of data minimization, i.e., the processing of PII is limited to the minimum necessary to validate the existence of the claimed identity. Explain how your Solution only processes PII for the purpose of Identity Verification and enrollment, including identity attributes, biometrics, images, video, scans, or copies of identity evidence. If used for other purposes, please explain.	Y	There is more response than is viewable. Socure supports the entire range of digital identity verification, from progressive onboarding to full PII submission based on the level of verification needed. It is common to let user create an account with as little PII as: -First name -Last name -Email address With this progressive onboarding scenario, Email Risk and Correlation Scores predict the risk of an email and its correlation to an identity considering hundreds of data elements. Email addresses are correlated with a user's name to establish the prior history and patterns using advanced analytics. Predictive factors include deliverability, legitimacy of host, age of the email, and evaluation as possibly being auto generated by a bot. The Decision Logic module encapsulates any combination logic with other modules, such as device information or IP address to greatly enhance the efficacity of the response with such small amount of PII. For a more complete digital identity verification, it is recommended to provide: -Physical address (full street, city, state, Zip) -Phone number -Email -Date of birth -SSN or ITIN -Device information (via Digital Intelligence Suite) -IP address With these additional PII elements, not only can the Socure Verify module authoritatively confirm that the information matches to an existing individual, but the entire fraud suite can show different aspects the risk of stolen identities, synthetic identities,
IDP09	Appeals Process	Provide the End User with an appeals or dispute resolution process for contested errors in the Identity Verification process that resulted in an Identity Verification rejection. Explain the process presented to the End User, including options for corrections, contacting the proposed Solution provider, legal assistance, etc.	Y	Socure designs its offerings to function as an integrated part of the State's existing user experience. Socure assumes that the state will continue to maintain direct user interface / engagement with customers so as not to create a jarring experience with a third party company. For contested efforts, Socure provides customers with tools such case management to help faciltiate review processes. For every identity verification transaction, the solution provides a set of reason codes that provide explainability around identity verification decisions to better inform the state's processes.
IDP10	Data Privacy Risk Assessment	Conduct data privacy risk assessments. If yes, what is the frequency of those assessments. What action(s) do you take to accept, mitigate, or share any risks found? How is this information reported to the Authorized User?	Y	[redacted]

IDP11	Document Data Extraction – NFC	Provide mobile software development kits (SDKs) that support using near field communication (NFC) to read radio frequency identification (RFID) chips in identity documents where they are present under the ICAO 9303 standard. https://www.icao.int/publications/pages/publication.aspx?docnum=9303	Y	Yes, SocureGov supports using NFC to read RFID chips in identity documents under the ICAO 9303 standard, facilitated through our proprietary Socure SDKs. This integration allows for secure and efficient verification of biometric travel documents such as ePassports, confirm that the electronic data matches the printed information. Our NFC reading capability is entirely developed in-house, leveraging our own proprietary technology within the Socure SDKs to provide full control over security and functionality. This proprietary approach enables a high level of compliance with international standards and provides robust protection for sensitive personal data.
IDP12	Document Data Extraction – Barcode	Extract identity data from the PDF417 barcode used on many identity documents.	Y	SocureGov effectively extracts identity data from the PDF417 barcode found on many identity documents. Our technology goes beyond basic barcode reading; over the years, we have extensively studied the specifications of issuing documents, gaining deep insights into both the consistencies and inconsistencies that appear within barcode specs for each credential type. This knowledge is crucial in identifying anomalies that may indicate fraudulent activities, such as when a bad actor creates a counterfeit or overly perfect barcode. Moreover, Socure holds patents related to barcode technology, which significantly enhances our capability in this area. One such patent involves the enhancement of blurry barcodes using GenAI reconstruction techniques, allowing us to recover and accurately read data from barcodes that would otherwise be too degraded for standard readers. This is especially useful when a picture of the barcode is imperfect because of glare or normal wear and tear of the document. In these cases, the barcode reconstruction model enhances the barcode to drive super resolution to confirm it can be used for document verification purposes where the barcode could not be read prior. We analyze built-in mechanisms in the barcodes, such as redundancy, check digits, start and stop patterns, error detection and correction, etc, to confirm that a barcode is read correctly and conveys the right information. Another patent covers the detection of fraud signals specifically extracted from the PDF417 barcode and its metadata, providing a sophisticated layer of fraud detection that leverages deep insights into the barcode's structural and content-based peculiarities. These innovations underscore Socure's commitment to advanced document verification, ensuring high accuracy and security in identity validation processes.
IDP13	Data Sources	Data Sources	Y	Socure maintains established, proprietary integrations with numerous strategic data partnerships ranging from government databases, to credit bureau agencies, and several alternative credit providers, developed over years of trusted partnerships. We maintain stringent legal and compliance protocols to enable secure and responsible data access. Furthermore, we are actively expanding our connection network to provide even broader coverage and enhanced services to our clients. Data sources are carefully curated by Socure and their consortium members over the course of the last 12 years. It includes

IDP14	Identity Verification Methods	Verify and validate the End User's identity via remote digital channels, where an image or video of a passport, driver's license, or an identity document with a photo is captured via a mobile phone camera or webcam. Explain the process and include any relevant diagrams to illustrate the process.	Y	Automated processes are used for verifying documents in the DocV module and the process is supported by our fraud investigations team. DocV is a fully automated, omni-channel document verification solution. It applies advanced analytics to quickly confirm the authenticity of many identity documents in circulation. DocV combines the power and scale of computer vision and ML to provide greater accuracy across a broad set of demographics. Its features include OCR for data extraction, automated image capture, and predictive signals for risk assessments conformant to NIST 800-63 identity assurance levels. See Tab IDP14 - Predictive DocV The image capture app provides an intuitive guided user experience, correcting for blur, glare, and low-light situations, so suitable images that will pass security checks can be taken on the first try. The frame-finder detects appropriate documents or faces for a self portrait to help prevent photos of any other subject matter and, further, auto fires the shutter to capture the image when the conditions are right. Optical character recognition (OCR) extracts data from the front of the document which is then matched with data extracted from the barcode or machine-readable zone (MRZ) on the back of the document. If a self-portrait is captured, the self-portrait is compared to the photo on the identification card to confirm a match. In this way, physical identification and identity data are validated together for a holistic judgment. The Socure DocV solution does not employ 1:N verification. DocV incorporates predictive signals to determine the risk associated with each identity transaction. Device, phone, and address data (when provided by a government customer) are validated against a library of indicators, such as phone to name correlation, address to name correlation, device first seen, and IP distance to a physical address. The solution employs hundreds of these signals as part of our risk-score decisioning to provide a holistic view of the identity to verify authentic users and help eliminate fraudulent attempts. Socure provides web and native software development kits (SDKs) to create a seamless consumer experience.	See Tab IDP14 - Predictive DocV
IDP15	Identity Verification Methods	Provide a remote, unattended IAL2 Identity Verification process without facial recognition. If yes, what technologies or methods are used and how do those technologies or methods demonstrably mitigate the risks of a remote, unattended IAL2 erification process?	Y	SocureGov's has the ability to provide passive verification at account creation and during account updates that will significantly reduce fraudulent ID creation without increasing friction on the end users. The single RESTful API call would use a combination of the tools below that would be completely transparent to the state resident as it occurs in less than 150 milliseconds. This involves analyzing, given PII, user behavior and device attributes in the background to verify identities without requiring overt user actions. This seamless process sets the foundation for a secure and unobtrusive user experience. In meeting IAL2 without a biometric, documents can be captured (both defined and unstructured) to determine overall evidence authenticity and correlation to the PII provided through the passive verification process. Additionally, the same platform can be called to check contact channel changes in an existing account such as email, phone, or address. These are risk moments where fraudsters attempt account takeovers.	

IDP16	Evidence Differentiation	Differentiate between different forms of identification (e.g., out of state driver's licenses, college IDs, etc.) and ensure it is customizable so that an Authorized User can specify acceptable and unacceptable forms of identification. If yes, how does Supplier's Solution do this? Include any relevant diagrams to illustrate the process.	Y	SocureGov's DocV platform provides coverage for 95%+ identity evidence documents issued by a tribal, state or federal entity and has demonstrated the ability to authenticate 99% of quality images for documents issued by those entities. Global coverage continues to expand with the capability to add country-specific IDs in less than 5 days. In addition to U.S. identity documents (e.g., State Issued IDs, Driver's License, Passport, Tribal IDs), the offering provides coverage for international passports, ICAO-compliant travel documents, Mexican Election Cards, and Canadian Drivers licenses and health cards, enabling ever-expanding reach to underserved individuals and communities. Socure provides global document coverage in 180+ countries. A document with the detailed information is attached. Document Types: Customers can customize the display and availability of document types during the capture process. For instance, they may choose to exclusively present the option for License Document Type, omitting the selection between licenses and passports. Additionally, Socure offers configuration options to specify the types of documents customers wish to accept. For example, if a customer prefers to only accept US-based documents and US passports, Socure will provide a reason code to justify acceptance decisions. Customers can then configure different decisions based on the reason code using Socure's Decision Logic configuration on the dashboard.
IDP17	Document Types	Provide information regarding coverage with respect to countries and document types supported.	Y	[redacted]
IDP18	Image Optimization	Provide real–time feedback (e.g., too dark, too light, too blurry) to help an End User optimize an image. If yes, how many granular reasons can be returned? Does this apply to both auto-capture and manual capture?	Y	
IDP19	Document Error Correction	Offer options to the End User to fix a rejected document that was uploaded during the Identity Verification process. If yes, describe the process, the number of attempts allowed, and any other resolution steps.	Y	
IDP20	Image Quality	Provide information about the percentage of End Users required to take a second or third image due to inadequate quality in the first image.	Y	
IDP21	Drop Out Rate	Provide information about the percentage of current/past End Users that drop out during the image capture process within the proposed Solution's workflow.	Y	
IDP22	Document Tampering	Compare the text and image from a chip with the text and image from a picture taken of a document. If yes, how does Supplier identify document tampering?	Y	Yes, Socure performs both active authentication and chip authentication as part of our verification process to confirm that the chip in an identity document has not been cloned. The checks involve, Active Authentication (AA) by verifying that the chip contains a private key that matches the public key in the document and Chip Authentication (CA) verifying the cryptographic proof of chips itself. The text and image from the chip is compared with the text and image from the picture taken of a document. These security measures are critical in preventing the risks associated with cloned or tampered chips, enhancing the overall security and trustworthiness of the identity verification process. By implementing both AA and CA, Socure provides a robust defense against potential security breaches involving cloned chips.

IDP23	Image Comparison	Supplier's Solution must compare the End User's selfie taken during the erification process to the image from the picture taken of a document used for erification the image from a chip, or both. Explain picture comparison capabilities and if this process is configurable by the Authorized User.	Y	Socure DocV uses a biometric verification that compares document photos or a photo from an NFC chip with a live image of the presenter, including: ●Selfie to ID photo match ●Facial liveness detection (NIST PAD L2) ●Reduced bias machine driven decisioning ●Age discrepancy analysis The functions are embedded in the document verification process and are part of the analysis conducted after the VITA collects the information via the web or native app SDK.
IDP24	End User Experience	Supplier's Solution must instruct the End User in positioning their device and/or their document(s) correctly to successfully read the chip/document. If yes, describe the End User experience.	Y	Yes, Socure instructs the End User in real-time for both document and face image capture to assist users: 1. The system analyzes the lighting and provides prompts if the environment is too dark or too bright, ensuring that the document/face is clearly visible 2. Computer vision models continuously analyze the frames to detect blurriness. Users receive instructions to hold the device steady or refocus the camera, ensuring that the document/face is captured with the necessary clarity 3. Feedback includes prompts to adjust the document/ face position, ensuring it is fully within the frame, preventing issues such as cut-off edges or skewed images 4. Users are prompted to remove any obstructions like masks, ensuring a clear and unobstructed capture Quality Validation: Both documents and face images undergo server-based quality validation. If the captured images do not meet the required standards, users receive specific feedback to retake the images, minimizing the need for resubmissions.
IDP25	Multiple Identities	Confirm relationships of End Users who are associated with organizations such as LLCs, Corporations, or other types of organizations.	Y	Yes, we have capabilities to discern a Know-You-Business (KYB) relationship between a end user and organizations such as LLCs, Corporations, or other types of organizations.
IDP26	Attributes	Supplier's Solution must exclusively identify and match End Users. If yes, explain how this is accomplished.	Y	Socure identifies and matches End Users via **SocureID** is a unique persistent identifier, designed to view an identity holistically across an account, or sub-accounts. Creating an id that is unique based on an identity graph but unique for an account enables the Authorized Users to control and maintain privacy of the unique ids across a well defined set of accounts.
IDP27	Facial Recognition	Identify the End User by means of facial recognition technology. If yes, explain the process and include any relevant diagrams to illustrate the process.	Y	Yes, the Authorized Users can establish a revalidation flow using Socure's capabilities to support selfie re-verification for users who have previously been onboarded. By utilizing the previous transactionID or the customer's userID, you can reverify a user's identity solely through a selfie. During this process, users receive live feedback on positioning, angle, and lighting to provide an ideal selfie capture. This selfie is then compared to the headshot from the front of the ID used in the initial transaction, checked for liveness, and subsequently decisioned upon. The Authorized Users can configure this flow to determine how many attempts a user is allowed, and whether to trigger a document request if the original ID has expired, among other settings. From a performance standpoint, the true match rate for selfies is over 98%, ensuring a high level of reliability and user convenience.
IDP28	Duplicate Face Detection	Detect if the same face was used on multiple identity presentations. If yes, explain how this process is handled.	Y	[redacted]
IDP29	Identity Presentation Customization	Provide Authorized Users the ability to mark specific identity presentations as being fraudulent for the purpose of building a "watch list" of faces for checking against. If yes, indicate whether this is accomplished individually per Authorized User or batched for all Authorized Users.	Y	Yes, for the last 10+ years, Socure has allowed customers to offer feedback on individual transactions through various methods: by uploading a batch file via the dashboard, submitting data through an API, or directly within the Socure Case Manager. This feedback, once collected, is thoroughly analyzed by Socure's fraud investigation team. If the feedback indicates fraudulent activity, the relevant data is incorporated into Socure’s Alert List to enhance future fraud detection and refine the accuracy via model training sets and feature engineering to capture the new pattern we've possibly missed. This multi-channel feedback approach confirms that Socure’s systems continuously evolve to address emerging fraud patterns effectively. Socure has successfully built the industry's largest consortium database of known good and bad identities (2B+ rows of performance feedback data).

IDP30	Data Return	Describe what data, if any, the Solution returns to the End User after a document check and after a selfie check, and what data interchange format is used to return it. If yes, explain how this is accomplished.	Y	SocureGov's DocV user experience is fully customizeable and can be white labeled to match the text, color, and font of VITA's defined user experience. To maintain the integrity of VITA's verificatoin process, it is recommended that data detailing the result, risk score, and rationale surrounding a verification event remain viewable only by the commonwealth. **Data Interchange Format:** Webhooks use JSON format to return data, making it easy to parse and integrate with your existing systems. The data includes session details, document information, and verification results, ensuring you have all the necessary information for further processing. In summary, Socure's DocV provides comprehensive and real-time data through callbacks and webhooks in JSON format, ensuring a smooth and secure verification process with clear guidance and prompt issue resolution.
IDP32	In Person Authorization	Validate the End User's identity via in-person authorization by using certified documentation, fingerprints, etc. If yes, explain the process and include any relevant diagrams to illustrate the process.	Y	SocureGov solutions can be deployed to support in-person identity verification processes based on VITA needs. In the event that identity evidence cannot be validated digitally, or the end user has insufficient evidence to validate themselves digitally, and alternate path and user experience can be invoked in order to direct the end user to in-person channels for validation. There are many options for how this may be implemented and Socure appreciates the opportunity to further discuss the states desired implementation approach.
IDP33	Language	Support the use of multiple languages. If yes, provide a list of the languages supported.	Y	The DocV product currently supports the following languages in the capture experience: • English • Canadian French • Spanish • Simplified Chinese • Traditional Chinese • Brazilian Portuguese • Tagalog • Arabic • Korean • Vietnamese • Armenian Additional languages can be added with two weeks' notice.
IDP34	OCR Support	Support multiple languages for Optical Character Recognition. If yes, which languages are supported?	Y	Socure's DocV OCR system supports English, German, French, Spanish, Italian and Portuguese language extraction. Besides languages in Latin scripts, our OCR also supports Chinese, Korean, Japanese, Cyrillic, and Arabic scripts. We are constantly adding more languages to support for OCR this year using our new Document Understanding model. This model was built to be language agnostic from the start so can be quickly trained to add support for new languages and document types with very few samples to train on.
IDP35	Age Verification	Verify and/or return the age of the End User.	Y	Yes, Socure provides age verification. One of the main challenges in verifying consumer age is that individuals may provide false information or use fake identification documents to bypass age restrictions. Socure's solutions leverage artificial intelligence and machine learning algorithms to analyze various data points and identify potential fraud indicators, such as anomalies in user information or behavior patterns. Below are Socure's products that can help you effectively verify a consumer's age: • Socure Verify (KYC) — Global KYC and identity verification data. • Predictive Document Verification — Global identity document verification and anti-fraud. The solution checks for age discrepancies by comparing the document DOB with the assessed age of the selfie and credential photo. • Decision — Customize the default criteria and thresholds of risk that tell Socure to accept, reject or review a transaction.

IDP36	Mobile Solution	Allow End Users to use mobile phones, tablets, or other similar technology to access their applications.	Y	End users may use mobile phones, tablets, or other similar technology to access their applications. The SocureGov platform is supported by any web accessible user interface that is able to call our API endpoint. There is no limitation based on mobile device or desktop computer, and we do support MacOS, Windows, Linux, among many other platforms. Socure's Document Verification (DocV) capability currently supports all mobile browsers with more than a 1% browser share on https://analytics.usa.gov/
IDP37	Verification Error Rate	Provide information about Identity Verification error rates associated with the Supplier's Solution.	Y	[redacted]
IDP38	Accuracy Rate	Provide examples of what percentage of End Users successfully pass through the entire Identity Verification process. If yes, what variables would you describe as having the most impact on this?	Y	
IDP39	Identity Verification Equity	Provide a method(s) to proof user groups that do not possess the necessary minimum evidence to meet the requirements of a given IAL. If yes, how is that achieved? Include any relevant diagrams to illustrate the process. Examples of End User groups include: those without access to needed technology; persons with disabilities; persons who wear facial coverings for religious purposes; those with evidence that lacks the ability to capture different skin tones or facial features well enough to perform comparisons, etc.	Y	
IDP40	Demographic Bias	Supplier's Solution can track how false match rate (FMR) and false non-match rates (FNMR) in the presentation attack detection (PAD) and face comparison can vary across demographic groups (e.g., race, gender, age).	Y	
IDP41	Verification Time	Proof/verify the End User's identity in real time. If no, please provide/explain the erification time.	Y	Socure uses in-house data sources to prove decisioning on a user's identity **in real time** (under 150 ms). The in-house data sources avoid having to send PII outside of Socure to 3rd party vendors, thus limiting any risks to access to that PII. Part of this decisioning is Socure's Fraud Suite which provides an instant and near 100% accurate identity fraud decision in less than **150 milliseconds.**

IDP42	APIs	Provide APIs to the Authorized User to interface with applications and other systems. If yes, provide a list of your APIs including a short description of each.	Y	SocureGov modules are invoked via a single RESTful API endpoint. The SocureGov Endpoint will provide risk analysis, scores, reason codes and outcomes from the SocureGov Platform within a JSON API response. For additional capabilities, Socure's platform provides different API endpoints to interface with applications and other systems. • SocureGov Endpoint: The primary endpoint for identity verification scores, decisions, and analysis. As a modular endpoint, nearly all integrations use this endpoint in the workflow. For example, Predictive Document Verification customers will upload images using the SDK or Image Upload endpoint, then will retrieve results using this endpoint. • Reason Code Endpoint: Socure provides an endpoint that returns a list of reason codes used in SocureGov. A GET request with one optional parameter returns a list of all reason codes used by SocureGov. • Feedback API Endpoint: An endpoint for partners to send Sigma Identity Fraud, Sigma Synthetic, and Predictive Document Verification transaction data to Socure on a continuous basis. This information helps us train our machine learning models to improve fraud capture rates, lower the number of false positives, and reduce the number of cases requiring manual review. • Transaction Details Endpoint: Socure customers can retrieve previous transaction data via the Transaction Details endpoint. A GET request with a prior reference ID returns data on a previous transaction.	
IDP43	Identity Management Integration	Integrate with an Authorized User's identity management solution. If yes, describe how and provide any relevant diagrams to illustrate the process.	Y	Socure is based on a single RESTful API call to allow inclusion into any automation pipelines that support such calls. Integration with an identity management solution including but not limited to Okta, Ping, Forgerock, Microsoft, or any modern standards based solutioncan be fully integrated or performed side by side. See Attachments IDP43 Okta and Attachment IDP43 Forgerock as examples	See Attachments IDP43 Okta and Attachment IDP43 Forgerock as examples
IDP44	Fraud Detection	Employ methods to detect fraud (e.g., date of death) or fraud detection techniques (e.g., device fingerprinting). If yes, explain those methods and techniques.	Y	Socure's solution includes supervised machine learning models to classify and predict if an applicant is who they claim to be. These models use the collective intelligence and outcome-oriented performance feedback data provided by the company's clients to target patterns of fraud risk across multiple industries. Coupled with the Socure's proprietary identity graph which is informed by diverse data sources to help confirm proof of life, these fraud models provide an unparralled 360 degree view into the identity fraud risk of an applicant. Specifically, SocureGov includes the following products designed to detect and migitate fraudulent activities: • Sigma Identity Fraud – fraud risk module that employs machine learning models trained with 350+ predictors to detect the likelihood of third-party identity fraud. The model analyzes consumer identity dimensions—name, email, phone, address, date of birth, SSN, IP, device, velocity, network and behavioral intelligence, and more—and then further analyzes how these elements correlate to each other. • Sigma Synthetic Fraud – purpose-built and trained with consortium data to tackle fake and randomized synthetic patterns to produce highly accurate, real-time, actionable risk scores, and reason codes, with up to 90% auto-capture in the riskiest 3% of users. • Email RiskScore – predicts the risk of an email and its correlation to an identity considering hundreds of data elements. Using advanced analytics, email addresses are correlated with a user's name to establish the prior history and patterns. Predictive factors include deliverability, legitimacy of host, age of the email, and evaluation as possibly being auto-generated by a bot. • Phone RiskScore – predicts the risk of a phone and its correlation to an identity considering hundreds of data elements. Phones are correlated with a user's name to establish prior history and patterns using advanced analytics. Predictive factors include carrier legitimacy and velocity, phone number validity, and length of time a number has been linked to an identity. • Address RiskScore – predicts the risk of an address and its correlation to an identity considering hundreds of data elements. Addresses are correlated to a user's name to establish residency. Predictive factors include distance from phone area code, distance from IP address, and commercial versus residential address evaluation. • Digital Intelligence Suite - a multi-tiered service offering unified under a single API to enhance identity proofing and the risk analysis of every applicant based on technical and behavioral patterns. The module combines the Device Intelligence service that provides network and device-level data, our Behavioral Analytics service for the analysis of user behavior, and our Entity Profiler to provide historical profiles (digital footprints) at an individual PII element level to qualify applicant risk based on known	

IDP45	Hacking Detection	Provide the capability or policies to recognize patterns in behavior that might be hacking attempts (e.g., End User changing his password on a daily basis for several consecutive days, changing answers to security questions repeatedly, etc.). If yes, how do you notify the Authorized User's identity manager when these events occur?	Y	[redacted]	
IDP46	Evidence Assessment Document-Centric Fraud Detection	Validate the document-centric proof submitted by the End User for signs of tampering or counterfeiting. If yes, explain the process and include any relevant diagrams to illustrate the process.	Y	Socure's Predictive Document Verification module validates document authenticity by analyzing all aspects of the license including security features, holograms, and formats, as well as checks for tampering or counterfitting indicators. Socure uses a comprehensive strategy to determine the authenticity of IDs, leveraging thousands of data points collected from the images to distinguish real documents from fake ones and confirm the identity of the presenter. This strategy centers around the document capture process triggered when a DocV transaction is run. During a DocV transaction either a SMS link or QR code are used to launch a capture experience via a mobile device. The user is promoted to take pictures of identity evidence conforming to a given IAL. As images are captured, there is real time validation (for State IDs, Drivers Licenses, Passports, etc) to confirm that a high quality image was captured. Upon completion of the capture process a result is rendered. Specifically, DocV integrates the following technologies: • OCR Techniques: Advanced OCR extracts and verifies textual data against established standards, comparing PII in the form fields with data from the document or its barcode to spot inconsistencies. • Forensic Analysis and Machine Learning: ML algorithms inspect visual characteristics for tampering signs, such as altered text, headshot modifications, or security feature irregularities. Socure's patented barcode-based fraud detection technology focuses on PDF417 encoding, regenerating blurred or decayed barcodes. • Liveness Detection: The solution confirms the document isn't a photocopy or digital fabrication, checks the gyroscope level, and calculates camera angles to detect fakes. • Biometric Verification: Biometric verification compares document photos with a live image of the presenter, including matching a selfie to a headshot with NIST Level 2 Liveness for presentation attack detection (PAD). • Age Discrepancy: The solution checks for age discrepancies by comparing the document DOB with the assessed age of the selfie and credential photo. • Consortium Signal Assessment: Using Socure's cross-sector identity graph, the solution checks if the headshot on a credential has been linked to different PII on other credentials. • Passive Signal Enrichment: Socure enhances document assessment with passive identity signals, such as comparing PII linkage to the related device and the device linkage to the provided DL.	See attachment IDP14-PredictiveDocV

IDP47	Evidence Assessment Authenticity	Validate the authenticity of government issued credentials presented by a End User in the course of Identity Verification. If yes, explain the methodology, processes and procedures the proposed Solution uses.	Y	SocureGov's Predictive DocV enables the verification of **government-issued ID**s (driver's license, passport, photo ID card) utilizing facial biometrics and AI-powered decisioning. DocV provides distinct advantages, including passive fraud signals, customizable logic based on risk posture, a highly customizable user experience with minimal reliance on development teams (no code/low code), and an exceptional front-end capture experience with real-time quality checks (on-device and server-side). This confirms highly confident decisions with fewer resubmits and a response time under 2 seconds. This system is capable of confirming the authenticity of all 50 state ID documents, US Passports, as well as government issued documents from more than 180 different countries. For non-listed government issued ID cards, Socure can expand to cover additional documents with the capability to add country-specific IDs in less than **5 days**. When the system detects an **un-listed ID card**, it automatically provides key insights into risk associated with the document: DocV can often extract data (name, date of birth, expiration date, etc.) from such IDs. Any data extracted will be automatically compared to the submitted data for the individual. DocV can recognize general fraud indicators, such as non-live captures. DocV can compare the photo in any ID headshot to selfie images provided by the user. It is important to recognize and support a wide range of government issued identification cards, books, and other formats to promote equitable access by accommodating individuals who may possess different types of identification or documentation. This approach acknowledges the diversity of personal circumstances and confirms that people from different backgrounds can participate in verification processes without facing unnecessary barriers. Additionally, offering multiple options allows individuals to choose the most suitable form of identification based on their personal preference, further enhancing inclusivity and fairness. Our approach to document classification draws lessons from traditional methods and further innovates by leveraging Natural Language Processing (NLP) instead of rigid templates. Unlike the conventional approach, which demands significant training data
IDP48	Evidence Assessment Fraud Detection	Detect and prevent fraud in the presentation of government issued credentials by an End User. If yes, explain the methodology, processes and procedures the proposed Solution uses to accomplish this.	Y	Socure's solution examines physical aspects of documents that cannot be replicated digitally. We assess characteristics unique to authentic paper documents, such as texture and edge integrity, distinguishing them from digital forgeries like screen replays or photographed copies. We also detect signs of manual forgery, such as portrait substitutions where a printed headshot might be overlaid on a genuine document base. For credentials that include a headshot, we deploy specialized algorithms to detect manipulation of the headshot on the document itself, identifying whether a headshot has been digitally altered or replaced with a deep fake image. This is crucial for preventing fraudsters from using sophisticated graphic editing tools to create counterfeit documents with false identities but authentic-looking features.
IDP49	Evidence Assessment Acceptance Rate	Track information about the false acceptance rate (FAR) and false rejection rate (FRR) for detecting fraud in the presentation of government issued credentials by an End User. If yes, describe the methodology, processes and procedures the proposed Solution uses to accomplish this.	Y	[redacted]

IDP50	Evidence Assessment Facial Recognition Fraud Detection	Detect fraud with the use of facial recognition methods. If yes, explain the measures used to determine and detect the fraud.	Y	Socure employs a comprehensive suite of technologies to combat fraudulent submissions of facial images and genAI-generated deep fakes in our liveness (selfie) detection process. We have developed a multi-layered approach that incorporates advanced deep learning models, sophisticated selfie analytics, and robust device intelligence. Deep fake Detection Models: Our advanced models are specifically engineered to recognize deep fake images, trained on a diverse dataset that includes various synthetic media types. These models adeptly identify anomalies and artifacts typical in deep fake content, achieving 99% accuracy in detecting fraudulent selfies during tests with our production dataset. Selfie Analytics for Background Consistency: We employ analytics to examine the background for signs of artificial manipulation, such as virtual or digitally altered environments. This helps verify the physical presence of a real person, a crucial element in liveness detection. Deep fake and selfie analytics also assess camera angle, positioning of photo, shadows and other factors that would indicate use of a fabricated image. Liveness Checks for Authenticity: Our system is vigilant against common fraud tactics, such as image-of-image detection and screen replay. We look for telltale signs of a digital screen capture, which further authenticates the physical presence of the document and its holder. Device Intelligence and Entity Profiler: After submission, we analyze data from the user's device, including metadata and behavioral interaction patterns, to identify inconsistencies typical of injection attacks. Our entity profiler uses this data to detect anomalies, like irregular session activities and mismatched geographic information. Image Alert List and Velocity Checks: This feature tracks the recurrence of identical facial images across various documents and different personal identifiers (leveraging Socure's identity graph), helping to identify reused content—a common strategy in injection attacks. These integrated measures have proven highly effective in our rigorous internal testing and real-world application, demonstrating our commitment to maintaining robust defenses against emerging digital threats. Currently, Socure does not	
IDP51	Evidence Assessment Liveness Detection	Offer both active and passive presentation attack detection (PAD), a.k.a. liveness detection. If yes, describe the End User interface for each.	Y	[redacted]	
IDP52	Document Authenticity Assessment – U.S. Citizen	Validate the authenticity of the following documents presented by End Users who are U.S. citizens during the Identity Verification process as proof of identification and legal presence: a. Official birth document issued by a U.S. state, jurisdiction or territory. b. Valid, unexpired U.S. passport or U.S. passport card. c. U.S. Certificate of Citizenship or Certificate of Naturalization. If yes, describe the methodology your Solution uses to accomplish this. If there are any other documents not listed that can be used, please list them as well. (Note: All credentials issued by the COV must be validated with a COV data source.)	Y	Yes, Socure validates **b. Valid, unexpired U.S. passport or U.S. passport card.** "a. Official birth document issued by a U.S. state, jurisdiction or territory." and "c. U.S. Certificate of Citizenship or Certificate of Naturalization." may be uploaded as unstructured documents to document additional evidence of identity but not validated. Please see "Attachment - IDP52 - Global Document Coverage" for our document coverage. Please note, Socure can add additional documents to our library within 5 business days. The methodology to validate documents can be found in IDP55.	Please see Attachment IDP52 - Global Document Coverage.pdf as an attachment to Appendices

IDP53	Document Authenticity Assessment – Non U.S. Citizen	Validate the authenticity of the following documents presented by End Users who are non-U.S. citizens during the Identity Verification process as proof of identification and legal presence: a. Unexpired foreign passport with an unexpired or expired U.S. visa and unexpired I-94 or entry stamp. b. Unexpired Employment Authorization Document (I766) AND USCIS form I-797 displaying the End User's name. c. Unexpired Permanent Resident Card If yes, describe the methodology your Solution uses to accomplish this. If there are any other documents not listed that can be used, please list them as well. (Note: all credentials issued by the COV must be validated with a COV data source.)	Y	Yes, Socure validates "**a. Unexpired foreign passport with an unexpired or expired U.S. visa and unexpired I-94 or entry stamp**." and "**c. Unexpired Permanent Resident Card**" "b. Unexpired Employment Authorization Document (I766) AND USCIS form I-797 displaying the End User's name." may be uploaded as unstructured documents to document additional evidence of identity, but not validated. The comprehensive methodology by which our document verification solution validates the authenticity of documents is outlined in IDP46, IDP47, IDP48, IDP50, IDP51 & IDP55
IDP54	Document Authenticity Assessment – Social Security Number	Validate the authenticity of the following documents presented by End Users during the Identity Verification process as proof of Social Security Number: a. Social Security card. b. U.S. Internal Revenue Service tax reporting W-2 form. c. Payroll check stub issued by employer that shows full Social Security number. If yes, describe the methodology your Solution uses to accomplish this. If there are any other documents not listed that can be used, please list them as well. (Note: all credentials issued by the COV must be validated with a COV data source.)	N	Socure harnesses advanced computer vision in its Document Verification product to enable the capture of unstructured documents such as social security cards, utility bills, birth certificates, etc. Human review is typically required to assess the risk of the documents. We have the ability to integrate with COV issuing sources to enable the validation of these documents. Given the advanced capabilities of fraudsters across the country, Socure often works with its customers to deploy multi-layered strategies that do not rely on the validation of these documents given they are easy to replicate and pass as legitimate.

IDP55	Document Authenticity Assessment – Virginia Voter	Validate the authenticity of the following documents presented by End Users during the Identity Verification process as proof of eligibility to vote in the Commonwealth of Virginia: a. Virginia driver's license b. Virginia DMV-issued ID card c. Valid employee ID card, containing a photograph, issued by End User's employer in ordinary course of business. d. U.S. Military ID. e. Valid student ID issued by a public or private high school or institution of higher education located in Virginia or the United States. f. Government-issued ID card from a federal, Virginia, or local political subdivision. g. Voter ID card issued by the Virginia Department of Elections. h. Voter confirmation documents. i. Valid tribal enrollment or other tribal ID issued by one of the 11 tribes recognized by Virginia. j. Nursing home resident ID issued by a government facility. k. Current utility bill, bank statement, government check, or paycheck containing the name and address of the end-user. l. Other current government document containing the name and address of the End User. m. Signed ID Confirmation Statement. If yes, describe the methodology your Solution uses to	Y	There is more reponse in this cell than is viewable. Yes, SocureGov validates "a.", "b.", "f.", "i.". Currently, "b. Unexpired Employment Authorization Document (I766) AND USCIS form I-797 displaying the End User's name." may be uploaded as unstructured documents to document additional evidence of identity, but not validated. For all ID card types not included on this list, the system automatically provides key insights into risk associated with the document: • DocV can often extract data (name, date of birth, expiration date, etc.) from such IDs. • Any data extracted will be automatically compared to the submitted data for the individual. • DocV can recognize general fraud indicators such as non-live captures. • DocV can compare the photo in any ID headshot to selfie images provided by the user. These combinations of these signals are analyzed, and an outcome/decision provided back to Authorized Users to verify the document authenticity. It is important to recognize and support a wide range of government issued identification cards, books, and other formats to promote equitable access by accommodating individuals who may possess different types of identification or documentation. This approach acknowledges the diversity of personal circumstances and ensures that people from different backgrounds can participate in verification processes without facing unnecessary barriers. Additionally, offering multiple options allows individuals to choose the most suitable form of identification based on their personal preference, further enhancing inclusivity and fairness. The solution employs proprietary natural language processing (NLP) and other machine learning tools to learn from new ID documents as they are discovered in real life scenarios. As part of the document classification approach, the NLP based tools can discernand employs patented capabilities (Patent: US-11748586-B2) to detect visually indistinguishable inauthentic IDs using data encoding and consistency techniques. Unlike the legacy approach for template matching, our solution is not reliant on predefined format and can quickly update to
IDP56	Primary Document Authenticity Assessment – Virginia Residency	Validate the authenticity of the following documents presented by End Users during the Identity Verification process as primary proof of Virginia Residency: a. Deed, mortgage, monthly mortgage statement or residential rental/lease agreement. b. U.S. Postal Service change of address confirmation form or postmarked U.S. mail with forwarding address label. c. Utility bill, not more than two months old, issued to the End User (cell phone bills are not accepted). If yes, describe the methodology your Solution uses to accomplish this. If there are any other documents not listed that can be used, please list them as well. (Note: all credentials issued by the COV must be validated with a COV data source.)	N	Socure harnesses advanced computer vision in its Document Verification product to enable the capture of unstructured documents such as social security cards, utility bills, birth certificates, etc. Human review is typically required to assess the risk of the documents. We have the ability to integrate with COV issuing sources to enable the validation of these documents. Given the advanced capabilities of fraudsters across the country, Socure often works with its customers to deploy multi-layered strategies that do not rely on the validation of these documents given they are easy to replicate and pass as legitimate.

IDP57	Secondary Document Authenticity Assessment – Virginia Residency	Validate the authenticity of the following documents presented by End Users during the Identity Verification process as secondary proof of Virginia Residency: a. Postmarked mail displaying the End User's name and current address. b. Official document or correspondence from a federal, state, or local government agency displaying the End User's name and current address (DMV–issued documents without postmarked envelopes are not accepted). c. Billing statement or other official document from a recognizable business displaying the End User's name and current address. If yes, describe the methodology your Solution uses to accomplish this. If there are any other documents not listed that can be used, list them as well. (Note: all credentials issued by the COV must be validated with a COV data source.)	N	Socure harnesses advanced computer vision in its Document Verification product to enable the capture of unstructured documents such as social security cards, utility bills, birth certificates, etc. Human review is typically required to assess the risk of the documents. We have the ability to integrate with COV issuing sources to enable the validation of these documents. Given the advanced capabilities of fraudsters across the country, Socure often works with its customers to deploy multi-layered strategies that do not rely on the validation of these documents given they are easy to replicate and pass as legitimate.
IDP58	Validation With No Credentials	Validate the identity of End Users who do not have any of the credentials listed above. If yes, please describe the methodology your Solution uses to accomplish this.	Y	[redacted]
IDP59	Fraud Alerts	Provide alerts to designated personnel of the Authorized User(s) when fraud is detected. If yes, describe this capability and include any relevant diagrams to illustrate the process.	Y	During the certification process Socure collects contact information enabling us to alert designated personnel or groups if we detect signals of fraudulant activity. Once VITA is promoted to the production environment, Socure sets up monitoring tools and distributes their output to stakeholders on an agreed upon schedule. Included in these reports are trends that may indicate fraud (like a spike in a risk code), drops in data frequency rates or sudden increases or decreases in performance (accept rates, decline rates, or friction). Socure will contact via email the specified person or group if warning signs occur and bring in Data Scientists or Fraud Investigators as needed. A typical scenario would include recognizing an increase in a fraud pattern, notifying the client contact, working with data science to isolate the fraud pattern through decision logic, testing new logic to address the issue against a given real data set and deploying the logic when ready. This process can take less than a day during a significant fraud attack because of the agility of Socure's platform and no-code Decision Module.
IDP60	PAD Acceptance Rate	Track and report information about the false acceptance rate (FAR) and false rejection rate (FRR) for presentation attack detection (PAD). If yes, please describe.	Y	Socure will track and report information about the False Accept Rate (FAR) and False Reject Rate (FRR) for Presentation Attack Detection Level 2 liveness detection and document verification performance. Please reference false acceptance rate (FAR) & false rejection rates (FRR) in IDP-40
IDP61	ISO/IEC 30107-3 Evaluation	Provide evidence that the Solution has been evaluated and found to conform with ISO/IEC 30107-3. (https://www.iso.org/standard/79520.html). If yes, provide a copy of the evaluation report or certificate from a locally accredited third-party.	Y	[redacted] Please Reference "Attachment - IDP61 - 2

IDP62	Product Documentation	Provide current documentation of Solution's features and functionality. Describe how Supplier provides updated documentation when updates are made to the Solution.	Y	Socure's features and functionality are fully documented in **DevHub located online accessible directly (https://developer.socure.us/) or through Socure's Admin Dashboard**. Updates to product documentation are published to Devhub prior to the production deployment on an as-needed basis. Any module updates affecting our customers are communicated, agreed upon, and implemented in conjunction with Socure. **Background** Devhub is Socure's comprehensive developer hub designed to empower customers with self-service capabilities. Devhub houses extensive API reference guides and SDK guidelines, alongside quick start guides that provide immediate help for seamless integration and optimization of Socure's services. It's designed to assist customers in effectively implementing and scaling their solutions. Devhub serves as a knowledge base with a robust collection of best practices, updates on upcoming features, and real-time status updates. This resource is pivotal for live customers who seek to deepen their understanding of logic and reason codes, enabling them to enhance their operational efficiency through self-serve capabilities. Outside of DevHub, Socure offers dedicated **Slack channels** for live customers, providing a direct and efficient way to answer questions promptly. This personalized communication channel facilitates real-time problem-solving and instant support directly from our technical team. Customers can reach out to our support team anytime via **email** at Support@Socure.com. Our dedicated staff is available 24/7 to assist with any inquiries or issues, confirming timely and effective resolutions.
IDP63	Performance	Provide information about how many minutes of service outage, including breakdown of availability, Supplier has experienced during the lifetime of the Solution, including a chronology of these outages during the most recent three year period.	Y	[redacted]
IDP64	Performance	Provide information about how long the Solution has been commercially available.	Y	Socure, established in 2012, offers a cutting-edge predictive analytics platform that seamlessly integrates the latest machine learning and artificial intelligence technologies with both digital and offline data. This integration enables us to deliver the market's most precise and robust solutions for identity verification and fraud risk prediction. With a diverse customer base spanning various industries requiring robust digital identity verification, we currently serve nearly 2,400+ clients. This includes 14 of the top 15 banks, 13 of the top 15 major credit card issuers, 4 of the 4 largest state agencies, leading gaming providers, and multiple tier 1 payroll providers. We are providing some form of identity verification (both documentary or non-documentary), fraud prediction, and sanctions screening for nearly every consumer fintech. Our solutions spans all of the different high-value, high transaction volume, highly regulated spaces where accurately identifying consumers is critical to the business. Many of Socure's customers are also strategic investors in the company, including Citi Ventures, Wells Fargo Strategic Capital, Capital One Ventures, MVB Bank, and Synchrony.
IDP65	Availability	Supplier's Solution is available 24x7x365. If no, what is the proposed Solution's availability?	Y	Socure's purpose-built offerings leverage Amazon Web Services (AWS) cloud computing services in the AWS GovCloud regions to provide agencies capabilities that adhere to the essential cloud computing guidelines defined by the National Institute of Standards and Technology, and confirm to FedRAMP moderate security requirements. SocureGov is designed to perform twenty-four (24) hours per day, 365 days per year. Our standard SLA provides for 99.9% uptime.
IDP66	Up Time	Provide information on the up-time percentage of the Solution during its lifetime. Provide a chronology of these percentages over a 3 year period.	Y	[redacted]

IDP67	Change Control	Allow the Authorized User(s) to have a role in the process for change control policies and procedures. If yes, explain how this is accomplished.	Y	SocureGov's administrative dashboard provides a fully self service Graphical User Interface (GUI) for managing soluiton configurations, active modules, and decision logic. Along with the implementation team, a change control process, the policies and proceedures of which have been shaped and agreed upon by the state will be put into place.
IDP68	Role Based Access	Employ role-based access for administrators of the Solution. If yes, describe the roles, and how the roles and permissions are managed.	Y	Socure Dashboard supports RBAC. More details below: A role determines what a user can do and see in Socure Dashboard. A user's role usually relates to their responsibilities in customer's organization. Some roles are administrative and are designed for managing users and accounts. Other roles are non-administrative, and are designed for users who only need access to certain key features in Socure Dashboard. There are two types of roles in Socure Dashboard: system defined roles and custom roles. System defined roles are predefined roles that you can assign to users or use as a template to create custom roles. System defined roles cannot be deleted and, in some cases, have strict usage rules. Custom roles are typically created by an Account Owner or Administrator. Custom roles can be unique to customer's organization and specific to an employee's job. Each role has a set of permissions that controls access to the pages and functionality in Socure Dashboard. There are two types of permissions in Socure Dashboard: Account permissions and Environment permissions (Account Permissions: Controls access to specific pages in Socure Dashboard; Environment Permissions: Control access to specific pages in Socure Dashboard in the Production, Certification, and Sandbox environments). Customers can add users to account and need to assign one or more roles to the user. This determines which accounts a particular user has access to and what specifically the user can view and/or modify for the accounts they have access to (based on the role assigned)
IDP69	Testing Protocols	Support testing of the Solution including: unit testing, system testing, interface testing, end-to-end testing, user acceptance testing, and performance testing. If yes, do you have non-production instances that can be used for testing prior to deploying changes to the Solution? Include how this is accomplished and what tools are used.	Y	The SocureGov platform provides pre-production environments (Sandbox, Certification) to perform any testing required by the State. Socure will work with the State to provide action plans regarding any performance testing being done within these environments.
IDP70	Additional Capabilities	Describe any additional capabilities that are not referenced in Supplier's responses above. Provide as much detail as possible about these additional capabilities.	Y	SocureGov's modular platform orchestrates the entire user lifecycle, beginning with onboarding and mitigates specific identity verification use cases, returning a risk score and supporting reason codes. All SocureGov product modules are available through a single API. Additional capabilities not featured include: GLOBAL WATCHLIST SCREENING WITH MONITORING Global Watchlist Screening with Monitoring mitigates risk with hyper-accurate watchlist screening that reduces false positives up to 95%, with a 50% reduction in manual review. Socure's sophisticated matching algorithms, proprietary data, and true continuous monitoring deliver industry-leading accuracy, real-time alerts, and uninterrupted compliance with CIP/KYC regulations. This offering allows organizations to focus on the data they need with bespoke coverage relevant to their agency.
IDP71	Audit logs	Provide audit logs to external tools, for example, feeding audit logs to Agency Splunk. If yes, describe how this accomplished and what tools are used.	Y	Socure's Administrative Dashboard provides audit logs for each account the Agency creates, which can be downloaded or monitored in external tools as required. These logs monitor Agency user interaction, and provide insight on any changes that are input by users.
IDP72	Identity Verification Legal Protection	Support the Authorized User(s) if any End User sues the state for issues associated with your Identity Verification Solution, i.e., a dispute between the End User and the Authorized User over the outcome of an Identity Verification attempt.	Y	Socure will provide the Commonwealth with reasonable documentation and similar support the Commonwealth requests to assist in any dispute with an End User.

IDP73	End User Bias Reporting	Provide established metrics and testing methodologies to assess performance and understand the impacts across End User populations (e.g., bias in artificial intelligence). If yes, explain the metrics and methodologies used.	Y	[redacted]
IDP74	Logging and Auditing	Capture and log all of the steps to verify the identity of the End User and the types of evidence presented, i.e., Strong, Superior, Fair, etc. If yes, describe the logging and auditing features of your Solution.	y	There is more response in this cell than is viewable. The SocureGov Administrative Dashboard captures and logs all transactions processed and the decision logic used to inform application outcomes to provide a complete logging/auditing review of the steps taken by the End User and the review of the types of evidence presented. This transaction view is a single component of the total functionality provided by the Admin Dashboard. The dashboard provides the Commonwealth with tools to manage the operations of the SocureGov platform. Additional capabilities include: -Upload functionality to support transaction upload and batch process file interchanges between Socure and VITA -Analytics - Real time system & module performance reporting used to inform the management and operation of the system -Case Management (optional upgrade) - the ability to put a human in the loop to review Document Verification outcomes and approve/deny access -DocV App - the ability for the state to customize DocV experience to Commonwealth specifications -Decision Engine - User interface for customers to review, simulate and potentially self-manage the SocureGov risk tolerances informing decision outcomes -Batch Jobs - the ability to review batch upload outputs -Reports - Self Service reporting functions for our clients to request transaction detail, audit and consent reports -Accounts - self-service capabiltiy for our clients to create separate API keys to integrate SocureGov strategies along their customer user management life-cycle -Users and Roles - Self service Adminstrative Dashboard and Developer customer access management solution for VITA to manage application roles & users -Developers - Functionality to whitelist IP domains, request addition ID & SDK keys, as well as set up web hooks to monitor SocureGov outcome analysis -Product Settings - a self service functionality to manage system and outcome calibrations The Adminstrative Dashboard was designed as a way for our customers to manage the identity & fraud management program and technical support functions within an integrated identity interface.
IDP75	Identity Verification Sessions	Allow supervised remote and in-person identity verification sessions. (In most cases, Authorized User(s) will provide locations and conduct in-person identity verification sessions. However, there could be exceptions where Authorized User(s) will ask Suppliers to provide this service.)	y	While SocureGov's offering effectively triages up to 100% of applications using online services, Socure's Administrative Dashboard can be integrated into the Authorized User(s) locations to provide verification services as part of the Commonwealth's in-person process
IDP76	Remote Supervised Identity Verification Sessions	Provide a means to determine if a remote supervised identity verification session is possible or not. If a remote supervised identity verification session is not possible, please explain how your solution would address this.	y	SocureGov will work with the application user interface (UI) to offer a remote supervised identity verification session to End Users. In the event that an End User is unable to complete the remote supervised verification session, SocureGov will inform the application user interface of this and a notification along with instructions will be provided to the End User on how to proceed. Additionally, if an End User opts out of the remote supervised verification process via the UI due to technology, documentation, or other constraints, the same notification and instructions will be provided to the End User to result in an in-person End User identity verification session.

IDP77	Scheduling Identity Verification Sessions	Allow for a mechanism to schedule supervised remote and in person identity verification sessions. Explain how this could be accomplished.	y	Socure's offering includes the ability to schedule out supervised remote & in-person identity verification sessions as part of the onboarding user journey. When applicants enage with the Commonwealth registration page, our API can be integrated behind user defined application processes to perform automated, supervised, or in-person verification activities. For the automated application processes, information will be collected via a Commonwealth designed user interface to align with required evidence to support the verification level. Once collected, this information is passed to Socure behind the restful API endpoint and the analysis and disposition of the verification is provided back in a single attribute. Should the applicant require biometric verification, Socure provides SDKs for the Commonwealth to leverage for easy integration. For remote supervised, scheduled & unscheduled, the Commonwealth would design a user interface (UI) to engage these services and begin a remote session. Applicants can select for an immediate session, or schedule a session for a later time. Regardless of selection, the applicant would engage through video/voice call to perform verification services. SocureGov will work with the application user interface to determine the need for an in-person identity verification session, and present a notification of this need to the End User along with instructions. End Users will be directed to an authorized user location of their choice and will be informed of the necessary identity evidence they will be required to present at the authorized user location. End Users will schedule (if necessary) an appointment via the scheduling platform of the authorized user location they have selected. Once at the location, Authorized Users will work with SocureGov to perform in-person verification of the End User, assisting them in the collection and submission of the proper identity evidence. Results will be communicated to the Authorized User IAM team or infrastructure to complete the account creation activity.

Tier 2 Identity Verification Help Desk Support				
Req. No.	**Category**	**Requirement**	**Yes (Y) Future (F) No (N)**	**Provide an explanation of how the Solution fulfills the requirement. *The Supplier's detailed explanation should not simply be an affirmative reiteration of the question, but should describe the manner in which the requirement is met.* Where possible and beneficial, please provide screenshots or graphics to help illustrate your response. Where your response is described as a future release or update as the provision, please provide a timeline for that provision. Supplier may also use this column to cross-reference a detailed explanation included as an attachment to its proposal.**
Tier 2 Identity Verification Technical Support				
Supplier Responsibilities include:				
T2-ID01	Technical Support Implementation Experience	Provide the number of implementations of Tier 2 support you have executed in the past three years.	Y	[redacted]
T2-ID02	Support Channels	Describe the types of Tier 2 support channels Supplier offers, e.g., phone, email, chat, and the hours of availability for each.	Y	Socure's Tier 2 support can be engaged via email 24/7/365 through support@socure.com for immediate and after hours issue triage. Notifications received at this inbox are funneled to the appropriate dedicated account management team members, as well as C-level executives to ensure service delivery.
T2-ID03	Service Level Agreements	Describe Supplier's incident management escalation thresholds, severity levels, and the associated initial response times, frequency of case updates, and expected resolution times for each (SLAs) per support channel.	Y	[redacted]
T2-ID04	Identity Mgmt. and Verification Support	Describe Supplier's experience supporting End User identity verification. Provide examples and the number of years of experience acting in this capacity.	Y	Socure was founded in 2012 with the audacious goal of helping 100% of people prove who they are online without subjecting them to undue burden due to differences in race, gender, age, ethnicity, or socioeconomic class. Today, Socure's identity proofing and fraud risk management platform is the gold standard for 2400 clients across government, healthcare, online gaming, telecom, e-commerce, fintechs, and financial services. Our platform is fully automated and accessible via a single, Representational State Transfer (REST) Application Programming Interface (API), which can be seamlessly integrated into the IBM Identity platform you work with today. We have a demonstrated history of supporting the largest companies with the highest volumes in the world, other state governments as well smaller earlier stage companies.
T2-ID05	Incident Management System	Provide an incident management system. Include a description of the incident management system used, whether it is SaaS or OnPrem, how often it is updated, and how it interfaces with other systems, e.g., API, ELT, other.	Y	As a SaaS offering, Socure's services are limited to the identity verification and fraud prevention modalities. Incident management response systems fall outside of our commercial offering.

T2-ID06	Incident Management System	Supplier agrees to grant Authorized User(s) access to its incident management system. If no, how will Supplier keep Authorized User informed of incidents related to the identity verification?	Y	Socure assumes the government's definition of an incidents is a problem associated with the identity verification transaction. Socure provides our clients transaprency to ensure the SocureGov environment is up and running via status.socure.com. This website provides real-time status of the SocureGov environment and provides notice for any incidents of the service. Socure also provides our clients full transparency into the SocureGov platform performance to review transaction histories and outcomes through the Administrative Dashboard & by providing full identity & fraud module outcomes via our JSON responses. The Administrative Dashboard serves as a centralized location for the Commonwealth to manage all aspects of the SocureGov platform including: -Transaction history/lookup functionality -Onboarding risk tolerance & decision module calibration -Reporting capabilities -User Access Management & Role Definition -Developer tools to support SocureGov integration Authorized Users will be provisioned with access to the status page upon request.
T2-ID07	Incident Management System	Describe any End User data stored in Supplier's incident management system, if applicable.	Y	Socure does not store PII in the incident management system. Instead, when a PII data set is provided to Socure, a transaction reference number is assigned and provided back to our customers so as to limit PII exposure. Transaction PII is only accessible to those performing detailed analysis on customer accounts.
T2-ID08	Performance	Provide the number of minutes of service outage Supplier's incident management system has experienced during the lifetime of the Supplier's solution, including a chronology of these outages during the most recent three year period.	Y	[redacted]
T2-ID09	Knowledge Base	Supplier's incident management system that has a knowledge base component which can be updated with content. If yes, please explain.	Y	Socure conducts after-action reports for all incidents, and houses that data in the AWS GovCloud environment, and will share those items upon request for anything with a customer impact.
T2-ID10	Support Personnel Characteristics	Explain how Supplier profiles its Tier 2 support personnel, e.g., IDP support experience, customer service experience level, incident management process knowledge, troubleshooting experience, etc.	Y	Socure's Tier 2 support personnel are recruited and trained based on the roles & responsibilities dictated by their positions. When Socure onboards a new client, we align a dedicated Account Management Team consisting of a Account Executive, Solutions Consultant, Solutions Engineer & Strategic Account Manager. Each of these functions has been defined within requirement T2-ID17 stated below. In addition to the dedicated Account Management Team, our clients also benefit from having 24/7/365 support from T2 technical support roles that specializes in systems and technical integration components. Depending on the role, each function is recruited based on minimum requirements, years experience, and familiarity with the identity & fraud management landscape. Post onboarding, each employee must complete necessary training on the Socure products and components they have responsibility for.

T2-ID11	Support Personnel Training	Supplier agrees to deploy fully trained Tier 2 support personnel. Describe your training methodology.	Y	All Socure employees undergo extensive training as part of their onboarding training to ensure that employees are empowered through education to fully execute the responsibilities of their job role as well as understand system functionality. Training programs vary by role and anticipated responsibilities. For technical roles, training focuses more on the technical achitecture and processes that support overall system performance, including but not limited to: platform integration modalities and capabilities, system enablement functions, troubleshooting & triage, and finally, a shadowing function to ensure adoption. For business and analytic roles, training encompasses end to end system functionality. These training programs will focus on the SocureGov business utility, how to operationalize and manage SocureGov modules within different technical environments, module calibration, and understanding how we utilize AI/ML to develop our products. Additional information can be provided upon. Due to the many different functions we incorporate into our SaaS model, the differences to our training approaches are vast.
T2-ID12	Security	Supplier agrees to provide an incident response plan(s) to respond promptly and effectively to data breaches and security incidents to its incident management system. If Supplier cannot provide a plan(s), please explain how data breaches and security breaches are handled.	Y	Socure has provided it's Incident Response Plan as an attachment to our RFP response. See Attachment T2-ID12 Socure_Incident Response Plan 3.0
T2-ID13	Security	Supplier agrees to conduct regular audits and risk assessments of data security and HIPAA compliance practices to identify and address potential vulnerabilities for its incident management system. If yes, describe how this is accomplished and the frequency of these audits and assessments.	Y	Socure agrees with this requirement. Socure does not store any PHI and therefore does not fall under HIPAA compliance requirements. The SocureGov platform has been assessed (at least annually) against and currently complies with the following industry security standards: StateRAMP Moderate (Authorized), TX-RAMP Moderate (Authorized), System and Organization Controls (SOC) 2 Type 2, International Organization for Standardization (ISO) 27001, 27017, 27018, 27701, Web Content Accessibility Guidelines (WCAG) 2.1 Level AA, and NIST Identity Assurance Level 2 (IAL2). Socure is compliant with FedRAMP requirements and has been assessed by a FedRAMP-approved third-party assessor (3PAO) as compliant with FedRAMP security controls.
T2-ID14	Security	Supplier agrees to stay up-to-date on and adapt practices for changes in relevant data protection laws and regulations to your incident management system. If yes, explain how this is accomplished.	Y	Socure provides services nationwide and globally, and is required to stay up-to-date on all relevant data protection laws and regulations. Employees are required to go through annual training on these regulations, and Socure has processes in place to maintain these obligations.
T2-ID15	Security	Supplier agrees to create and maintain policies or controls to ensure third-party vendors or subcontractors adhere to data protection and compliance standards for its incident management system. If yes, describe these policies and controls.	Y	Socure contractually requires all vendors that may access customer data to adhere to data protection and compliance standards.

T2-ID16	Tier 2 Support Use Cases Identity verification	Describe how Supplier would address the following Tier 2 Identity verification use cases for identity verification. For those you cannot address, describe the reason why and how you would resolve them. Please note this list is not all inclusive or without limitations. 1. Monitor identity verification processes to identify and resolve errors, e.g., false positives and false negatives. 2. The ability to deny identity verification for users that do not pass the criteria for a given IAL. 3. Connection issues between the Identity Management solution and your solution.	Y	1. Socure's account management team is on hand to support integrating our SocureGov platform into the Commonwealth's onboarding process from integration to go-live and post implementation support. Socure has designed the Solutions Consulting & Strategic Account Management roles for the purpose of ensuring our clients are using best in class, empirically driven solutions to combat fraud and create more advantageous onboarding experiences for good users. Post go-live, Solutions Consultants & Strategic Account Managers review fraud signals from our data consortium and customer performance outcomes to identify high risk outcomes that may not be caught with the current solution calibration. Socure works with the state on a quarterly and ad hoc basis to make refinements to decision logic that will inform fewer false positives & negatives, as well as increase frictionless onboarding for low risk users. 2. The SocureGov platform is designed to be installed throughout the customer journey and calibrated per location to align to the customer risk tolerance and IAL levels defined by the Commonwealth. By leveraging the Decision Module, the Commonwealth will benefit from being able to calibrate the onboarding criteria within the identity verification & fraud management module locations to receive a "Reject" for individuals who pose risk to the agency. "Reject" outcomes can be dispositioned by the existing user onboarding workflow. 3. SocureGov Platform integration with the identity management provider is completed, tested and certified prior to implementation & go-live. Socure Account Management & 24/7/365 tech support are available to support and triage integration related issues.
T2-ID17	Account Management	Supplier agrees to provide a dedicated account manager and support team for questions and concerns from Authorized Users and End Users. If yes, include a description of your plans to support the Authorized User(s).	Y	After contract award, Socure defines a dedicated Account Management Team which guides product implementation and post production release account management. The Strategic Account Manager will be the dedicated account manager. The Solution Consultant acts as the product implementation lead. Additional product support team functions are outlined below: **Solution Consultant** - accountable for overall project implementation. Works with Solution Engineer and Account Manager to define objectives and timelines. Coordinates kickoff meetings and will work with Technical Account Manager to schedule recurring status meetings. Engages additional resources (Development Support Engineers, Data Scientists, etc.) as necessary to solve client related issues. **Solution Engineer**- Socure solutions implementation specialist. Provides training on solutions, guidance on SocureGov settings, implements client risk tolerances into Decision Module, provides expertise on technical aspects of integrating into the client environment, , and helps troubleshoot client implementation issues as they arise. Responsible for customers Implementation Certification process that enables clients go-live. Will work to set project timelines and align resources to support customer implementation timeline, including post go-live support. T**echnical Account Manager:** Acts as the Socure solutions implementation specialist, providing training on solutions, guidance on SocureGov calibration settings, and expertise on technical aspects of integrating into the client environment.

Tier 3 Identity Verification Technical Support					
Req. No.	**Category**	**Requirement**	**Yes (Y)**	**Provide an explanation of how the Solution fulfills the requirement. *The Supplier's detailed***	Redaction rationale
Tier 3 Identity Verification Technical Support					
Supplier Responsibilities include:					
T3-ID01	Technical Support Implementation Experience	Provide the number of implementations of Tier 3 support you have executed in the past three years.	Y	Socure provides Tier 3 support to all our customers as part of the annual license fee. We do not charge professional services to support the ongoing calibration and management of our solution. To that end, we've performed 285 client integrations in the past 3 years.	
T3-ID02	Account Management	Supplier agrees to provide a dedicated account manager and support team for questions and concerns from Authorized Users and End Users. If yes, include a description of your plans to support the Authorized User(s).	Y	Socure will provide a dedicated account team comprised of one Solutions Engineering and Account Manager to provide the highest level of support, and represent the dedicated team of Data Scientists, Developer Support Engineers, and Solution Consultants who will be working with VITA and Authorized Users for the entireity of the partnership. Each Authorized User will be given the same high level of support from implementation to trouble shooting, along with easily digestible reporting and insight from the Socure Dashboard. These roles can be engaged any time through direct email, or by contacting support@socure.com which is available 24x7x365.	
T3-ID03	Service Level Agreements	Describe Supplier's incident management escalation thresholds, severity levels and the associated initial response times, frequency of case updates, and expected resolution times for each (SLAs) per support channel.	Y	[redacted]	
T3-ID04	Support Channels	Describe the types of Tier 3 support channels Supplier offers, e.g., phone, email, chat, and what the hours of availability are for each.	Y	Email support is available 24x7x365 at Support@socure.com, and phone, email, and chat are supported during business hours.	
T3-ID05	Identity verification Support	Describe Supplier's experience supporting End User identity verification. Provide examples and the number of years of experience acting in this capacity.	Y	Socure was founded in 2012 with the audacious goal of helping 100% of people prove who they are online without subjecting them to undue burden due to differences in race, gender, age, ethnicity, or socioeconomic class. Today, Socure's identity proofing and fraud risk management platform is the gold standard for 2,400 clients across government, healthcare, online gaming, telecom, e-commerce, fintechs, and financial services. In the Public Sector, Socure has launched and supported 27 State Agencies and 2 Federal Agencies, including the largest statewide identity portals in Ohio, Texas, and New York. Socure was selected over 17 competitors as the only provider for GSA's login.gov, the single Federal Application for citizen access. Our platform is fully automated and accessible via a single, Representational State Transfer (REST) Application Programming Interface (API), which can be seamlessly integrated into the IBM Identity platform you work with today. We have a demonstrated history of supporting the largest companies with the highest volumes in the world, other state governments as well smaller earlier stage companies.	
T3-ID06	End User Support Availability	Describe Supplier's End User support availability, e.g., 24x7x365.	Y	Socure offers support 24x7x365 for T3 technical requests via our actively monitored inbox support@socure.com. The dedicated account team is also available from 7am-8pm on business days.	
T3-ID07	Authorized User Support Availability	Describe Supplier's Authorized User(s) support availability, e.g., 24x7x365.	Y	Socure's technical and account management team, as well as C level executives are available 24x7x365 via support@socure.com. It is encouraged for our customers to directly engage their account management teams should any issues arise.	

T3-ID08	Incident Management System	Supplier's solution includes an incident management system. If yes, describe the incident management system used, whether it is it SaaS or OnPrem, how often it is updated, and how it interfaces with other systems, e.g., API, ELT, other.	Y	Socure provides an incident management system that is hosted within our AWS GovCloud environment. A dedicated support team is assigned to the SocureGov environment. Socure's GovCloud JIRA instance is utilized for incident response through a triaged ticketing process. The SocureGov SRE team monitors application uptime and anomalous activity in DataDog and AWS Synthetic. All Infrastructure failures will be treated as Sev1 issues. The SocureGov SRE team will assign an Incident manager role to serve as the responsible party for any incident. This system interfaces seamlessly with the customer support functions - and is updated in real-time by the SRE and Account Management team.
T3-ID09	Incident Management System	Supplier agrees to grant Authorized User(s) access to its incident management system. If no, how will Supplier keep Authorized User informed of incidents related to the identity verification?	N	SocureGov is a FedRAMP conformant environment. Socure cannot adhere to the requirements and provide Authorized User access to our internal environment. Incidents are communicated to customers as determined by the SLAs defined between VITA and Socure.
T3-ID10	Incident Management System	Describe any End User data stored in Supplier's incident management system, if applicable.	Y	As a security practice, Socure does not perpetuate customer PII within our incident management system.
T3-ID11	Performance	Supplier agrees to provide the number of minutes of service outage your incident management system has experienced during the lifetime of its identity verification Solution, including a chronology of these outages during the most recent three year period.	Y	Socure agrees to provide this information on request.
T3-ID12	Knowledge Base	Supplier's incident management system has a knowledge base component that can be updated with content. If yes, please explain.	N	Socure conducts after-action reports for all incidents and houses that data in the AWS GovCloud environment. Socure will share information relevant to Commonwealth's use of the services upon request for issues that impact the Commonwealth.
T3-ID13	Support Personnel Training	Supplier agrees to deploy fully trained Tier 3 support personnel. Describe your training methodoloy.	Y	Socure Tier 3 support team undergoes extensive onboarding & continuing education to support the effective and efficient SocureGov performance. There are at least 4 roles within the organization that support Tier 3: Solutions Engineers, Fraud Investigations, Data Science, Product Managers. High level training and education requirements are listed below: Complete Socure's internal foundational, intermediate and advanced product Training Program up to specified levels per role Complete a baseline and on-going technical training and programming courses to understand architectural infrastructure, system operations and changes Participate in identity & fraud training courses designed by Socure or outside institutes Detailed role curriculums can be provided upon request.
T3-ID14	Security	Supplier agrees to provide an incident response plan(s) to respond promptly and effectively to data breaches and security incidents to your incident management system. If Supplier cannot provide a plan(s), please explain how data breaches and security breaches are handled.	Y	Socure's incident response plan in outlined in Section 7 of this document.

T3-ID15	Security	Supplier agrees to conduct regular audits and risk assessments of data security and HIPAA compliance practices to identify and address potential vulnerabilities for its incident management system. If yes, describe how this is accomplished and the frequency of these audits and assessments.	Y	Socure agrees with this requirement. Socure does not store any PHI and therefore does not fall under HIPAA compliance requirements. The SocureGov platform has been assessed (at least annually) against and currently complies with the following industry security standards: StateRAMP Moderate (Authorized), TX-RAMP Moderate (Authorized), System and Organization Controls (SOC) 2 Type 2, International Organization for Standardization (ISO) 27001, 27017, 27018, 27701, Web Content Accessibility Guidelines (WCAG) 2.1 Level AA, and NIST Identity Assurance Level 2 (IAL2). Socure is compliant with FedRAMP requirements and has been assessed by a FedRAMP-approved third-party assessor (3PAO) as compliant with FedRAMP security controls.
T3-ID16	Security	Supplier agrees to stay up-to-date on and adapt practices for changes in relevant data protection laws and regulations for its incident management system. If yes, explain how this is accomplished.	Y	Socure provides services nationwide and globally, and is required to stay up-to-date on all relevant data protection laws and regulations. Socure's Legal Team continuously monitors for changes in relevant data protection laws and regulations. Socure's Legal Team then directs the GRC Team, which coordinates with multifunctional teams to maintain compliance with evolving laws and regulations. Employees are required to go through annual training on these regulations and Socure updates the training based on the evolution of the legal and regulatory lanscape.
T3-ID17	Security	Supplier agrees to create and maintain policies or controls to ensure third-party vendors or subcontractors adhere to data protection and compliance standards for its incident management system. If yes, describe these policies and controls.	Y	Socure's incident management system is hosted within the AWS GovCloud infrastructure. Any third-party providers leveraged as part of the platform are contractually bound to adhere to the same requirements and implementation approaches outlined in Section 7 - Security Requirements of this response.
T3-ID18	Tier 2 Support Identity verification Privileges	Provide sufficient privileges to Tier 2 Identity verification support analysts to help them determine root cause or the ability to escalate their cases to Tier 3 identity verification support. If Supplier cannot provide sufficient privileges to Tier 2, explain how Supplier will manage incidents escalated from Tier 2.	Y	Socure's pre-defined roles enable the right level of access to be provided to support analysts - to allow them access to see transaction reason codes while either obfuscating or allowing access to the PII submitted, depending on the need of the analysis.
T3-ID19	Tier 3 Support Use Cases Identity verification	Describe how Supplier would address the following Tier 3 Identity verification use cases for identity verification. For those you cannot address, describe the reason why and how you would resolve them. Please note this list is not all inclusive or without limitations. 1. Monitor identity verification processes to identify and resolve errors, e.g., false positives and false negatives. 2. The ability to deny identity verification for users that do not pass the criteria for a given IAL. 3. Connection issues between the Identity Management solution and your solution.	Y	Socure's Platform allows for automated identity verificaiton through data science and analysis built from the largest consortium of feedback data in the industry. 1. Socure employs a dedicated team of Certified Fraud Investigators to manually review suspected false positives and false negatives to optimize performance. 2. Socure's Decision Logic automates the pass/fail determination set for each use case or application. 3. The SocureGov platform and Identity Management solution will be integrated through our API endpoint, but should any issues arise there is a 24x7x365 helpdesk which is available at support@socure.com

Implementation					Redaction Rationale
Note to reviewers: The current scope of implementation includes implementation AND configuration.					
Req. No.	**Category**	**Requirement**	**Yes (Y)**	**Provide an explanation of how the Solution fulfills the requirement. *The Supplier's detailed***	
		Implementation			
		Supplier Responsibilities include:			
IMP01	Implementation Services	Describe in detail Supplier's implementation methodology and estimated timeline to implement an identity verification solution for the Authorized User, e.g., Virginia has approximately 8 million End Users and roughly 70 COV End User-facing applications.	Y	Socure follows a stringent implementation process, which we refer to as our certificaiton process. This process is led by the Socure Solutions Engineering team. Upon contract award, a kickoff meeting is scheduled between developer teams and the Solutions Engineers to provide training on Socure's SocureGov API and Developer portal. Once training is conducted - the modules and baseline logic preferences must be set, and once test transactions are successfully run - the Authorized User is considered live. Each subsequent End-User facing application would either be able to leverage this integration, or for optimal performance a sub-account would be assigned for each application enabling Socure's Data Scientists to more uniquely design recommended approaches. Underpinning all of the integeration efforts, Socure's on the ground (Virginia based) project management will facilitate communications, relationships, training, and specific technical configurations with VITA and with each participating state entity.	
IMP02	Identity Verification Implementation Experience	Describe Supplier's experience and number of executed End User-facing identity verification solution implementations within the past three years.	Y	[redacted]	
IMP03	Authorized User Onboarding	Decribe Supplier's onboarding process for Authorized User, including your baseline timeframe. Include the components for determining the timeframe and any drivers that would extend the timeline.	Y	Upon contract award, a kickoff meeting is scheduled between developer teams and the Solutions Engineering team to provide training on Socure's SocureGov API and Developer portal. Once training is conducted - the modules and baseline logic preferences must be set, and once test transactions are successfully run - the Authorized User is considered live. The timeframe is based on the availability of technical resources on the Authorized User, and may be extended based on their availability. In addition, any security or privacy review - or additional user testing required by the authorized user or user-facing applications may extend that timeline.	
IMP04	Prerequisites	Describe any/all prerequisites before implementation begins.	Y	Prior to implementation, Socure will request architectural diagrams, critical points of contact, and project timelines to ensure seamless integration with the project team. Socure's SaaS offering is designed to be integrated at any point in the customer journey, from any web accessible environment. From working with many state partners, Socure is well aware that a one-size-fits-all approach will not be optimal for the wide array of business use cases and technical complexities existing at each Commonwealth agency. Therefore, working closely with each agency to develop an implementation and onboarding approach customized to their needs will be crucial - and Socure's projct management is structured to provide precisely this level of program personalization. Beyond connectivity, we have no technical pre-requisites before implementation begins.	

IMP05	Interface	Supplier agrees to coordinate and execute an interface between the Authorized User's identity management solution and the identity verification solution, e.g., Okta CIAM identity management system.	Y	Socure has integrated with Okta and other identity management systems (Ping, Forgerock, Microsoft, etc) on multiple occassions, and is a preferred partner for Okta primarily due to the ease of integration and customizable user flows. The full integration pattern can be viewed on the identity management solutions Integration Network, and Socure's team would seamlessly interface between the Authorized User and the identity management solution.
IMP06	Implementation Planning	Describe critical information and/or activities (e.g., resource availability, availability windows, etc.) needed from the Authorized User(s) as part of implementation planning, solution development, implementation readiness assessment, work turnover, and critical assumptions.	Y	The initial project kickoff and proper identification of business and technical resources are critical for the success of the partnership. Post contract signature, Socure will schedule a kickoff meeting with VITA, to define project objectives, Commonwealth timelines, platform requirements, and provide recommendations based upon the system architecture and desired user journey of the Commonwealth. The project management team will be on site at VITA for this kickoff meeting. All critical activities and inputs required to support the Authorized User integration are defined in IM07 below.
IM07	Start Up Support	Supplier agrees to provide the Authorized User(s) with start-up and technical support to train its users (including upgrades or feature enhancements) and configuration. Include an outline of your plan.	**Y**	[redacted]
IMP08	Ongoing Support	Supplier agress to provide implementation support and a workplan for Authorized User(s), specifically with a dedicated account manager and support team, to address inquiries and address concerns specifically for Authorized Users.	Y	Socure will provide a dedicated account team to provide implementation support and a workplan for Authorized User(s). Led by the Senior Account Manager and the Onsite Senior Project Manager. The Solutions Consultants and Account Managers provide the highest level of support, and represent the dedicated team of Data Scientists, Developer Support Engineers, and Solution Consultants who will be working with Authorized Users for the entireity of the partnership. These roles can be engaged any time through direct email, or by contacting support@socure.com which is available 24x7x365.
IMP09	IAL 1 Evidence Examples	Supplier agrees to allow the Authorized User(s) to define the minimum documents it will accept for IAL1 identity verification. Refer to Evidence Examples document based on NIST 800-63 v.4. Include additional comments regarding your perspective of these pieces of evidence.	Y	SocureGov will work with the Authorized User(s) to define the minimum documents acceptable to achieve IAL 1. Socure provides automated document verification for government issued IDs such as Drivers Licenses, Passport, State IDs, etc. and can provide support for the capture of unstructured documents as well. Onboarding new document types is simple and easy for SocureGov and can be achieved in days, as opposed to weeks or months with legacy vendors.
IMP10	IAL2 Evidence Examples	Supplier agrees to allow the Authorized User(s) to define the minimum documents it will accept for IAL2 identity verification. Refer to Evidence Examples document based on NIST 800-63 v.4. Include additional comments regarding your perspective of these pieces of evidence.	Y	SocureGov is prepared to ingest and/or verify any and all identity documents defined as "acceptable" for IAL2 identity verification. Socure provides automated document verification for government issued IDs such as Drivers Licenses, Passport, State IDs, etc. and can provide capture for unstructured documents. Onboarding new document types is simple and easy for SocureGov and can be achieved in days, as opposed to weeks or months with legacy vendors.
IMP11	IAL3 Evidence Examples	Supplier agress to allow the Authorized User(s) to define the minimum documents it will accept for IAL3 identity verification. Refer to Evidence Examples document based on NIST 800-63 v.4. Include additional comments regarding your perspective of these pieces of evidence.	Y	SocureGov is prepared to ingest and/or verify any and all identity documents defined as "acceptable" for IAL3 identity verification. Socure provides automated document verification for government issued IDs such as Drivers Licenses, Passport, State IDs, etc. and can provide capture for unstructured documents. Onboarding new document types is simple and easy for SocureGov and can be achieved in days, as opposed to weeks or months with legacy vendors.

IMP12	On-premises to Cloud Transition	Describe in detail the Supplier's implementation methodology in the event an Authorized(s) User moves from an On-Premises solution to a Cloud Solution.	Y	Moving from an on-premise solution to SocureGov is a very easy process. The entire SocureGov Platform has been built to provide risk insights and identity verificaiton at the time of application - and can be accessed via a single Rest API call. This low-effort interface allows for applications looking to migrate to a hosted solution to do so without interrupting customer interactions. If VITA is asking how does the Authorized User move from an on-premise SocureGov solution to a cloud based SocureGov solution, the question is non-applicable due to socure being a fully SaaS cloud offering, and there is no such migration. If VITA is asking about migration from an existing on-premise identity verification solution to SocureGov's SaaS Cloud Based solution, Socure offers a phased approach to implementation. Socure will work with VITA to design and implement decision logic based on the needs of the state in order to meet and exceed the capabilities of the current deployment. All future fraud evaluations and identity verification events will be processed via the newly implemented SocureGov solution. For identities verified using the legacy on-premise solution, a portfolio scrub will be conducted in order to provide maximum assurance that all good identities are properly marked as good, and all fraudulent identities are properly marked as fraud. Finally, it should be noted that all identities will remain inside of the Identity Access Management (IAM) solution, and migration of users of any kind will not be required for implementation of the SocureGov solution.
IMP13	CI/CD Capability	Provide a continuous integration (CI)/continuous deployment (CD) capability for on-premises, cloud, or hybrid solutions.	Y	New and updated Socure ID+ application code is deployed on a regular basis as part of Socure's continuous deployment methodology. Socure employs an Agile deployment process to release updated application versions to the Socure ID+ production system. Each release consists of a period of development, review, testing, and quality assurance review. Automated scripts are used in our Infrastructure as Code (IaC) tool to spin up instances and deploy software, which serves as a reset to the baseline configuration, and any unauthorized software that has been introduced to the environment will be terminated with the instances they are running on when the new deployment occurs. Our clients can grow, adapt and enhance their user experience without requiring technical change management processes to test implications to our identity & fraud SaaS offerings. Conversely, this functionality also affords the ability to instantly process updates to models and risk logic calibrations without impacting VITA online services.

Reporting				
Req. No.	**Category**	**Requirement**	**Yes (Y)**	**Provide an explanation of how the Solution fulfills the requirement. *The Supplier's detailed***
Reporting Requirements				
Supplier Responsibilities include:				
RPT01	Standard Reporting	Provide standardized reporting types supplied to Authorized Users. Include a list with descriptions of these reports.	Y	[redacted]
RPT02	Real Time Reporting	Describe your real-time or near real-time reporting capability. Explain details and timing of your reports.	Y	The Socure Dashboard provides a transaction list view, which displays all API requests processed by SocureGov for that account (if the user has appropriate permissions to view transactions) in near real-time. Transactions, audit event data and various subreport types are available for near real-time reporting. Socure provides a UI for executing a batch process to execute the report which then becomes available for download.
RPT03	Automated Reports	Describe automated reports that are run at a set time (daily, weekly, quarterly, monthly, Authorized User defined).	Y	Socure will provide regular reports on performance metrics, trends, and other aggregate data at regular intervals. When these reports show actionable data Socure will recommend optimizations. These reports are often customized to the needs of each customer, but typically include: • Transaction volumes per account and sub-accounts • PII firing rates • Email domain trends • Aggregate outcome performance (Accept, Reject, Review, Refer, Resubmit) • Top Reason Codes • Errors Fired
RPT04	Scheduled Reports	Describe the capability to schedule and distribute reports to Authorized Users automatically (via link, email, or other method).	Y	[redacted]
RPT05	Custom Reports	Describe the capability to create custom or advanced reports on an as-needed basis and the capability to export the data from those reports.	Y	
RPT06	Report Point of Access	Allow Authorized Users direct access to the Solution's reports.	Y	Socure provides an out of the box permission, which gives role based permission to either view reports or edit reports.
RPT07	Search	Allow Authorized User to search for detailed information about identity proofing events.		Socure provides out of the box permissions which can apply to roles that govern whether a user can create or view transactions. Permissions can also be applied that determine whether a user who can view transaction data can see sensitive PII data (social security number, date of birth and ip address remain masked for users with restricted permissions).
RPT08	Search Criteria	Describe the search functionality within Supplier's reporting (e.g., by name; by document number; by document type; by identity proofing outcome).	Y	[redacted]
RPT09	Visible Data	The Supplier's Solution must not display any PII data about a given End User.	Y	
RPT10	Role Based Access	Provide role-based access and management guidelines for the Supplier's reporting functions.	Y	All reporting functionality can be controlled through permissions and role-based assignments. Initial guidelines come from out of the box roles that cover most standard users. These out of the box roles can be copied and modified to meet more specific access configurations.

See Tab RPT02 - Repo

RPT11	Metrics Reporting	Describe established metrics and testing methodologies to assess platform performance and understand the impacts across End User populations.	Y	Socure believes that fair and equitable identity verification and fraud assessment should be a requirement of every identity solution provider. We apply these principles to each Socure machine learning model solution from start to finish. That means our approach persists from feature selection through entity resolution, as well as for investments we make in the data used to generate our best-in-class solutions. We do this as part of our overall governance process by creating Socure Disparate Impact Analysis reports for every model used in our services. The reports define protected classes by race and ethnicity, sex, immigration status, age (elderly and younger generations) and apply our analysis methodology to measure model performance for these classes against a base class. Metrics included in the analysis include area under the curve (AUC - the measure of model performance), acceptance rate, acceptance rate gap, and individual variable impacts on the model. We publish these reports so that clients are assured of Socure's performance superiority in the fair treatment of all user's identity proofing experience. Our reports list the specific testing methodologies used for the model.
		Tier 2 & 3 IDP Tech Support Reporting Requirements		
RPT12	Standard Reporting	Provide T2 and T3 standardized reporting types supplied to Authorized Users. Include a list with descriptions of these reports.	Y	Socure will provide Authorized Users reports detailing out the customers performance as well as firing rates and percentages of applicable reason codes. Additionally, these reports will include metrics on key performance indicators including, but not limited to, decision outcome percentages (accept, reject, refer, review, etc), traffic volumes and counts, and model distributions. Authorized Users will also have the ability to export raw information from the Reporting feature in the Admin Dashboard to utilize for custom reporting.
RPT13	Real Time Reporting	Describe T2 and T3 real-time or near real-time reporting capability. Explain details and timing of your reports.	Y	Socure will build Customed Reports and can be configured to send on a timely basis at the customers request (i.e. daily, weekly, monthly). Additionally, the Admin Dashboard provides an analytics service which will provide near real-time reporting of the key performance indicators of the integration, including traffic volumes, decision outcomes, and model distributions/performance metrics.
RPT14	Automated Reports	Describe T2 and T3 automated reports that are run at a set time (daily, weekly, quarterly, monthly, Authorized User defined).	Y	Socure will build Custom Reports and can be configured to send on a timely basis at the customers request (i.e. daily, weekly, monthly). Additionally, the Admin Dashboard provides an analytics service which will provide near real-time reporting of the key performance indicators of the integration, including traffic volumes, decision outcomes, and model distributions/performance metrics.
RPT15	Scheduled Reports	Describe T2 and T3 the capability to schedule and distribute reports to Authorized Users automatically (via link, email, or other method).	Y	Socure can schedule and distribute reports at the cadence requested by the customer, typically though email.
RPT16	Custom Reports	Describe T2 and T3 the capability to create custom or advanced reports on an as-	Y	As a part of the service, the Socure Account Management Team manages and configures
RPT17	Client portal	Describe the reporting platform portal for the Authorized User to access the reports.	Y	Socure's Administrative Dashboard will also provide VITA with integrated reporting
RPT18	Logging and	Describe logging and auditing features within the reporting platform.	Y	All incoming traffic through our endpoints are logged, the responses are stored, and made
		Implementation Reporting Requirements		
RPT19	Status Reporting	Describe Supplier's plan for project status reporting and frequency on the progress of	Y	As part of our certification process we engage with implementation stakeholders on a weekly
RPT20	System Reports	Describe system usage reports, e.g., API usage reports. A sample may be included.	Y	The Admin Dashboard includes reporting on transactions (API included) and audit events.

Training				
Req. No.	**Category**	**Requirement**	**Yes (Y) Future (F)**	**Provide an explanation of how the Solution fulfills the requirement. *The Supplier's detailed explanation should not simply be an affirmative reiteration of the question, but should***
Training Requirements				
Supplier Responsibilities include:				
TR01	Training Strategy	Provide a comprehensive training strategy and written training documentation for Authorized User(s).	Y	Socure training and technical integration support is bundled in as a component of the annual license fee. All documentation to support SocureGov integration is available 24/7/365 on Socure's Developer's Portal (DevHub). The portal is a web-accessible location, with user permissions managed by the customer administrator via the Administrator Dashboard that provides product overviews, API guides, FAQs, release notes and all other applicable content required to integrate the SocureGov platform modules. The Socure Account team meets regularly with customers before go-live to provide hands-on training and guidance during implementation. When preparing for go-live, Socure will provide additional training on all aspects of the SocureGov platform. These sessions will provide a deep dive on Socure's Administrative Dashboard and Developer's Portal - including new account provisioning, Document Verification and Verify Settings, and a host of other topics to ensure the tools available are well understood. These training events may be recorded by the Commonwealth for further dissemination, or held on multiple occasions for various user groups. Post go-live, Socure meets with customers regularly to implement and maintain the customer's desired performance. These meetings are intended to review product settings to optimize customer onboarding. There will also be quarterly executive touchpoints scheduled to discuss roadmap features, overall performance, and provide an update on fraud trends affecting Public Sector Clients.
TR02	Designated Testing Environment	The Supplier must offer a designated training environment for the proposed version of the solution. Include a detailed description of this environment and how it is maintained and updated.	Y	Every account comes with 3 environments: Sandbox, Certification and Production, each with its own set of API and SDK keys and the ability to restrict IP and domain access to each of these environments. For each customer account, it is recommended that Sandbox and Certification are utilized for implementation and training purposes, while Production is reserved for production traffic and deployment.

TR03	Ongoing Training	The Supplier must offer a process for ongoing training for Authorized User(s), e.g. new hires, enhancements and modifications to your solution, new features, etc.	Y	For upgrades, maintenance and change control, the state can engage any member of the Socure Account Management team. Additionally, Socure meets with customers on a quarterly basis to review enhancements to solution configurations that can benefit the identity verification and fraud detection performance. Socure communicates any applicable software changes via the Socure Developer's Hub release page found here. Customers can subscribe via email to be notified of module upgrades and other pertinent solution information. Additional details can be requested by contacting our 24/7/365 support function, or by request to one of the Account Management team members (Account Executive, Solutions Consultant, Technical Account Manager, and Strategic Account Manager) assigned to the account.
TR04	Online Training Materials	Provide online training materials about Supplier's proposed solution for End Users, i.e., self-help resources to use the solution. Explain any alternate delivery methods, if any.	Y	The solution will provide a FAQ and online self-help resources for the proposed solution - tailored to the state implementation and requirements.
TR05	Online Training Materials – Authorized User	Provide online training materials to the Authorized User's technical staff as self-help resources to use the solution. Explain any alternate delivery methods beyond online access, if any.	Y	Socure provides training during the implementation phase on our Admin Dashboard and Developer Portal resources. Materials from the training will be emailed to participants. Developer Portal resources are online and controled through permissions granted in the Admin Dashboard. Anyone that needs to get access to online documentation can do so through user provisioning.
TR06	Authorized User Group Community	Provide information about your user group community, if applicable, to the Authorized User(s) for the Supplier's Solution. Include a link and information about the user group. If the group is open only to contracted Authorized Users, please describe the format.	Y	Socure provides the opportunity to speak directly with our Product Management Team in a group setting. The Commonwealth will have the opportunity to provide a delegate to meet quarterly with other State customers to drive roadmap requests and product feature generation.
TR07	Remote and InPerson Identity Verification Sessions	Provide training materials that will allow Authorized User(s) to train their staff members so they can conduct supervised remote and in person identity verification sessions.	Y	Training will be provided to the Authorized User(s). It will be created specifically for the the Authorized users workflow that supports their application. The process should contain but not be limited to UI training, Definitions, FAQ's, Identity workflow processes, communication, and resolution tactics.

Communication				
Req. No.	**Category**	**Requirement**	**Yes (Y) Future (F) No (N)**	**Provide an explanation of how the Solution fulfills the requirement. *The Supplier's detailed explanation should not simply be an affirmative reiteration of the question, but should describe the manner in which the requirement is met.* Where possible and beneficial, please provide screenshots or graphics to help illustrate your response. Where your response is described as a future release or update as the provision, please provide a timeline for that provision. Supplier may also use this column to cross-reference a detailed explanation included as an attachment to its proposal.**
Communications Requirements **Supplier Responsibilities include:**				
COM01	OCM Plan	Describe Supplier's plan to manage the organizational change for this implementation. If Supplier has a sample version from a previous Organizational Change Plan, you may include a copy.	Y	Managing change/enhancement requests and bug reporting are critical to the success of a deployment of this scale. While some changes are inevitable and may produce an improved result or fix an error in operation, changes to the scope of a project may present risk to successful delivery of the overall task. Socure has managed a multitude of state and large-scale services and has developed a comprehensive change management process to control, evaluate and manage changes, issue correction, and enhancements to a project. The change request process will be completed by Socure's project team and will do the following: 1- Identify the change or new requirement(s) 2- Provide the reason for the change 3- Detail the expected benefit of the change Approved changes to existing services are implemented via the Change Management capacity. This capacity is highly aligned and integrated with the Project Management capacity in the overarching ALM framework and uses the same core processes, phases, deliverables, and milestones. Socure recognizes that change to an eGovernment service can occur during, after, and outside of formalized projects. Change Management adheres to the same core principles as the Project Management process. The ALM framework approaches Project Management as an associated capacity of Change Management, therefore providing the same processes, deliverables, and milestones applicable regardless of scope, scale, or schedule. This unified methodology allows stakeholders and Socure to coordinate in a unified, efficient, and consistent format regardless of the solution's scope or scale.
COM02	Project Documentation	The Supplier agrees to make project documents available online to the Authorized User(s) staff including but not limited to: work plans, status reports, status meeting agendas, minutes, etc. If this requirement is not possible, explain how the Supplier will provide project documents.	Y	Project documentation shall be made available at all time to the Authorized User(s) in an agreed upon electronic format, to be determined during project kickoff and configured to best meet the needs of the Authorized User(s).
COM03	Readability	The Supplier must ensure that abbreviations and acronyms are defined and consistent throughout the documentation. Provide a copy of your documentation.	Y	Consistent definitions and acronyms are essential for mutual communication, and are a vital aspect of any successful project. Having worked with partners not only across the entire spectrum of government, but also the private banking sector, Socure understands full well the need to arrive at a collective understanding around language, and to provide a bedrock of defintons to be used throughout the lifecycle of the engagement. Socure shall ensure that all documentation is fully consistent in this manner.

COM04	Document Updates	The Supplier agrees to update electronic versions of its documents upon any update and version check one time per year. Each version must have: ▪ All pages numbered within each section ▪ A new revision date on each page ▪ All revisions clearly identified in bold print	Y	Socure understands and agrees to provide the Authorized User(s) with supporting documentation, updated in a timely manner and no less than once per calendar year, to reflect versioning or updates to the solution. Pages shall be numbered within each section, with revisions tracked clearly and dated on each page.

Peformance Measures & Reports										Redaction Rationale
No.	**Title**	**Minimum Value**	**Description**		**Report or SLA**	**Frequency of Delivery**	**Reference**	**Yes (Y) Future (F) No (N)**	**Provide an explanation of how the Solution fulfills the requirement. *The Supplier's detailed explanation should not simply be an affirmative reiteration of the question, but should describe the manner in which the requirement is met.* Where possible and beneficial, please provide screenshots or**	
Service Level Agreements										
Supplier responsibilites include compliance with the following proposed SLAs Supplier is expected to utilize this information to propose Service Level Agreements using 'Appendix A Supplier Service Level Agreement document'.										
PM-SLA- 01	Availability	99.90%	A measurement of the identity proofing service that indicates a percentage of time when the service is available during a month divided by the total time available during the month. The Availability % is determined as follows: 100% X (Total Minutes in the Month – Total Minutes Unavailable in the Month)		SLA	Monthly		Y	Socure has teams in place to provide customer support, handle incidents, and provide high availability of 99.9%. Socure implements disaster recovery and contingency plans in accordance with FedRAMP Moderate control requirements.	
PM-SLA- 02	Accessibility	86%	Accessibility requirements are derived from Web Content Accessibility Guidelines (WCAG) 2 Level AA. The vendor must allow for monthly scanning by VITA contracted SiteImprove service. Refer to WEB-38.		SLA	Monthly	EA-Solutions-Web-Systems-Standard-(updated).pdf (virginia.gov)	Y	WCAG and VPAT are available upon request. Due to security concerns, we would like to discuss the requirement for monthly SiteImprove scans.	
PM-SLA- 03	Security Scanning	NA	All Critical and High vulnerability defects identified by monthly security scans must be resolved within 30 days of identification. Refer to WEB-151.		SLA	Monthly	EA-Solutions-Web-Systems-Standard-(updated).pdf (virginia.gov)	Y	Socure's current security scanning posture is to resolve critical and high vulnerability defects within 30 days.	
PM-SLA- 04	Penetration Testing	NA	All Critical defects identified by annual testing shall be remediated within 30 days of identification.		SLA	Annual	EA-Solutions-Web-Systems-Standard-(updated).pdf (virginia.gov)	Y	Socure's current penetration testing posture is to resolve critical defects identified within 30 days.	
PM-SLA- 05	Sales Reporting System	First Working day of the month	Invoices will be delivered to the VITA SRS on or before the First working day of the month for the previous month’s service.		SLA	Monthly		N	Billing is largely based on transactions for the month so invoicing before the end of the month would not accurately capture the full costs for the previous month. To address this we typically bill within the first 6 days of the month for the previous month.	
PM-SLA- 06	Billing Accuracy	95%	The number of VIP consumers who are verified (success or failure)during the month. (Note: this assumes requests for verification that are not achieved will result in no billing to VITA.)		SLA	Monthly		Y	Customer transactions that result in no response or an error are not billed.	
PM-SLA- 07	Recovery Point Objective (RPO)	1 Hour	The measurement of the point in time to which data must be restored to resume processing transactions. Directly related to the amount of data that can be lost between the point of recovery and the time of the last data backup.		SLA	Continuous	EA-Solutions-Web-Systems-Standard-(updated).pdf (virginia.gov)	Y	[redacted]	

PM-SLA- 08	System Performance	90%	Use the Chrome Extension called Google Lighthouse and run a performance test on the URL of the Identity Verification solution.	SLA	Monthly	https://developer.chrome.com/docs/lighthouse/overview/		As there will be a number of platforms and environments in play, Socure will collaborate with VITA and partners concerning performance testing, regardless of the tools used.
PM-SLA- 09	Recovery Time Objective (RTO)	24 Hours	The period in which systems, applications or functions must be recovered after an outage. See WEB-143.	SLA	Continuous	EA-Solutions-Web-Systems-Standard-(updated).pdf (virginia.gov)	Y	[redacted]
	Reporting							
	Supplier responsibilites include providing the following reports: **Supplier should utilize Columns I and J to respond with 'Y', 'N' or 'F' if they can meet the reporting requirements. Supporting rationale or documentation may be**							
PM-R-01	Verification Speeds	TBD	The average time it takes to complete Identity Verification of a VIP consumer for Identity Assurance Levels 1, 2, and 3. This measurement starts when the Identity Proofing solution receives a request to perform verification and ends when it sends a message to the VITA Identity Provider (ex. Okta CIAM) with the results (successful or failure). Requests where results cannot be achieved are not counted in this measurement.	Report	Quarterly		Y	Passive verification API requests take under 400ms, often 200ms or less. DocV takes <4 seconds to respond with an outcome once a user submits their selfie. Median time to complete document verification processes is between 1.4 and 1.9 minutes. Socure publishes events that can be used to track these values for reporting processes.
PM-R-02	Verification Achieved Rate	TBD	The percentage of requests to perform verification for Identity Assurance Levels 1, 2, and 3 having a successful result. A result is defined as a determine whether the identity verification was successful or not. This measurement is determined by counting the total number of requests where results were achieved (successful or failure) divided by the total number of requests.	Report	Quarterly		Y	Socure can report on the percentage of succesful requests and seperate them by request type. We can additionally report on errors and error type so that we can resolve why issues are occuring (such as malformed request data).
PM-R-03	Receiver Operating Characteristics (ROC) and Area Under Curve (AUC)	TBD	Updated ROC and AUC graphs or values will be updated and provided on a semi-annual basis. Measurements for True Positive (TP), False Positive (FP), True Negative (TN), False Negative (FN) values will also be provided.	Report	Semi-annual		Y	Socure can report on the ROC/AUC performance of the models in use by VITA. If VITA provides feedback data we can also report on TP, TN, FP, and FN. These would typically be values that we discuss during quarterly performance reviews.
PM-R-04			TP – accurately identifies the honest individual	TN – accurately identifies a fraud				If VITA provides feedback data we can report on TP, TN, FP, and FN. These would typically be values that we discuss during quarterly
PM-R-05			FP – incorrectly	FN – incorrectly identifies an honest				If VITA provides feedback data we can report
PM-R-06	Concurrent Users	200	Concurrent users are defined as those consumers who are actively interacting with the identity proofing service during an identity verification request.	Report	Semi-annual		Y	Socure can provide periodic reporting for transaction volume at points in time.

PM-R-07	Sales Reporting System (SRS)	First working day of the month	IFA payments will be delivered to the VITA SRS on or before the First working day of the month for the previous month.	Report	Monthly		Y	Billing is largely based on transactions for the month so resolution of IFA payments before the end of the month would not accurately capture the full differences for the previous month. To address this we typically resolve this type of balance within the first 6 days of the month for the previous month.
PM-R-08	Customer Satisfaction	NA	VIP consumers will be offered an opportunity to voluntarily respond to a survey concerning ease of use, likeability, and	Report	Semi-annual		Y	Socure will actively participate in semi-annual surveys for VIP.

OnPremises Responsibility Matrix					
Category	**Description**	**Requested Minimum Standard**	**Vendor Responsibility (Y/N)**	**Authorized User Responsibility (Y/N)**	**Provide an explanation of how the Solution fulfills the requirement. *The Supplier's detailed explanation should not simply be an affirmative reiteration of the question, but should describe the manner in which the requirement is met.* Where possible and beneficial, please provide screenshots or graphics to help illustrate your response. Where your response is described as a future release or update as the provision, please provide a timeline for that provision. Supplier may also use this column to cross-reference a detailed explanation included as an attachment to its proposal.**
On-Premises Solution Requirements					
Supplier is expected to determine which entity is responsible for the following funtions within the proposed Solution.					
Data & Configuration	Information cached and managed within the Authorized User's own data centers, servers, and network infrastructure.	No PII retained on Authorized User's servers.	N	N	N/A Socure's platform is entirely SaaS based, hosted within the FedRamp boundary. Any requirements that would pertain to an on-premise solution are N/A. The same question set has been answered Y in tab 17-Cloud Responsibility Matrix
Application Code	Vendor provided solution for the purpose of identity proofing.	Certified penetration testing. Application code will be kept up-to-date with the latest patches, security updates and releases within 30 days of availability.	N	N	N/A see response in cell F5
Capacity	Response to spike in traffic with additional server delivery or removal of underused equipment.	200 concurrent users	N	N	N/A see response in cell F5
Up Time & Availability	Amount of time the service is up and running without any unplanned downtime and volume of simultaneous users.	99.9% up time	N	N	N/A see response in cell F5
OS	Manages the operation, execution, and processes of on-premises machines, on-prem servers, and on-premises infrastructure, as well as the back-end hardware and software resources.	Ongoing patch management on latest OS version and patch. Patches are implemened within 30 days of their availability.	N	N	N/A see response in cell F5
Security	Maintain privacy of all data collected from users of identity proofing solution.	Configure firewalls, implement role-based access controls (RBAC) to restrict user permissions, encrypt data at rest and in transit, and regularly apply security patches to servers and software in compliance with SEC530.	N	N	N/A see response in cell F5
Virtualization/Containerization	Partitions a physical server into multiple virtual servers	Authorized User maintained.	N	N	N/A see response in cell F5
Hardware	Any physical device, e.g., hard drive, monitor, keyboard, mouse, etc.	Hardware replacement lifecycle completed by initial term of contract.	N	N	N/A see response in cell F5

Cloud Responsibility Matrix					
Category	**Description**	**Requested Minimum Standard**	**Vendor Responsibility (Y/N)**	**Authorized User Responsibility (Y/N)**	**Provide an explanation of how the Solution fulfills the requirement. *The Supplier's detailed explanation should not simply be an affirmative reiteration of the question, but should describe the manner in which the requirement is met.* Where possible and beneficial, please provide screenshots or graphics to help illustrate your response. Where your response is described as a future release or update as the provision, please provide a timeline for that provision. Supplier may also use this column to cross-reference a detailed explanation included as an attachment to its proposal.**
Cloud Solution Requirements					
Supplier is expected to determine which entity is responsible for the following funtions within the proposed Solution.					
Data & Configuration	Information managed via cloud services, i.e., any personally identifiable information (PII) temporarily cached for the purpose of identity proofing.	No PII retained on Vendor's virtual environment.	Y	N	PII retention periods are configurable, pursuant to regulations and policies set by Socure's Customers. There is a tradeoff between between retention of PII and overall performance, as velocity of PII attributes will not be possible in this case. But PII retention is not required.
Application Code	Vendor provided solution for the purpose of identity proofing.	Certified penetration testing. Application code will be kept up-to-date with the latest patches, security updates and releases within 30 days of availability.	Y	N	Socure complies with FedRAMP standards for all patching as outlined below: Security vulnerabilities are required to be remediated according to the FedRAMP SLA: 15 days for Critical vulnerabilities (Socure SLA) 30 days for Critical (any outstanding) and High vulnerabilities 90 days for Medium vulnerabilities 180 days for Low vulnerabilities
Scaling	Adaptability to traffic spikes	Unlimited	Y	N	The Socure solution is hosted in AWS GovCloud, and as a result can scale virtually to account for traffic spikes - spinning up new VMs on demand. We have tested our solution to support 1,200 transactions per second.
Up Time & Availability	Amount of time the service is up and running without any unplanned downtime and volume of simultaneous users.	99.9%	Y	N	Socure's standard SLA is 99.9% uptime.
OS	Manages the operation, execution, and processes of virtual machines, virtual servers, and virtual infrastructure, as well as the back-end hardware and software resources.	Ongoing patch management on latest OS version and patch. Patches are implemened within 30 days of their availability.	Y	N	Socure complies with FedRAMP standards for all patching as outlined below: Security vulnerabilities are required to be remediated according to the FedRAMP SLA: 15 days for Critical vulnerabilities (Socure SLA) 30 days for Critical (any outstanding) and High vulnerabilities 90 days for Medium vulnerabilities 180 days for Low vulnerabilities
Security	Maintain privacy of all data collected from users of identity proofing solution.	Configure firewalls, implement role-based access controls (RBAC) to restrict user permissions, encrypt data at rest and in transit, and regularly apply security patches to servers and software in compliance with SEC530.	Y	N	Socure complies with FedRAMP standards for firewalls, Role-Based Access Control, Data Encryption (FIPS Compliant), and regularly applies server and software patching in accordance with those controls - which is a more stringent version of NIST 800-53 based SEC530 standards.
Virtualization/Containerization	Partitions a physical server into multiple virtual servers.	Vendor maintained.	Y	N	Socure provides uniquely dual-encrypted server space for each client, which is keyed at the disc and application levels. Security and management tools in separate VPCs are segmented using subnets for logical separation between public-facing components and backend components.
Hardware	Physical device, e.g., hard drive, monitor, keyboard, mouse, etc.	Vendor maintained.	Y	N	Socure maintains all required hardware to perform the requirements of the State.