

Cloud Questionnaire

IOT Mapping Doc for Cloud Solution	CGID	CID	NIST 800-53 Mapping	NIST Security Control Family	Control Specification	Assessment Question	Provider:			
							Assessment Response			
							Yes	No	N/A	Explanation of response
Cloud Classification & Configuration	CCC-1	CCC-1.0	EC -1		Ensures appropriate information security guards are established.	Is the cloud solution you are proposing a Software as a Service, Platform as a Service, or Infrastructure as a Service Delivery Model	✓			As a government agency, Indiana Department of Workforce Development (DWD) will benefit from a software development model that is not only cost effective, but also easy to deploy and maintain. Geographic Solutions is proposing a Software-as-a-Service (SaaS) operating model as the solution for DWD.
Cloud Classification & Configuration	CCC-2	CCC-2	EC - 2		Establishing, monitoring, and operating IT systems in a manner consistent with IOT Information Security policies and standards	Are you offering Public, Private or government cloud? Please describe the solution support model.	✓			Geographic Solutions is proposing a Software-as-a-Service (SaaS) operating model as the solution for DWD. Geographic Solutions first introduced this model to the workforce industry with our subscription offering in 1999. We currently support this exact model in 32 state workforce systems. Our SaaS model has allowed multiple state Case Management and Labor Exchange System agencies to completely eliminate any reliance on their own technical resources. We offer annual or multi-year agreements for hosting, maintenance, and upgrades, thus accommodating future technology refreshes, product evolution, and any updates required to comply with changes in applicable laws. We deliver product features seamlessly, and we ensure system updates and maintenance activities continuously enhance the client experience with the system. In addition to our time-tested SaaS model deployed in our own private cloud computing environment, Geographic Solutions can provide the same level of performance and reliability through implementation on a public cloud service. Geographic Solutions’ two state-of-the-art and geographically diverse production hosting facilities (east and west coast) house all of the infrastructure required to support the system demands generated by large, mission critical applications, such as the proposed Case Management and Labor Exchange System. This private cloud infrastructure provides elasticity to support the peaks and valleys in usage and traffic flows. Both of our hosting facilities provide continuously reliable and uninterrupted service. This includes full redundancy made possible by real-time replication of data across our hosting facilities, which eliminates any chance of data loss due to interruption in service. While technically different at the component and configuration levels, our public cloud offering delivers the same results in terms of reliability, performance, and flexibility. With either private or public cloud hosting, Geographic Solutions’ SaaS solutions require no additional hardware or third-party software purchases. There will also be no requirement for a DWD webmaster, system administrator, programmer, or database expert to support the system. Our technical support staff will provide all required infrastructure support, database management services, and system updates. [REDACTED]
Access Control: Policies & Procedures	ACP-1	ACP-1.1	AC-1	Technical	Develops, documents, and disseminates to all organization personnel, contractors, and service providers with a responsibility to implement access controls:	Does the provider have access control policies and procedures that are reviewed and/or updated at least annually or required due to environmental changes?	✓			Geographic Solutions has chosen to adopt the Access Control principles established in NIST SP 800-53 “Access Control” Control Family guidelines as the official policy for this domain. Our GSI-OPS-130-PL Controlled Document Management Program Policy describes the proper management and maintenance of controlled documents at Geographic Solutions, Inc., including at least an annual review of all of our Policies, Procedures, and Standards.
		ACP-2.1		Technical	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Does the solution have the capability to identify and select the following types of accounts: Individual, group, System, Service, Application, Guest/anonymous and temporary?	✓			Within the <i>VOS Sapphire 22</i> Administration System, authorized administrators can manage the security and access levels of all users. They can allow or disallow access to screens and screen functions by role, office, staff member, etc. The Administration System provides the ability to create role-based workgroups as “Access Groups” and to define their related privileges. Administrators can define the privileges by program areas or geographic locations, or by many other factors.
		ACP-2.2		Technical	Does the provider have the capability to segment and identify administrative accounts by tenant?	✓			Geographic Solutions segregates data by providing individual environments for each client. [REDACTED]	

Access Control - Account Management	ACP-2	AC-2	Technical		Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	✓			At Geographic Solutions, our physical and environmental security is designed to prevent unauthorized access and damage to, or interference with, IT services. We restrict and monitor access to all hosting facilities, staff offices, computer machine rooms, network switch rooms, and other work areas. All hosting facilities supporting critical or sensitive business and production activities are physically protected from security threats and environmental hazards. We identify risks and establish suitable physical and environmental controls for all secure areas and information-processing equipment. This ensures proper security and prevents opportunities for malicious or unauthorized activities.		
			ACP-2.3		Technical	Does provider document how access to tenant data is granted and approved?	✓			Geographic Solutions has chosen to adopt the Personnel Security principles established in NIST SP 800-53 “Personnel Security” Control Family guidelines, as the official policy. Our GSI-SEC-150-PS Policy documents our personnel security policy, including how access to DWD data is granted and approved. Only employees who are authorized, in writing by the Geographic Solutions’ Director of Operations, have access to the secure, hosted environment. Internal policies and practices strictly govern the approval process for such access. Geographic Solutions grants such access only to employees with the proper security credentials and job assignments within the specific hosted environments. Each of these individuals has signed an additional confidentiality agreement. A user with a business need to access tenant data must create an "Elevated Access" request. The request includes the reason the person needs the access, what level of access, and how long the access is needed. Once submitted, the request is approved by the Department Director, Chief Information Security Officer, and the Director of Operations.	
			ACP-2.4		Technical	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?	✓			Upon termination of an individual’s employment, Geographic Solutions performs a same-day access revocation from the information system. The user’s account is first disabled in the Active Directory, and then the Security Department and the Systems Team will systematically disable all other logins not controlled through Active Directory, such as web portal logins that might be required based on the user’s role. When the user’s account is disabled in Active Directory, it instantly terminates access to the network, VPN, and other VOS application production systems to which the user may have had access. In addition, the Termination Checklist provides a workflow for other areas to check for access revocation.	
			ACP-2.5		Technical	Do you provide tenants with documentation on how segregation of duties within proposed cloud service offering are maintained? Please provide copy of procedure(s)	✓			Geographic Solutions segments duties through different departments: The Directors of Development are responsible for the development and unit testing of the Data Access Policy. Developers do not have access to any environment outside of the Dev environment. Please see Appendix Q - Data Access Policy for data access restrictions. The Director of Quality Assurance is responsible for the manual and automated testing of the Data Access Policy. Once tested, the Director of QA's team deploys the code and configures the application. The Chief Information Security Officer is responsible for the Static and Dynamic scanning of the Virtual OneStop Application as well as the security of Geographic Solutions' infrastructure. The Director of Operations is responsible for the company's infrastructure including the building and configuration of Virtual OneStop Applications web and SQL servers and monitoring of the company's infrastructure and application. The access to all company assets is managed with Microsoft's Active Directory Groups; permissions are granted on the least privilege basis.	
			ACP-2.6		Technical	Control Enhancements for Sensitive Systems Removal of Temporary/Emergency Accounts.	Does the provider or solution automatically terminate temporary and emergency accounts after a predetermined period which is not to exceed 30-days in accordance with sensitivity and risk? Please provide copy of procedure(s)	✓			Geographic Solutions grants access on a need to know basis and for the shortest amount of time. Access is granted by the company's Online Project Communications (OPC) application and once approved it connects to the SecretServer application which grants access. The in user does not have access to the password and the password is rotated after the users' access has expired. Please see Appendix R - Server Access within the .NET Domain Procedure for a copy of our procedure.
			ACP-2.7				Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	✓			Electronic transacted system data routes through a defense-in-depth architecture and uses native SQL Server encryption and TLS certificate protection. To secure Internet communications in <i>VOS Sapphire 22</i> , Geographic Solutions uses strong encryption protocols with Secure Hypertext Transfer Protocol (HTTPS) to encrypt sessions between the server and web users. Geographic Solutions uses Secure Shell (SSH) File Transfer Protocol (also called Secure File Transfer Protocol or SFTP) for secure data file transfers.
							Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	✓			In support of maintaining security and enforcing McAfee and Windows Integrated security as an enterprise policy, only Windows-authenticated accounts generated by the Geographic Solutions Operations Group will have additional privileges based on written authorization from senior managers knowledgeable in the special needs and requirements of each position. [REDACTED]

Access Control - Separation of Duties	ACP-4	ACP-4.1	AC-4			Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only? Provide documentation on controls in place to prevent unauthorized access.				Geographic Solutions strictly controls administrative rights and controls, especially those related to monitoring, sniffing, and other security related activities. Comprehensive controls are in place to limit and monitor read/write/update access to the VOS Sapphire production source code, databases, and the servers on which they reside. Geographic Solutions grants access only to a restricted group of qualified individuals (least privileged). Only those Geographic Solutions staff members performing services under the Service Level Agreement will have access to DWD data. Geographic Solutions' team members with access to DWD data will sign a non-disclosure agreement. Geographic Solutions will not sell or share the data in any way. All Geographic Solutions staff with access to confidential, sensitive data have signed our thorough company confidentiality agreements, have undergone third-party background checks, as well as state of Florida level II security checks, and have signed various required government confidentiality agreements, such as those associated with the State Wage Interchange System (SWIS). In support of maintaining security and enforcing McAfee and Windows Integrated security as an enterprise policy, only Windows-authenticated accounts generated by the Geographic Solutions Operations Group will have additional privileges based on written authorization from senior managers knowledgeable in the special needs and requirements of each position. Before we grant elevated entitlements to personnel in special trust positions, they must execute specialized confidentiality agreements (in addition to the agreement signed by all employees). Both direct access and controlled security environments (with troubleshooting software) are available to support direct data troubleshooting and the temporary creation of a troubleshooting platform to allow a developer to debug site problems. Granting additional privileges necessary to perform authorized job functions requires a Database/Code Access Request to track the data access and privilege change. Designated senior staff must approve the request and then routes it to the Geographic Solutions Database Administration Team for implementation. The VOS Sapphire application code is compiled and signed prior to being promoted to a production-level environment; this ensures the code that was packaged for deployment is the code that was deployed and the code has not been tampered with. [REDACTED]
Access Control - Least Privilege	ACP-5	ACP-5.1	AC-5	Technical	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Do you document how you grant and approve access to tenant data? Please procedure for doing this.				Only those Geographic Solutions staff members performing services under the Service Level Agreement will have access to DWD data. Geographic Solutions' team members with access to DWD data will sign a non-disclosure agreement. Geographic Solutions will not sell or share the data in any way. All Geographic Solutions staff with access to confidential, sensitive data have signed our thorough company confidentiality agreements, have undergone third-party background checks, as well as state of Florida level II security checks, and have signed various required government confidentiality agreements, such as those associated with the State Wage Interchange System (SWIS).
		ACP-5.2		Technical		Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?				In support of maintaining security and enforcing McAfee and Windows Integrated security as an enterprise policy, only Windows-authenticated accounts generated by the Geographic Solutions Operations Group will have additional privileges based on written authorization from senior managers knowledgeable in the special needs and requirements of each position. Before we grant elevated entitlements to personnel in special trust positions, they must execute specialized confidentiality agreements (in addition to the agreement signed by all employees).
		ACP-5.3		Technical		Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?				Both direct access and controlled security environments (with troubleshooting software) are available to support direct data troubleshooting and the temporary creation of a troubleshooting platform to allow a developer to debug site problems. Granting additional privileges necessary to perform authorized job functions requires a Database/Code Access Request to track the data access and privilege change. Designated senior staff must approve the request and then routes it to the Geographic Solutions Database Administration Team for implementation.
		ACP-6.1		Technical	Enforces a limit of 3 consecutive invalid logon attempts by a user during a 15 minute period;	Do you allow tenants/customers to define password and account lockout policies for their accounts? Provide system password requirements and policies.				The <i>VOS Sapphire 22</i> application can disable a login after a predefined number of failed password entry attempts. It will allow a predefined number of unsuccessful attempts (determined by an administrator setting) before locking a user out and disabling his or her login. [REDACTED]

Access Control - Unsuccessful Logon Attempts	ACP-6	ACP-6.2	AC-6	Technical	Automatically locks the account/node for a minimum of a 30 minute period when the maximum number of unsuccessful attempts is exceeded.	Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement? Please provide policies for both standard and admin accounts.	✓			The <i>VOS Sapphire 22</i> application includes system parameters to define many defaults, including username and password requirements. The application's rules for password complexity are configurable. DWD can set the required mix of minimums and maximums for length, letters, upper/lower case, numerals, and special characters, although Geographic Solutions recommends a minimum password length of eight characters which includes one capital letter, one special character, and one number (check with Indiana's Chief Information Security Officer to verify the minimum requirements). Beyond the strong password rules and the minimum and maximum password configuration, DWD can define other specific configuration rules, if desired. For example, the system can require that the password never include the user ID. The system also has the ability to disable users' accounts when they exceed a specified number of unsuccessful login attempts. Check with Indiana's Chief Information Security Officer to verify the minimum requirements. System administrators can configure <i>VOS Sapphire 22</i> to display password expiration and reset warnings. This setting can be the same or different for each user type (e.g., job seekers, employers, staff, etc.). It can include additional rules (via settings) such as, whether the user can reuse previous passwords, the time period after which they can reuse passwords, etc. Agency staff cannot adjust this feature. <i>VOS Sapphire 22</i> administrators can establish a setting that times out users' sessions and requires them to reenter their login and password to reenter the system. The amount of time before session timeout can be set separately for each user type, such as for employers, staff, individuals, providers, administration, analysts, and even guest users. The system can also be set to alert users of an impending timeout
		ACP-6.3		Technical	Password Policy must meet or exceed minimum password policies.	Do you support tenant defined password complexity policies? Specify your password length and complexity requirements in the notes field	✓			The application's rules for password complexity are configurable. DWD can set the required mix of minimums and maximums for length, letters, upper/lower case, numerals, and special characters, although Geographic Solutions recommends a minimum password length of eight characters which includes one capital letter, one special character, and one number.
Awareness and Training - Policy and Procedures	ATP-1	ATP-1.1	AT-1 AT-2 AT-3 AT-4	Operational	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	✓			All personnel receive security training within the first 30 days of employment and the special trust positions receive additional training on the unique security aspects and needs of their sensitive positions (e.g., developers are trained on the OWASP Top 10). All employees participate in annual security awareness training and every employee is tested throughout the year by random phishing campaigns.
		ATP-1.2		Operational		Do you document employee acknowledgment of training they have completed?	✓			Yes, Geographic Solutions documents and monitors individual information system security training activities including basic security awareness training and specific information system security training and retains individual training records for at least 3 years.
		ATP-1.3		Operational		Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	✓			Geographic Solutions restricts employees, under any circumstances, from sharing or providing any access that could expose personally-identifiable information received, processed, and stored in the <i>VOS Sapphire 22</i> application. Geographic Solutions facilitates information sharing by enabling authorized users, defined as Manager-level and above, to determine whether access authorizations assigned to a sharing partner match access restrictions outlined in a signed NDA (Non-Disclosure Agreement).
		ATP-1.4		Operational		Is successful and timely completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	✓			Geographic Solutions provides role-based security training to personnel with assigned security roles and responsibilities prior to granting access to the information system or performing assigned duties, and at least annually thereafter.
		ATP-1.5		Operational		Are personnel trained and provided with customer defined awareness programs at least once a year?	✓			Yes, Geographic Solutions will require employees to take and pass Customer defined awareness programs annually.
Audit and Control -Audit and Accountability	AUC-1	AUC-1.1	AU-1	Technical	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you produce audit assertions using a structured, industry accepted format (e.g., Cloud Audit/A6 URI Ontology, Cloud Trust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	✓			Service Organization Controls (SOC) ® are a series of accounting standards that measure the security and control of information for a service organization. A service auditor's examination performed in accordance with the Statement on Standards for Attestation Engagements (SSAE) represents that a service organization has been through an in-depth audit of its control objectives and control activities, including controls over information technology and related processes. The SSAE is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA).
		AUC-1.2		Technical		Are your audits performed at least annually? if no, please describe in the comments section.	✓			Geographic Solutions undergoes SSAE audits annually. The audit reviews and assesses the broad range of internal controls we set to verify that our personnel, facilities, systems, and software operate securely and effectively for our business services.
		AUC-1.3		Technical	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	✓			The SOC reports are a series of internal control findings on the services provided by Geographic Solutions as a service organization, which are conducted by an independent auditor. [REDACTED]
		AUC-1.4		Technical		Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	✓			As a standard part of our security procedures, Geographic Solutions' systems undergo penetration and vulnerability testing. We conduct this testing internally and contract with a third-party vendor to conduct this testing, as well. We also review system updates weekly to determine what new vulnerabilities have surfaced, and we test the critical operating system patches on internal development and test environments before loading them to production or passive production systems. Geographic Solutions performs internal penetration and vulnerability testing continuously and conducts third-party testing annually. We then correct any vulnerabilities and risk factors when we find them.
		AUC-1.5		Technical		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	✓			Yes, Geographic Solutions has subjected the <i>VOS Sapphire 22</i> application and infrastructure to numerous external vulnerability tests, and the system has passed them all.

		AUC-1.6		Technical		Are the results of the penetration tests available to tenants at their request?	✓			Geographic Solutions will provide a Security/Penetration Test report explaining the performed security/penetration test results. The results of the Security/Penetration Test report will meet the acceptable security/penetrating testing standards criteria as acceptable to DWD.
		AUC-1.7		Technical		Are the results of internal and external audits available to tenants at their request?	✓			Geographic Solutions will provide internal and external audit results to DWD at their request.
Audit and Control: <i>Audit Events</i>	AUC-2	AUC-2.1	AU-2	Technical	An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet	Is the solution capable of auditing the following events? Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events.	✓			The <i>VOS Sapphire 22</i> application provides full, ad-hoc, account activity tracking capabilities to track actions taken by authorized users, track unauthorized attempts to access the system, or alter data/information by authorized and unauthorized staff. The <i>VOS Sapphire 22</i> application reports include information about suspicious activity in the system. Staff use these reports to determine if users are potentially misusing the <i>VOS Sapphire 22</i> application.
		AUC-2.2		Technical	Audit events on Web Applications	Is the solution capable of auditing the following events, for Web applications? All administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission	✓			<i>VOS Sapphire 22</i> logs a full audit trail of user actions within the system. An audit trail is accessible to all authorized staff. Additionally, the system generates alerts in Syslog format, which is consumed and monitored by Geographic Solutions' Security Information and Event Monitoring (SIEM) system.
Audit and Control: Audit Review, Analysis, and Reporting	AUC-3	AUC-3.1	AU-6	Technical	Audit Review, Analysis, and Reporting	Is the solution capable of automated mechanisms to centrally review, analyze and correlate audit and log records from multiple components of the solution to support organizational processes for investigation, alerting and response to suspicious activities? Is the	✓			<i>VOS Sapphire 22</i> Security Information and Event Monitoring (SIEM) system automates the collection, review, analysis, and correlation audit and log records from multiple components of the solution to support organizational processes for investigation, alerting, and response to suspicious activities. The information is not available to tenants.
Control Assessment and Authorization	CAA-1	CAA-1.1	CA-1 CA-3 CA-7	Management	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant	✓			Geographic Solutions performs annual Type 2 SOC 2 and Type 2 SOC 1 reports which will be shared with DWD on an annual basis or a GAP / Bridge letter stating the status of Geographic Solutions' environments.
		CAA-1.2		Management		Do you conduct risk assessments associated with data governance requirements at least once a year?	✓			Geographic Solutions follows the National Institute of Standards and Technology Special Publication (NIST SP) 800-37 guidelines for applying the Risk Management Framework to our case management and labor exchange systems. The framework includes the activities for security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. Geographic Solutions implements security safeguard controls, as defined in NIST SP 800-53, and follows the guidelines provided in NIST SP 800-53A. We maintain a compliant FISMA/FedRAMP Moderate system for planning, policies, assessments, and audits of the new Case Management and Labor Exchange system, the environments, the equipment used to support it, and the personnel who operate and maintain the environment and the application. The Security Department completes and reassesses the risk categorization of the <i>VOS Sapphire 22</i> System and supporting infrastructure in accordance with the Federal Information Processing Standards (FIPS) 199 System Categorization guidelines on an annual basis.
Configuration Management - Policy and Procedures	CMP-1	CMP-1.1	CM-1	Operational	Organization shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services	Do you provide your tenants with documentation that describes your quality assurance process?	✓			Evaluations examine the activities Geographic Solutions uses to develop/deliver products and services, ultimately determining if the activity is fulfilling requirements. The Quality Assurance Department establishes criteria for an evaluation, verifies the performance of the process, and collects the metrics to describe the results of those activities.
		CMP-1.2		Operational		Is documentation describing known issues with certain products/services available?	✓			Geographic Solutions will generate and maintain all required test documentation. Geographic Solutions will provide regular quality assurance reports to DWD using the metrics from this documentation. The Geographic Solutions Project Manager will prepare and submit the Quality Assurance status reports for all phases of the project. Geographic Solutions uses a standard format and layout for status reports, which we will present to DWD for approval.
		CMP-1.3		Operational		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings? Are tenants provided with documentation on remedied issues?	✓			Information on system upgrades, enhancements, bug fixes, and details of what has changed, as well as when the change occurred and why is available on the OPC system. Therefore, authorized DWD personnel will be able to access all this information, at any timeframe, online.
		CMP-1.4		Operational		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions? Are there technical controls in place to prevent?	✓			Geographic Solutions will utilize various methods and techniques to ensure effective test results, depending on the specific quality assurance activity, including walkthroughs, reviews, audits, evaluations, and process improvements. Geographic Solutions' overall test management approach ensures a high quality system that meets user acceptance criteria. During the initial Go Live of a new system or an upgrade to a new version, both the Manual Quality Assurance and the Automation Quality Assurance Teams regression test the entire system. Both teams review checklists of use cases tested on the production environment during a deployment event. The Automation Quality Assurance Team runs hundreds of test scripts on the production environment during Go Live deployment events to verify system quality. We release the production environment to DWD for approval only after both Quality Assurance Teams have tested all of the use cases thoroughly.
		CMP-1.1		Operational	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	✓			Geographic Solutions uses detailed internal assessment procedures to ensure a hardened control implementation and to verify those controls are operating as intended and producing the desired outcome with respect to meeting the security requirements for the entire system. We annually receive SOC 1 Type 2 and SOC 2 Type 2 audits, along with third-party vulnerability and penetration testing/assessments, which confirm the effectiveness of our control structure.

	CMP-2	CMP-1.2	CM-2 CM-3 CM-7	Operational		Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	✓			Geographic Solutions strictly prohibits violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations including, but not limited to, the installation or distribution of "pirated" or other software products not appropriately licensed for use by Geographic Solutions. Geographic Solutions strictly prohibits unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Geographic Solutions or the end user does not have an active license.
		CMP-1.3		Operational		Can you provide evidence that the proposed solution adheres to a security baseline, which is based on least functionality?	✓			Authorization mechanisms are in place to clearly define user types, and ensure the least privileged stance of operation and authorization are continuously challenged.
		CMP-1.4		Operational		Are all changes to proposed solution authorized according to change management policies?	✓			Geographic Solutions uses a strict change control process to ensure the impact of any proposed change to the project definition or specific components of the project (such as hardware or software deliverables or a business process associated with a service) are thoroughly understood, carefully considered, and formally approved.
Contingency Planning - Information System backup	CP-1	CP-1.1	CP-2 CP4 CP-6 CP-7 CP-9 CP-10	Operational	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: <ul style="list-style-type: none">• Defined purpose and scope, aligned with relevant dependencies• Accessible to and understood by those who will use them• Owned by a named person(s) who is responsible for their review, update, and approval• Defined lines of communication, roles, and responsibilities• Detailed recovery procedures, manual work-around, and reference information• Method for plan invocation	Do you provide tenants with geographically resilient hosting options?	✓			Geographic Solutions’ two state-of-the-art and geographically diverse production hosting facilities (east and west coast) house all of the infrastructure required to support the system demands generated by large, mission critical applications, such as the proposed Case Management and Labor Exchange system. This private cloud infrastructure provides elasticity to support the peaks and valleys in usage and traffic flows. Both of our hosting facilities provide continuously reliable and uninterrupted service. This includes full redundancy made possible by real-time replication of data across our hosting facilities, which eliminates any chance of data loss due to interruption in service. While technically different at the component and configuration levels, our public cloud offering delivers the same results in terms of reliability, performance, and flexibility.
		CP-1.2		Operational		Do you provide tenants with infrastructure service failover capability to other providers?	✓			Geographic Solutions’ active/passive database cluster solution provides the flexibility to create a group of independent servers, which act as a single system, resulting in higher availability and reliability. Automatic failover, based on preset conditions, allows rapid failover, restart, and recovery. Auditing and clustered servers mean database administrators have ready access to all logs for current and historical status, as well as post-event troubleshooting and analysis.
		CP-1.3		Operational		Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	✓			Geographic Solutions has a fully developed, tested, and published Disaster Recovery and Business Continuity plan. The plan prepares for and ensures full continuity of critical services in the event of a disaster at the primary data center. Geographic Solutions updates and tests the Disaster Recovery and Business Continuity Plan regularly. To ensure the team members can perform their responsibilities when or if they are ever needed, Geographic Solutions holds semi-annual tabletop training that walks through each phase of a disaster or an event that would require an activation of the Business Continuity Plan. The Disaster Recovery and Business Continuity Plans are also tested annually to verify the company’s documentation is up-to-date and that each team member understands his or her responsibilities.
		CP-1.4		Operational		Can the solution provide and maintain a backup of SOI data that can be recovered in an orderly and timely manner within a predefined frequency consistent with recovery time and recovery point objectives?	✓			Scheduled, automated and fully encrypted backups of all applications, data, and system files provide support for the recovery of the production environment in the event of hardware and software problems. [REDACTED]
		CP-1.5		Operational		Can the solution store a backup of SOI data, at least daily, in an off-site “hardened” facility, located within the continental United States, maintaining the security of SOI data?	✓			In order to protect the new Case Management and Labor Exchange System in the event of a hardware and/or software malfunction, [REDACTED] This serves to ensure no transactions are lost, with the possible exception of in-process transactions. In addition to the continuous, onsite transactional data log backups to capture data changes throughout the production day (which gives us point-in-time recovery ability to reduce data loss in the case of an outage), this proposal includes the maintenance and support of a full-service disaster recovery and business continuity facility for the proposed Case Management and Labor Exchange system. The disaster recovery emergency hosting facility in California will house standby equipment, programmed and ready to assume the primary hosting responsibilities for essential production services if circumstances call for disaster recovery.
		CP-1.6		Operational		Can the solution partition, in aggregate for this proposal, all SOI data submitted into the solution by the data owner in such a manner that it will not be impacted or forfeited due to E-discovery, search and seizure or other actions by third parties obtaining or	✓			Geographic Solutions builds database servers to meet individual client requirements for data growth, while adhering to their need for data segregation. We manage Microsoft SQL security and access to each server and database individually to enforce restricted access to sensitive data. Geographic Solutions is proposing that the data servers will be exclusive to the Indiana Case Management and Labor Exchange System Project so they remain segregated physically as well as virtually. This will provide maximum security and performance.
Identification and Authentication; Organizational Users	IDA-1	IDA-1.1	IA-1	Technical	Vendor should have An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	✓			Only employees who are authorized, in writing by the Geographic Solutions’ Director of Operations, have access to the secure, hosted environment. Internal policies and practices strictly govern the approval process for such access. Geographic Solutions grants such access only to employees with the proper security credentials and job assignments within the specific hosted environments. Each of these individuals has signed an additional confidentiality agreement (in addition to the agreement signed by all other employees) and they recertify the agreement annually.
		IDA-1.2		Technical						
		IDA-1.3		Technical		Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls	✓			Each individual accessing the system has signed an additional confidentiality agreement (in addition to the agreement signed by all other employees) and they recertify the agreement annually.

Identification and Authentication; Authenticator Management	IDA-2	IDA-1.1	IA-2 IA-5	Technical	Internal agency or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	✓			The <i>VOS Sapphire 22</i> Single Sign-On component allows the <i>VOS Sapphire 22</i> application and other partner systems to share a common repository of usernames and passwords for authentication purposes. DWD can choose to employ single sign-on architecture and can adjust and enforce password expiration frequency rules. Geographic Solutions can implement this using the LDAP and Active Directory domain controllers.
		IDA-1.2		Technical		Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	✓			Geographic Solutions' Single Sign-On architecture supports a wide variety of protocols, which include, but is not limited to, LDAP, Kerberos, and Security Assertion Markup Language (SAML) 2.0, WS-Federation and OAuth 2.0, which fully integrate with most single sign-on technologies.
		IDA-1.3		Technical		Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	✓			Physical protective measures protect the environment where Geographic Solutions stores the data. All hosting facilities have a limited access list and all employees assigned to this list undergo thorough screening and training and also have the authorization to perform system administration duties. The minimum access, locked facilities have multiple forms of positive access identification controls and monitoring tools. Each component has unique, assigned authentication access controls known only to those with authorized access. The <i>VOS Sapphire 22</i> application can integrate with Lightweight Directory Access Protocol (LDAP) directory services, allowing for the provisioning and synchronization of identities for centralized identity management. LDAP is a standard for directory services in a network. It allows the sharing of information about users, systems, networks, services, and applications throughout the network. LDAP can be used by the <i>VOS Sapphire 22</i> application to provide a central place to store usernames and passwords. This allows many different applications and services to connect to the LDAP server to validate users.
		IDA-1.4		Technical		Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?	✓			The system has an option to establish Strong Resource Access Control Facility (RACF) rules for passwords, including the expiry requirements, character/number combination requirements, and other password policy enforcement.
		IDA-1.5		Technical		Do you allow tenants to use third-party identity assurance services?	✓			Geographic Solutions' <i>VOS Sapphire 22</i> has integrated with various third-party identity assurance services such as IDme.
		IDA-1.6		Technical		Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?	✓			The <i>VOS Sapphire 22</i> application includes system parameters to define many defaults, including username and password requirements. The application's rules for password complexity are configurable. DWD can set the required mix of minimums and maximums for length, letters, upper/lower case, numerals, and special characters, although Geographic Solutions recommends a minimum password length of eight characters which includes one capital letter, one special character, and one number (check with Indiana's Chief Information Security Officer to verify the minimum requirements). Beyond the strong password rules and the minimum and maximum password configuration, DWD can define other specific configuration rules, if desired. For example, the system can require that the password never include the user ID. The system also has the ability to disable users' accounts when they exceed a specified number of unsuccessful login attempts.
		IDA-1.7		Technical		Do you support the ability to force password changes upon first logon?	✓			The VOS Sapphire application includes ability to force password changes upon first logon.
		IDA-1.8		Technical		Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual	✓			The VOS Sapphire application includes a mechanism for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock).
		IR-1.1		Operational	Identify immediate mitigation procedures, including specific instructions, based on information security incident categorization level, on whether or not to shut down or disconnect affected IT systems. Establish procedures for information security incident investigation, preservation of evidence, and forensic analysis.	Do you have a documented security incident response plan?	✓			Geographic Solutions publishes and updates its security policy, GSI-SEC-390 Security Incident Response Plan, annually and reviews the policy in security training for all employees on an annual basis. Additional security notifications reinforce the contents of the policy and procedures document and help our staff maintain an increased awareness and understanding of the actions required in the event of a suspected security incident.
		IR-1.2		Operational		Do you integrate customized tenant requirements into your security incident response plans?	✓			Yes. Geographic Solutions understands that we will finalize each Service Level Agreement during contract negotiations.
		IR-1.3		Operational		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	✓			Geographic Solutions will provide DWD our Service Level Agreement (SLA), which contains proposed incident severity levels and responsibilities of the parties.
		IR-1.4		Operational		Have you tested your security incident response plans in the last year?	✓			The Geographic Solutions Disaster Recovery and Business Continuity Plan outlines procedures for restoring services in the event of a disaster, including system and data restoration. The plan also includes approved backup arrangements and formal agreements for the prioritization of systems and modules; arrangements for use of a backup facility; and periodic (at a minimum annually) testing of the backup procedures.
		IR-1.5		Operational	The organization tracks and documents information system security incidents.	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	✓			<div> </div> It provides us with a comprehensive and centralized view of the security posture of our IT infrastructure and activity within our applications. <div> </div> The result is a
		IR-1.6	IR-4	Operational		Will you share statistical information for security incident data with your tenants upon request?	✓			Geographic Solutions provides regular reports to senior management and designated client representatives until closing the incident. We then complete and distribute a final assessment and report.

Incident Response	IR-1	IR-1.7	IR-5 IR-6	Operational	Requires personnel to report suspected security incidents to the organizational incident response capability within 24 hours from when the agency discovered or should have discovered their occurrence; and Reports security incident information to designated authorities.	Do you have a defined and documented incident notification process for reporting suspected security incidents within 24 hours?	✓			Geographic Solutions' Security Incident Response Plan (GSI-SEC-390-IR) outlines the methodology used to ensure that in the event of an adverse event a response team is able to minimize negative effects and maintain normal, secure operations.
		IR-1.8		Operational		Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	✓			Geographic Solutions uses LogPoint's comprehensive Security Information and Event Management (SIEM) solution to provide intelligence-driven threat detection and remediation. It provides real-time threat intelligence ingestion and correlation of all facets of an attack, including methods and global campaigns. Our Security Operation Center uses this SIEM system to 'operationalize threat intelligence in order to get a full picture of attacks impacting our environments.
		IR-1.9		Operational		Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	✓			Geographic Solutions' Security Department will work with the FBI, local law enforcement, and other third-party security firms to ensure security breach issue(s) have been eradicated.
		IR-1.10		Operational		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	✓			Geographic Solutions segregates data by providing individual environments for each client, including for producing data for subpoenas. Multiple layers of physical and logical segregation exist to isolate and protect client data throughout different environments, including development, user acceptance testing, and production.
Media Protection Policy and Procedures: <i>Media Sanitization</i>	MPP-1	MPP1.1	MP-6	Operational	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	✓			DWD's defined requirements will dictate specific retention, archive, and purge policies and procedures in the proposed <i>VOS Sapphire</i> solution. Geographic Solutions maintains rigorous restrictions on access to all data storage components.
		MPP1.2		Operational		Does the provider destroy all information systems media that cannot be sanitized?	✓			Geographic Solutions disposes of data in a manner that complies with the NIST SP 800-88, Guidelines for Media Sanitization. Geographic Solutions properly destroys and/or disposes of all materials containing sensitive company and client consumer information in accordance with procedures established in its published security policy and procedure documents.
Physical and Environmental Protection: Physical Access Authorizations	PEP-1	PEP-1.1	PE-2(1) PE-2(3)	Operational	The organization authorizes physical access to the facility where the information system resides based on position or role.	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	✓			Given the critical nature of DWD's business processes conducted by the proposed system, we specifically designed the Transition Plan to mitigate risk and secure the financial investment and ongoing operation of the mission-critical software application. The plan formally identifies the procedures and activities needed to perform an efficient and effective transition, together with the appropriate acceptance and exit criteria.
Physical and Environmental Protection: <i>Physical Access Control</i>	PEP-2	PEP-2.1	PE-3	Operational	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	Do you restrict physical access to information assets and functions by users and support personnel?	✓			At our Geographic Solutions campus, access to systems development staff offices, telephone wiring closets, computer machine rooms, network-switching rooms, and other work areas containing customer data and information is physically restricted. All production network equipment and network wiring closets are physically secured in separate locked and controlled access environments inside the general access controlled environment. Building access can be attained only by presenting proximity cards with unique serial numbers at all outside door sensors. Once in the building, access to the data center can be attained only by using the uniquely serial numbered proximity card presented to the data center door sensor. Separate and unique security access lists are maintained for building and data center access. Only those proximity cards specifically authorized for access to the data center can be used to gain such access. Both the building and data center access events are logged automatically, recorded, and retained as the record of entry for both the building and the data center.
		PEP-2.2		Operational		Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	✓			Geographic Solutions manages all aspects of its computing environment. Access to all hosting facilities is restricted and monitored, as is access to staff offices, computer machine rooms, network-switching rooms, and other work areas.
		PEP-3.1		Operational	All information system components and services remain within the continental United States.	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?		✓		Geographic Solutions has two geographically diverse data centers in Lakeland FL and Sacramento CA. No traffic is allowed to leave the continental United States.

Physical and Environmental Protection: <i>Physical Location</i>	PEP-3	PEP-3.2	PE-18	Operational	All physical components associated with an information system or service classified as sensitive with respect to confidentiality or integrity must be housed within the same storage location dedicated for the exclusive use of the organization and are clearly marked.	Can you provide the physical geographical location of the storage in advance for a tenants data?	✓			Geographic Solutions' Lakeland, FL, data center will serve as the primary production hosting location for the proposed system. In accordance with the Tier III requirements defined in TIA-942, this data center has multiple power and cooling systems, allowing the concurrent maintenance of all online systems. It allows any planned data center infrastructure activity to occur without disrupting computer hardware operations. Geographic Solutions is proposing to maintain and support a full-service disaster recovery and business continuity facility for the proposed Case Management and Labor Exchange System at our Sacramento, CA, data center.
		PEP-3.3		Operational	Each hypervisor can only host one tier of the application architecture and no hypervisor may host the application interface and the data storage component for any information system, even if the components in question do not interact within the same information system.	Can you provide the physical geographical location of a tenants data upon request?	✓			With our private cloud deployment, Geographic Solutions' Tier III data center in Lakeland, Florida will be the production data center for the new Case Management and Labor Exchange system. For disaster recovery purposes, our data center in Sacramento, California will be the backup, mirrored facility.
		PEP-3.4		Operational		Can you ensure that data does not migrate beyond a defined geographical residency?	✓			In our private cloud, Geographic Solutions owns, manages, and maintains all equipment in our computing services environments inclusive of switches, servers, network components, firewalls, data storage, security appliances, and all special appliances. We have fine-tuned this equipment specifically for our products. While public cloud deployments do not allow Geographic Solutions to own the compute or storage equipment, we employ the same level of engineering, configuration, tuning, monitoring, and management of the overall system to ensure robust and reliable performance.
		PEP-3.5		Operational		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	✓			Complex software solutions, such as <i>VOS Sapphire 22</i> , benefit from efficient, tightly controlled, and well managed hosting services that ensure availability and high performance. To this end, Geographic Solutions closely monitors and manages key components of the compute, storage, and communications environment, whether hosting occurs within our own private cloud or, upon client request, a public cloud. Regardless of the hosting solution, all application development occurs and all data is stored totally within the continental United States. Geographic Solutions does not outsource any of the <i>VOS Sapphire 22</i> application development.
		PEP-3.6		Operational		Does the solution have the capability to set affinity on tiered systems, no one hypervisor can host the application and the data storage?	✓			Geographic Solutions host the web application on the VMware Farm and the data is hosted on a Physical SQL server. There is no way for the data and application to reside on the same hypervisor.
System and Information Integrity: <i>Vulnerability / Patch Management (Flaw Remediation)</i>	SII-1	SII-1.1	SI-2 RA-5 RA-5-COV	Operational	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices? Provide the frequency.	✓			<div>Scans are scheduled and results are collected/analyzed from a central server, with standalone scanners residing at different geographic locations to reduce bandwidth usage. After scanning for vulnerabilities, the tool will generate reports that can be shared with teams that describe the vulnerability or configuration issue and how to remediate it.</div>
		SII-1.2		Operational		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices? Provide the frequency	✓			<div>These tools scan for the most common vulnerabilities, such as cross-site scripting, SQL Injection, HTTP response splitting, parameter tampering, hidden field manipulation, backdoors/debug options, and buffer overflows. The software produces a report outlining any potential vulnerabilities. Geographic Solutions' Security Department corrects these vulnerabilities and risk factors as found.</div>
		SII-1.3		Operational		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices? Provide the frequency	✓			<div>Scans are scheduled monthly and results are collected/analyzed from a central server, with standalone scanners residing at different geographic locations to reduce bandwidth usage. After scanning for vulnerabilities, the tool will generate reports that can be shared with the teams. These reports describe the vulnerability or configuration issue and how to remediate it.</div> <div>The application provides the Geographic Solutions Security Team with real-time alerts and notifications about network irregularities and high-priority security events. Our Security and Systems teams use these alerts to immediately remediate any identified vulnerabilities.</div>
		SII-1.4		Operational		Will you make the results of vulnerability scans available to tenants at their request?	✓			Geographic Solutions will conduct vulnerability scans of DWD-specific infrastructure systems to include servers, virtual machines, and network devices. This security scanning activity is planned to be penetration testing and will be executed behind the public-facing web servers. We will provide the executive summary results of the security penetration testing to DWD for review and determination on whether remediation is required.
		SII-1.5		Operational		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?	✓			Geographic Solutions reviews system updates weekly and reviews urgent updates daily to identify new changes and vulnerabilities that have surfaced. We test critical operating system patches on internal development and test environments before loading them to production or passive production systems.

		SII-1.6		Operational		Will you provide your risk-based systems patching time frames to your tenants upon request?	✓			Geographic Solutions' technology change management process includes such items as regular updates, version upgrades, special patches, and necessary hardware and software changes, which improve system availability. Geographic Solutions schedules and plans regular updates and version upgrades with the client, to prepare the client for the release. Special patches are immediate releases of Geographic Solutions loads to the system, via coordination and communication with the customer, to address an immediate need. Clients can hold patches for scheduled client staging events or Geographic Solutions can load them as emergency hot fixes, as mutually determined by Geographic Solutions and the client. We schedule all upgrades of production systems and notify the appropriate parties, including System Administration, Database Administration, Client Services, and Production personnel. Geographic Solutions will open a ticket through the change management process and send a maintenance notice to all parties impacted by the scheduled maintenance event.
System and Information Integrity: <i>Malicious Code protection</i>	SII-2	SII-2.1	SI-3	Operational	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Does the provider ensure that they will utilize industry standard malware protection, incorporating both signature and non-signature-based detection mechanisms, on all systems with access to SOI data?	✓			McAfee's Web Gateway will be used to deliver comprehensive security for all aspects of web traffic in an appliance software architecture. For user-initiated web requests, this advanced malware detection technology developed by Intel Security combines customizable sandboxing with in-depth static code analysis. McAfee Web Gateway will be integrated with McAfee Advanced Threat Defense together with the in-line scanning capabilities of the Gateway Anti-Malware Engine in McAfee Web Gateway; this provides the strongest protection solution available for Internet-delivered threats.
		SII-2.1		Operational		Does the provider ensure that malware protection will be centrally managed and receive regular automatic updates to malicious code protection mechanisms and data files from the software vendor?	✓			<div></div> This product provides actionable dashboards with advanced queries and reports that we use to shorten the time from insight to response. McAfee provides a unified, collaborative platform with all the components for operationalizing threat intelligence, including global threat intelligence feeds, local intelligence creation, real-time sharing of threat information across the IT infrastructure, security information and event management, and delivery of automated, adaptive protection.
System and Communications Protection: <i>Boundary Protection</i>	SCP-1	SCP-01.1	SC-7	Technical	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., databases) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Does the provider ensure that the solution will utilize industry standard firewalls regulating all data entering the internal data network from any external source which will enforce secure connections between internal and external systems and will permit only authorized data to pass through?	✓			Firewalls are an essential component of the information systems security infrastructure. Firewalls are security systems that control and restrict network connectivity and network services, thus establishing a control point to enforce access controls. Geographic Solutions recommends using multiple clustered, highly available firewall configurations for security and controls on all internal and external traffic. <div></div>
		SCP-01.2		Technical		Does the provider ensure that external connections incorporated into the solution have appropriate security controls including industry standard intrusion detection and countermeasures that will detect and terminate any unauthorized activity prior to entering the firewall maintained by offeror?	✓			As part of the <i>VOS Sapphire 22</i> SaaS, Geographic Solutions provides full security and perimeter protection services, which include Security Patch Management, Virus/Spyware Scanning, Port Monitoring, Port Permission Configuration, Firewall Configuration Management, Application Filtering, Anti-Spam and Emailing, and Network and Host-based Intrusion Prevention System.
System and Communications Protection; <i>Encryption</i>	SCP-2	SCP-02.1	SC-1 SC-8 SC-23 SC-28	Technical		Do you encrypt tenant data at rest (on disk/storage) within your environment?	✓			Geographic Solutions handles and stores all data with the most secure methods available, including defense-in-depth architecture, SQL Server encryption, Transport Layer Security (TLS) certificate protection, frequent encrypted backups, and secure offsite storage. The security of all data files restricts unauthorized access. Geographic Solutions secures information stored in electronic or hard copy formats in facilities that prevent access by unauthorized persons before, during, and after processing.
		SCP-02.2		Technical		Do you use encryption for storing and transmitting email attachments?	✓			We use 2-way, asymmetric/public-key encryption to encrypt all stored and transmitted "sensitive data" in <i>VOS Sapphire 22</i> (including personal, financial, federally, and state protected, and password/ID data).
		SCP-02.3		Technical		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	✓			Geographic Solutions uses Secure Shell (SSH) File Transfer Protocol (also called Secure File Transfer Protocol or SFTP) for secure data file transfers.
		SCP-02.4		Technical		Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g., identity-based encryption)?			✓	No, at this time Geographic Solutions does not support tenant-generated encryption keys.
		SCP-02.5		Technical		Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?	✓			Yes, Geographic Solutions maintains its GSI-SEC-203-SI Encryption Policy and GSI-SEC-1103-SI Encryption Standard documents.
Systems and Communication Protection; <i>Cryptographic Key Establishment and Management</i>	SCP-3	SCP-3.1	SC-12 SC-13	Technical	The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with the organization-defined requirements for key generation, distribution, storage, access, and destruction. Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	✓			<i>VOS Sapphire 22</i> employs server-side storage of state information using NIST standard encryption and authentication algorithms. <i>VOS Sapphire 22</i> employs fully vetted cryptographic algorithms native to the .NET framework and library suite. Periodically, the Geographic Solutions Technology Review Board reviews the algorithms to ensure they are not obsolete.
		SCP-3.2		Technical		Do you support encryption keys being solely maintained by the cloud consumer or a trusted key management provider?	✓			Geographic Solutions has a Hardware Security Module (HSM) which securely stores the encryption keys in a vault. Geographic Solutions would look at a solution where the encryption keys were solely maintained by the cloud consumer or a trusted key management provider.

		SCP-3.3		Technical	shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	Do you store encryption keys in the cloud?		✓		At this time, Geographic Solutions has a Hardware Security Module (HSM) which securely stores the encryption keys in a FIPS 140-2/3 certified vault.
		SCP-3.4		Technical		Do you have separate key management and key usage duties?	✓			Yes, Geographic Solutions has a team dedicated to the management of the keys which are responsible for their storage in the FIPS 140-2/3 certified Hardware Security Module, and separate teams responsible for the encryption of data.
Data Security & Information Lifecycle Management <i>Nonproduction Data</i>	DS-01	DS-01.1	SA-11	Management	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	✓			When Geographic Solutions hosts <i>VOS Sapphire 22</i> for our clients, we create and maintain separate environments for development, quality assurance testing, training, and production throughout the project lifecycle. To ensure the stability of the production environment, Geographic Solutions maintains a separate, isolated testing and training environment. We establish dedicated websites and databases for training, testing, and user acceptance testing separate from the production systems. These provide proper operations and data segregation and prevent non-production users from corrupting production data or affecting the performance of the live system when training or testing is underway.
IOT Governance - Portability Requirements										
Interoperability & Portability <i>APIs</i>	IPY-01	IPY-01			The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	✓			The Indiana Case Management and Labor Exchange System API Library documentation are available from a browser. Each API is fully documented with its purpose and use. Each input and output data element is documented and valid values are listed as necessary. Sample input and output messages are also available online in this documentation. Code samples are available as well as sample posting/retrieving code. Geographic Solutions will document any DWD-specific web service needs after discussion with business and technical analysts and will develop a specification for each unique web service. The specification serves to support the data exchange between DWD and Indiana Case Management and Labor Exchange System data structures by mapping each data element.
Interoperability & Portability <i>Data Request</i>	IPY-02	IPY-02			All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	Is customer data (Structured & Unstructured) available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	✓			
Interoperability & Portability <i>Policy & Legal</i>	IPY-03	IPY-03.1			Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	✓			Geographic Solutions assigns a unique API key to each client. To increase system security, sending web service requests requires API key credentials. Additional security measures are available, such as Transport Layer Security (TLS) encryption, dedicated circuits, and Virtual Private Networks.
		IPY-03.2				Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	✓			Our integration specialists will map data from the existing database and create import programs to convert all relevant data in the system. The scripts and sequences needed to complete the mapping solution successfully drive the overall data flow solution. The Data Mapping documents and Data Migration Test Plan contain information on every core and reference table, including all data elements in the tables.
Interoperability & Portability <i>Standardized Network Protocols</i>	IPY-04	IPY-04.1			The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	✓			Geographic Solutions will use the established secure file transfer protocol (SFTP) process and execute scripts to move data to their mapped destination fields in the <i>VOS Sapphire 22</i> Solution.
		IPY-04.2				Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	✓			The Geographic Solutions team will use several methods to verify the completeness and accuracy of the data.
Interoperability & Portability <i>Virtualization</i>	IPY-05	IPY-05.1			The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	✓			Yes, the server virtualization standard for our production web servers is VMware.
		IPY-05.2				Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?			✓	Geographic Solutions does not make any custom changes or solution-specific virtualization hooks into the Hyper-V or VMware applications.
Security Framework - Organizational Security Framework	SF -01	SF-01.1			Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing integrity and related security policies.	What Security Framework do you follow (i.e. NIST, , ISO/IEC 27001, etc....)?	✓			Geographic Solutions aligns our Security and Risk Management programs with the Cybersecurity Framework (CSF) from the National Institute of Standards and Technology (NIST). Geographic Solutions will comply with all Indiana security rules, standards, policies, and reporting requirements for the protection and security of information technology and data. We will ensure that the new Case Management and Labor Exchange System will be compliant with the federal requirements specified by DWD. We comply with FedRAMP (moderate) controls as independently verified and validated by a FedRAMP-accredited Third Party Assessment Organization, for the services associated with the new <i>VOS Sapphire 22</i> application, and are in the process of having our compliance validated.