Att_N_-_IOT_Cloud_Provider_Questions_Form

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	X			Infastructure as a Service.
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.	X			Public when moving CoreMMIS to the Cloud.
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?	X			HIPAA OPM: Section 14, P.38 - Updates to the Security Manual - The Gainwell security officer is responsible for reviewing or coordinating the review of this document periodically and updating it, as needed, in response to environmental or operational changes affecting the security of electronic PHI.

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
		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?	X			HIPAA OPM: Section 5, P.19 - Access Authorization to Electronic Protected Health Information - Access to electronic PHI is approved for authorized workforce members. Before receiving access, approval must be obtained by the appropriate Gainwell leadership. Workforce members, including contractors, must successfully complete the HIPAA Privacy and HIPAA Privacy and Security Training before receiving access. In addition, workforce members requesting access to CoreMMIS must pass a background investigation before receiving access. The respective Gainwell leadership is responsible for making sure workforce members receive appropriate access to electronic PHI and receive appropriate and timely training on security and the use of such electronic PHI. Access rights are audited and modified accordingly. Access to electronic PHI is limited to the minimum access necessary required to perform job duties. The workforce members' leaders monitor access to electronic PHI.
		ACP-2.2		Technical		Does the provider have the capability to segment and identify administrative accounts by tenant?	X			Perform quarterly audits of privileged user access and server administator access.

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
		ACP-2.3		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?	X			HIPAA OPM: Section 5, P.19 - Access Authorization to Electronic Protected Health Information (see item 7). HIPAA OPM: Section 5, P.19 - Access Establishment and Modification - Procedures have been implemented to review and modify a user's right of access to a workstation, transaction, program, application, or process. Gainwell leadership is responsible for making sure workforce members have appropriate access to electronic PHI, and that such access is terminated when the employment of a workforce member ends, or job functions are modified to the extent that access requirements end or change. When a workforce member terminates employment for any reason, the Gainwell security administrator is notified by the respective leader and is responsible for seeing that access in appropriate systems is terminated.
		ACP-2.4		Technical		Does provider document how access to tenant data is granted and approved?	X			HIPAA OPM: Section 4, P.17 - Security Access Procedures - Access to locations where electronic PHI is housed is approved by the respective leader. Security access requests are processed by the Gainwell security administrator and badge administrator. The Site Administration Manual explains how the security administrator processes these requests. This document is for managers only.

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
Access Control - Account Management	ACP-2	ACP-2.5	AC-2	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?	X			HIPAA OPM: Section 5, P.19 - Access Establishment and Modification - Procedures have been implemented to review and modify a user's right of access to a workstation, transaction, program, application, or process. Gainwell leadership is responsible for making sure workforce members have appropriate access to electronic PHI, and that such access is terminated when the employment of a workforce member ends, or job functions are modified to the extent that access requirements end or change. When a workforce member terminates employment for any reason, the Gainwell security administrator is notified by the respective leader and is responsible for seeing that access in appropriate systems is terminated.
		ACP-2.6		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)	X			HIPAA OPM: Section 1, P.7 - Gainwell security officer - Steve Schofner Gainwell facility coordinator - Patty Warrenfelt Gainwell security administrator - Lennie Paul
		ACP-2.7		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)	X			HIPAA OPM: Section 13, P.36 - Technical Emergency Access - Access to electronic data housed at Gainwell is available to appropriate FSSA staff during contingency mode operations. These locations operate at secure facilities. The FSSA staff is admitted to these locations to perform specific functions.

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
						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)?	X			Decryption Protocol - Gainwell follows the State's standard for encryption protocol. Encryption and decryption mechanisms for files containing electronic PHI that are transmitted over the LAN require application-layer encryption – for example, secure file transfer protocol (SFTP) or Secure Shell (SSH). Files containing electronic PHI use a protocol with security built into the application. Files containing electronic PHI exchanged with outside entities may continue to use encryption mechanisms. A new entity required to exchange electronic PHI with Gainwell must meet specific minimum requirements. Access to electronic PHI across the internet must also meet minimum requirements for encryption. Email containing PHI must be encrypted and contain a disclaimer that the content is intended for a specific recipient. HIPAA OPM: Section 13, P.36 - Email Encryption Tool - Users who send PHI via email should have the corporate-approved encryption tool on their desktops. Subscribing to and using this tool is documented in the Title XIX E-mail Encryption Guide. Questions regarding how and when to use an encryption tool may be directed to the Gainwell

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
						Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	X			HIPAA OPM: Section 6, P.22 - HIPAA Privacy and Security Rule Training Requirements - Each Gainwell leader is required to notify the Gainwell security officer with the actual start date of a new workforce member. The Gainwell security officer is responsible for making sure workforce members participate in HIPAA Privacy and Security Rule Training and receive a passing score on the post-training evaluation. Training components address, in detail, the components contained in this manual. New workforce members are required to receive training within the first 2 days of employment and before receiving access to CoreMMIS. Annual corporate privacy and security training is also required.
						If users are found to have inappropriate entitlements, are all remediation and certification actions recorded/documented? If different actions are taken for Admin and User Accounts, please provide information on both.	X			HIPAA OPM: Section 5, P.20 - Monitoring CoreMMIS Access - On a quarterly basis, Gainwell leaders review the CoreMMIS profile summary for their business units in relation to PHI access via CoreMMIS.
		ACP-2.8		Technical	Disable Inactive Accounts	Does the provider or solution automatically disable inactive accounts after 90 consecutive days of non-use?	X			HIPAA OPM: Section 5, P.20 - Monitoring CoreMMIS Access - On a quarterly basis, Gainwell leaders review the CoreMMIS profile summary for their business units in relation to PHI access via CoreMMIS.

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
		ACP-2.9		Technical	Inactivity logout	Does the solution logout users automatically when the session inactivity time has exceeded 30 minutes?	X			HIPAA OPM: Section 13, P.35 - Automatic Logoff Session Parameters - Individual systems have timeout parameters as part of their function. Electronic sessions in systems housing electronic PHI are terminated after a specified period of inactivity, requiring the user to log on to systems again when access is needed. CoreMMIS timeout parameters are set to 15 minutes of inactivity.

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
Access Control - Access Enforcement	ACP-3	ACP-3.1	AC-3	Technical	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	X			Safeguards - Before making storage devices and removable media available for reuse, care must be taken that the device or media does not contain electronic PHI. If the device or media contains electronic PHI that is not required or needed, and the copy of that data is not a unique copy, a disk sanitizer is used to destroy or clean the data on the device or media before reusing it. HIPAA OPM: Section 12, P.34 -Data Backup and Storage - Individual desktops and laptops should not have PHI stored on the hard drives. Storing electronic PHI on a CD, DVD, USB storage device, or external hard drive is allowed, provided the data is encrypted and is locked up securely when not in use or unattended. It is recommended to store electronic PHI on a LAN or SharePoint site, because of the security of the servers and access to these servers. A device or media that contains the only copy of electronic PHI should have a retrievable copy made before moving or disposing of the original. Gainwell workforce members are permitted to format, reformat, and use approved
Access Control - Separation of	ACP-4	ACP-4.1	AC-4	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	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? Provide documentation on controls in place to prevent unauthorized access.	X			HIPAA OPM: Section 5, P.19 - Access Authorization to Electronic Protected Health Information (see item 7).

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
Duties	~~ACP-4~~	~~ACP-4.1~~	~~AC-4~~		conflict of interest.	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.	X			HIPAA OPM: Section 5, P.19 - Access Authorization to Electronic Protected Health Information (see item 7).
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.	X			HIPAA OPM: Section 5, P.19 - Access Authorization to Electronic Protected Health Information (see item 7).
		ACP-5.2		Technical		Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	X			HIPAA OPM: Section 5, P.19 - Access Authorization to Electronic Protected Health Information (see item 7).
		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?	X			HIPAA OPM: Section 7, P.24 - Response and Reporting of Security Incidents - Workforce members report known or suspected security incidents to the Gainwell security officer. The Gainwell security officer notifies the FSSA of incidents and maintains appropriate documentation.
Access Control - Unsuccessful Logon Attempts	ACP-6	ACP-6.1	AC-6	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.	X			HIPAA OPM: Section 5, P.19 - Response and Reporting of Security Incidents - Password Management
		ACP-6.2		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.	X			Provide CoreMMIS_PasswordPolicy_AccountLockout.doc
		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	X			Provide CoreMMIS_PasswordCriteria.doc

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
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?	X			
		ATP-1.2		Operational		Do you document employee acknowledgment of training they have completed?	X			LMS and Gainwell tracks training compliance.
		ATP-1.3		Operational		Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?		X		Contractors or non-employees do sign an NDA.
		ATP-1.4		Operational		Is successful and timely completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	X			
		ATP-1.5		Operational		Are personnel trained and provided with customer defined awareness programs at least once a year?	X			
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.)?	X			
		AUC-1.2		Technical		Are your audits performed at least annually? if no, please describe in the comments section.	X			
		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?	X			
		AUC-1.4		Technical		Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	X			

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
		AUC-1.5		Technical		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X			
		AUC-1.6		Technical		Are the results of the penetration tests available to tenants at their request?	X			
		AUC-1.7		Technical		Are the results of internal and external audits available to tenants at their request?	X			
Audit and Control: *Audit Events*	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 specific and ongoing audit needs.	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.	X			
		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 changes.	X			The solution does use web applications.
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 information available to your tenants?	X			Splunk is the tool selected when in the cloud.
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	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?	X			We have a cloud security posture management application that continuously monitors.

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
		CAA-1.2		Management	stored and transmitted across applications, databases, servers, and network infrastructure	Do you conduct risk assessments associated with data governance requirements at least once a year?	X			Security Risk Assessment is performed consistently and annually.
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?	X			
		CMP-1.2		Operational		Is documentation describing known issues with certain products/services available?	X			
		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?	X			
		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?	X			
	CMP-2	CMP-1.1	CM-2 CM-3 CM-7	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?	X			Scans performed on a scheduled basis.
		CMP-1.2		Operational		Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			McAfee is installed and monitors.
		CMP-1.3		Operational		Can you provide evidence that the proposed solution adheres to a security baseline, which is based on least functionality?	X			
		CMP-1.4		Operational		Are all changes to proposed solution authorized according to change management policies?	X			
		CP-1.1		Operational	A consistent unified framework for business continuity planning and plan development	Do you provide tenants with geographically resilient hosting options?	X			Colorado is the current CoreMMIS site used.

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
Contingency Planning - Information System backup	CP-1	CP-1.2	CP-2 CP4 CP-6 CP-7 CP-9 CP-10	Operational	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: • 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 infrastructure service failover capability to other providers?	X			
		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?	X			Disaster Exercise is performed annually.
		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?	X			
		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?	X			DR data is replicated to the Colorado site.
		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 attempting to obtain records, information or SOI data for reasons or activities that are not directly related to the business of the data owner?				Data is encrypted and unusable inflight and at rest; backups are stored offline and offsite.
Identification and Authentication; Organizational Users	IDA-1	IDA-1.1	IA-1	Technical	Vendor should have An identification and authentication policy that addresses purpose,	Does your management provision the authorization and restrictions for user access	X			
		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	Do you require at least annual updates and reviews of your access policies for all system users and administrators (exclusive of users maintained by your tenants)?	X			

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
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?	X			
		IDA-1.2		Technical		Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	X			
		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?	X			Identity management is in place and offers segregation of duties. Allows authorization of privileged access.
		IDA-1.4		Technical		Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?	X			
		IDA-1.5		Technical		Do you allow tenants to use third-party identity assurance services?	X			
		IDA-1.6		Technical		Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?	X			
		IDA-1.7		Technical		Do you support the ability to force password changes upon first logon?	X			
		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 unlock)?	X			
		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	Do you have a documented security incident response plan?	X			
		IR-1.2		Operational		Do you integrate customized tenant requirements into your security incident response plans?	X			

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
Incident Response	IR-1	IR-1.3	IR-4 IR-5 IR-6	Operational	procedures for information security incident investigation, preservation of evidence, and forensic analysis.	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	X			
		IR-1.4		Operational		Have you tested your security incident response plans in the last year?	X			
		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?	X			We perform root cause analysis on incidents and share with the client/tenants.
		IR-1.6		Operational		Will you share statistical information for security incident data with your tenants upon request?	X			
		IR-1.7		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?	X			
		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?	X			Splunk and ArcSight.
		IR-1.9		Operational		Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	X			
		IR-1.10		Operational		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X			
Media Protection Policy and Procedures: *Media Sanitization*	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	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	X			
		MPP1.2		Operational		Does the provider distroy all information systems media that cannot be sanitized?	X			

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
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?	X			
Physical and Environmental Protection: *Physical Access Control*	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?	X			
		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?	X			
Physical and Environmental Protection: *Physical Location*	PEP-3	PEP-3.1	PE-18	Operational	All information system components and services remain within the continental United States. 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. 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 you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	X			Restricted to United States zones.
		PEP-3.2		Operational		Can you provide the physical geographical location of the storage in advance for a tenants data?	X			Restricted to United States zones.
		PEP-3.3		Operational		Can you provide the physical geographical location of a tenants data upon request?	X			AWS will not disclose the exact location. Restricted to the United States.
		PEP-3.4		Operational		Can you ensure that data does not migrate beyond a defined geographical residency?	X			Restricted to United States zones.
		PEP-3.5		Operational		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X			
		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?	X			AWS managed.
		SII-1.1		Operational	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices? Provide the frequency.	X			Penetration testing is performed annually and planning to perform quarterly.

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
System and Information Integrity: *Vulnerability / Patch Management (Flaw Remediation)*	SII-1	SII-1.2	SI-2 RA-5 RA-5-COV	Operational	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)	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices? Provide the frequency	X			Coverity - Daily.
		SII-1.3		Operational		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices? Provide the frequency	X			Nessus - Monthly at a minimum.
		SII-1.4		Operational		Will you make the results of vulnerability scans available to tenants at their request?	X			
		SII-1.5		Operational		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?	X			
		SII-1.6		Operational		Will you provide your risk-based systems patching time frames to your tenants upon request?	X			We do triage based on priority.
System and Information Integrity: *Malicious Code protection*	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?	X			McAfee.
		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?	X			McAfee is the provider of this service managed by Hayden Grey Company.
System and Communications Protection:	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,	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?	X			

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
Protection: *Boundary Protection*	SCP-1	SCP-01.2	SC-7	Technical	and regulatory compliance obligations.	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?	X			
System and Communications Protection; *Encryption*	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?	X			Oracle database level.
		SCP-02.2		Technical		Do you use encryption for storing and transmitting email attachments?	X			
		SCP-02.3		Technical		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	X			
		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)?	X			Certificates are managed by Gainwell and Entrust.
		SCP-02.5		Technical		Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?	X			
Systems and Communication Protection; *Cryptographic Key Establishment and Management*	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 shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	X			
		SCP-3.2		Technical		Do you support encryption keys being solely maintained by the cloud consumer or a trusted key management provider?	X			Entrust manages the keys for Gainwell.
		SCP-3.3		Technical		Do you store encryption keys in the cloud?		X		Entrust manages the keys for Gainwell.
		SCP-3.4		Technical		Do you have separate key management and key usage duties?	X			

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
Data Security & Information Lifecycle Management *Nonproduction Data*	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?	X			Environments are set up seperately to prevent commingling of environments data.
IOT Governance - Portability Requirements										
Interoperability & Portability *APIs*	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?	X			
Interoperability & Portability *Data Request*	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)?	X			
Interoperability & Portability *Policy & Legal*	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?	X			
		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?	X			
Interoperability & Portability *Standardized Network Protocols*	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)	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	X			File Exchange is the tool used, and documents are published on how to connect/use.

Att_N_-_IOT_Cloud_Provider_Questions_Form

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
		IPY-04.2			detailing the relevant interoperability and portability standards that are involved.	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	X			
Interoperability & Portability *Virtualization*	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?	X			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?			X	No custom changes.
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…,)?	X			NIST version 4 moderate.