CJIS Responsibility Matrix

The Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy sets the minimum security requirements to provide an acceptable level of assurance to protect the full lifecycle of Criminal Justice Information. Agencies using cloud-based services are required to make informed decisions on whether or not the cloud provider can offer services that maintain compliance with the requirements of the CJIS Security Policy.

This document outlines the specific security policies and practices for Genasys Evertel Cloud Services and how they are compliant with the CJIS Security Policy, version 5.9.5. Genasys has leveraged CJIS's Requirements Companion Document to provide details on control responsibilities when agencies use Genasys Evertel Cloud Services. The Requirements Companion Document is provided as an additional resource within the CJIS Security Policy Resource Center (https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center) and describes which party has responsibility to perform the actions necessary to ensure a particular CJIS Security Policy requirement is being met.

Genasys has also provided responses to questions posed in the CJIS Security Policy Appendix G.3 Cloud Computing at the end of this document.

Responsibility is color-coded within the columns based on the agreed ability to perform the actions necessary to meet requirements. They are as follows:

Dark Gray	CJIS/CSO
Dark Green	Agency
Dark Blue	Service Provider
Orange	Both
Light Blue	TBD

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
1.3	Relationship to Local Security Policy and Other Policies	The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy **shall** always be the minimum standard and local policy may augment, or increase the standards,…	Agency	Agency must address this requirement through appropriate policies and procedures.	N/A
	"	...and local policy may augment, or increase the standards, but **shall not** detract from the CJIS Security Policy standards.	Agency		
	"	The agency **shall** develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy.	Agency		
	"	The policies and procedures **shall** be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.	Agency		
CJIS Policy Area: Roles & Responsibilities					
3.2.1	CJIS Systems Agencies (CSA)	The head of each CSA **shall** appoint a CJIS Systems Officer (CSO).	CJIS/CSO	Agency must address this requirement through appropriate policies and procedures.	N/A
	"	Such decisions **shall** be documented and kept current.	CJIS/CSO		
	CJIS Systems Officer (CSO)	Pursuant to The Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO **shall not** be outsourced.	CJIS/CSO		
	"	The CSO **shall** set, maintain, and enforce the following:			
3.2.2(1)	"	1. Standards for the selection, supervision, and separation of personnel who have access to CJI.	CJIS/CSO	Agency must address this requirement through appropriate policies and procedures.	N/A
3.2.2(2)	"	2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.	CJIS/CSO		
	"	a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.	CJIS/CSO		
	"	b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.	CJIS/CSO		
	"	c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.	CJIS/CSO		
	"	d. Ensure the designation of a Terminal Agency Coordinator (TAC) within each agency with device access to CJIS systems.	Agency		
	"	e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).	Agency		
	"	f. Ensure the LASO receives enhanced security awareness training (ref. Section 5.2).	CJIS/CSO		
	"	g. Approve access to FBI CJIS systems.	CJIS/CSO		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	h. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.	CJIS/CSO		
	"	i. Perform other related duties outlined by the user agreements with the FBI CJIS Division.	CJIS/CSO		
3.2.3(3)	"	3. Outsourcing of Criminal Justice Functions		Agency must address this requirement through appropriate policies and procedures.	N/A
	"	a. Responsibility for the management of the approved security requirements **shall** remain with the CJA.	Agency		
	"	b. Responsibility for the management control of network security **shall** remain with the CJA.	Agency		
3.2.6	Contracting Government Agency (CGA)	A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor **shall** appoint an Agency Coordinator.	Agency	Agency must address this requirement through appropriate policies and procedures.	N/A
3.2.7	Agency Coordinator (AC)	The AC **shall** be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.	Agency	Agency must address this requirement through appropriate policies and procedures.	N/A
	"	The AC **shall**:			
	"	1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.	Agency		
	"	2. Participate in related meetings and provide input and comments for system improvement.	Agency		
	"	3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.	Agency		
	"	4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.	Agency		
	"	5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).	Agency		
	"	6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.	Agency		
	"	7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.	Agency		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.	Agency		
	"	9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CJA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.	Agency		
	"	10. Any other responsibility for the AC promulgated by the FBI.	Agency		
3.2.8	CJIS System Agency Information Security Officer (CSA ISO)	The CSA ISO **shall**:		The CSA ISO must address this requirement through appropriate policies and procedures.	N/A
	"	1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.	CJIS/CSO		
	"	2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.	CJIS/CSO		
	"	3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.	CJIS/CSO		
	"	4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.	CJIS/CSO		
3.2.9	Local Agency Security Officer (LASO)	Each LASO **shall**:		Agency must address this requirement through appropriate policies and procedures.	N/A
	"	1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.	Agency		
	"	2. Identify and document how the equipment is connected to the state system.	Agency		
	"	3. Ensure that personnel security screening procedures are being followed as stated in this policy.	Agency		
	"	4. Ensure the approved and appropriate security measures are in place and working as expected.	Agency		
	"	5. Support policy compliance and ensure CSA ISO is promptly informed of security incidents.	Agency		
3.2.10	FBI CJIS Division Information Security Officer (FBI CJIS ISO)	The FBI CJIS ISO **shall**:		Agency must address this requirement through appropriate policies and procedures.	N/A
	"	1. Maintain the CJIS Security Policy.	CJIS/CSO		
	"	2. Disseminate the FBI Director approved CJIS Security Policy.	CJIS/CSO		
	"	3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.	CJIS/CSO		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.	CJIS/CSO		
	"	5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.	CJIS/CSO		
	"	6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.	CJIS/CSO		
	"	7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.	CJIS/CSO		
3.2.12	Compact Officer	Pursuant to the National Crime Prevention and Privacy Compact, each party state **shall** appoint a Compact Officer…	CJIS/CSO	The CSO must address this requirement through appropriate policies and procedures.	N/A
		...Compact Officer who **shall** ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.	CJIS/CSO		
CJIS Policy Area: CJI/PII					
4.2.1	Proper Access, Use, and Dissemination of CHRI	The III **shall** be accessed only for an authorized purpose.	Agency	Agency must address this requirement through appropriate policies and procedures.	N/A
	"	Further, CHRI **shall** only be used for an authorized purpose consistent with the purpose for which III was accessed.	Agency		
4.2.2	Proper Access, Use, and Dissemination of NCIC Restricted Files Information	Proper access to, use, and dissemination of data from restricted files **shall** be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual.	Agency	Agency must address this requirement through appropriate policies and procedures.	N/A
	"	The restricted files, which **shall** be protected as CHRI, are as follows:			
	"	1. Gang File	Agency		
	"	2. Threat Screening Center File	Agency		
	"	3. Supervised Release File	Agency		
	"	4. National Sex Offender Registry File	Agency		
4.2.2	"	5. Historical Protection Order File of the NCIC	Agency	Agency must address this requirement through appropriate policies and procedures.	N/A
	"	6. Identity Theft File	Agency		
	"	7. Protective Interest File	Agency		
	"	8. Person with Information [PWI] data in the Missing Person Files	Agency		
	"	9. Violent Person File	Agency		
	"	10. NICS Denied Transaction File	Agency		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
4.2.3.2	For Other Authorized Purposes	Non-restricted files information **shall** not be disseminated commercially.	Agency	Agency must address this requirement through appropriate policies and procedures.	N/A
	"	Agencies **shall not** disseminate restricted files information for purposes other than law enforcement.	Agency		
4.2.4	Storage	When CHRI is stored, agencies **shall** establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information.	Agency	Agency must address this requirement through appropriate policies and procedures.	N/A
	"	These records **shall** be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files.	Agency		
4.2.5.1	Justification	In addition to the use of purpose codes and logging information, all users **shall** provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.	Agency	Agency must address this requirement through appropriate policies and procedures.	N/A
4.3	Personally Identifiable Information (PII)	PII **shall** be extracted from CJI for the purpose of official business only.	Agency	Agency must address this requirement through appropriate policies and procedures.	N/A
	"	Agencies **shall** develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI.	Agency		
CJIS Policy Area: Information Exchange Agreements					
5.1	Information Exchange Agreements	The information shared through communication mediums **shall** be protected with appropriate security safeguards.	Agency	Agency is responsible for establishing information exchange agreements with parties with whom they share data through Genasys Cloud Services.	The Genasys Terms of Service outlines the data protection roles, responsibilities, and data ownership when using the Genasys Cloud Services.
5.1.1	Information Exchange	Before exchanging CJI, agencies **shall** put formal agreements in place that specify security controls.	Agency		
	"	Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS **shall** specify the security controls and conditions described in this document.	Agency		
	"	Information exchange agreements **shall** be supported by documentation committing both parties to the terms of information exchange.	Agency		
	"	Law Enforcement and civil agencies **shall** have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI.	Agency		
5.1.1.1	Information Handling	Procedures for handling and storage of information **shall** be established to protect that information from unauthorized disclosure, alteration or misuse.	Agency	Agency must establish policies related to the access and usage of data stored within Genasys Cloud Services.	Genasys maintains policies and practices within Genasys Cloud Services for securely handling information.
	"	Using the requirements in this policy as a starting point, the procedures **shall** apply to the handling, processing, storing, and communication of CJI.	Agency		
5.1.1.2	State and Federal Agency User Agreements	Each CSA head or SIB Chief **shall** execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this policy before accessing and participating in CJIS records information programs.	Agency	CSA heads or SIB Chiefs are responsible for maintaining this written agreement.	Genasys Cloud Services does not connect to or have any access to the FBI CJIS systems.
	"	This agreement **shall** include the standards and sanctions governing utilization of CJIS systems.	Agency		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	As coordinated through the particular CSA or SIB Chief, each Interface Agency **shall** also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F.	Agency		
	"	All user agreements with the FBI CJIS Division **shall** be coordinated with the CSA head.	Agency		
5.1.1.3	Criminal Justice Agency User Agreements	Any CJA receiving access to FBI CJI **shall** enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access.	Agency	CSA heads or SIB Chiefs are responsible for maintaining this written agreement.	Genasys Cloud Services does not connect to or have any access to the FBI CJIS systems.
	"	The written agreement **shall** specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere.	Agency		
	"	These agreements **shall** include:			
	"	1. Audit.	Agency		
	"	2. Dissemination.	Agency		
	"	3. Hit confirmation.	Agency		
	"	4. Logging.	Agency		
	"	5. Quality Assurance (QA).	Agency		
	"	6. Screening (Pre-Employment).	Agency		
	"	7. Security.	Agency		
	"	8. Timeliness.	Agency		
	"	9. Training.	Agency		
	"	10. Use of the system.	Agency		
	"	11. Validation.	Agency		
5.1.1.4	Inter-Agency and Management Control Agreements	A NCJA (government) designated to perform criminal justice functions for a CJA **shall** be eligible for access to the CJI.	Agency	Agency must address this requirement through appropriate policies and procedures.	Genasys Cloud Services does not connect to or have any access to the FBI CJIS systems.
	"	Access **shall** be permitted when such designation is authorized pursuant to Executive Order, statute, regulation, or inter-agency agreement.	Agency		
	"	The NCJA **shall** sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA.	Agency		
5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum	Private contractors who perform criminal justice functions **shall** meet the same training and certification criteria required by governmental agencies performing a similar function, and…	Both	Agency is responsible for maintaining a signed copy of the CJIS Security Addendum delivered by Genasys.	Genasys acknowledges and abides by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is included by reference in the Genasys MSPA which contractually commits Genasys to the CJIS Security Policy requirements. CJIS Security Addendum Certification pages are maintained for each authorized Genasys
	"	...and **shall** be subject to the same extent of audit review as are local user agencies.	Both		
	"	All private contractors who perform criminal justice functions **shall** acknowledge, via signing of the Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	Modifications to the CJIS Security Addendum **shall** be enacted only by the FBI.	CJIS/CSO		employee and are available to customers.
	"	1. Private contractors designated to perform criminal justice functions for a CJA **shall** be eligible for access to CJI.	Agency		
	"	Access **shall** be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice.	Agency		
	"	The agreement between the CJA and the private contractor **shall** incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).	Agency		
	"	2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) **shall** be eligible for access to CJI.	Agency		
	"	Access **shall** be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice.	Agency		
	"	The agreement between the NCJA and the private contractor **shall** incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).	Agency		
5.1.1.6	Agency User Agreements	A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, **shall** be eligible for access to CJI.	Agency	Agency must address this requirement through appropriate policies and procedures.	Genasys Cloud Services does not connect to or have any access to the FBI CJIS systems.
	"	Access **shall** be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.	Agency		
	"	A NCJA (public) receiving access to FBI CJI **shall** enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access.	Agency		
	"	A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, **shall** be eligible for access to CJI.	Agency		
	"	Access **shall** be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.	Agency		
	"	A NCJA (private) receiving access to FBI CJI **shall** enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access.	Agency		
	"	All NCJAs accessing CJI **shall** be subject to all pertinent areas of the CJIS Security Policy (see appendix J for supplemental guidance).	Agency		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	Each NCJA that directly accesses FBI CJI **shall** also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F.	Agency		
5.1.1.7	Outsourcing Standards for Channelers	Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions **shall** be eligible for access to CJI.	Agency	Agency must address this requirement through appropriate policies and procedures.	Genasys Cloud Services does not connect to or have any access to the FBI CJIS systems.
	"	Access **shall** be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.	Agency		
	"	All Channelers accessing CJI **shall** be subject to the terms and conditions described in the Compact Council Security and Management Control Outsourcing Standard.	Agency		
	"	Each Channeler that directly accesses CJI **shall** also allow the FBI to conduct periodic penetration testing.	Agency		
	"	Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient **shall** meet the same training and certification criteria required by governmental agencies performing a similar function…	Agency		
	"	...and **shall** be subject to the same extent of audit review as are local user agencies.	Agency		
5.1.1.8	Outsourcing Standards for Non-Channelers	Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions **shall** be eligible for access to CJI.	Agency	Agency must address this requirement through appropriate policies and procedures.	Genasys Cloud Services does not connect to or have any access to the FBI CJIS systems.
	"	Access **shall** be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.	Agency		
	"	All contractors accessing CJI **shall** be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers.	Agency		
	"	Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient **shall** meet the same training and certification criteria required by governmental agencies performing a similar function, and…	Agency		
	"	...and **shall** be subject to the same extent of audit review as are local user agencies.	Agency		
5.1.2	Monitoring, Review, and Delivery of Services	As specified in the inter-agency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider **shall** be regularly monitored and reviewed.	Agency	Agency must address this requirement through appropriate policies and procedures.	Genasys Cloud Services does not connect to or have any access to the FBI CJIS systems.
	"	The CJA, authorized agency, or FBI **shall** maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response.	Agency		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	The incident reporting/response process used by the service provider **shall** conform to the incident reporting/response specifications provided in this policy.	Agency		
5.1.2.1	Managing Changes to Service Providers	Any changes to services provided by a service provider **shall** be managed by the CJA, authorized agency, or FBI.	Agency	Agency must address this requirement through appropriate policies and procedures.	Genasys Cloud Services does not connect to or have any access to the FBI CJIS systems.
	"	Evaluation of the risks to the agency **shall** be undertaken based on the criticality of the data, system, and the impact of the change.	Agency		
5.1.3	Secondary Dissemination	If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency **shall** log such dissemination.	Agency	Agency must address this requirement through appropriate policies and procedures.	Genasys Cloud Services does not connect to or have any access to the FBI CJIS systems.
5.1.4	Secondary Dissemination of Non-CHRI CJI	Dissemination **shall** conform to the local policy validating the requestor of the CJI as an employee or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.	Agency	Agency must address this requirement through appropriate policies and procedures.	Genasys Cloud Services does not connect to or have any access to the FBI CJIS systems.
CJIS Policy Area: Awareness and Training					
5.2: AT-1	Policy and Procedures	a. Develop, document, and disseminate to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI:	Both	Agency is responsible for ensuring personnel who access Genasys Cloud Services undergo appropriate security awareness training.	Genasys maintains a comprehensive security awareness policy and program which includes annual role-based training. Authorized Genasys personnel with access to CJI are required to complete Level 4 CJIS Security Training upon assignment and biennially thereafter. Training programs are updated annually, and individual training records maintained for three (3) years.
	"	1. Organization-level awareness and training policy that:	Both		
	"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Both		
	"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Both		
	"	2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;	Both		
	"	b. Designate organizational personnel with information security awareness and training responsibilities to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and	Both		
	"	c. Review and update the current awareness and training:	Both		
	"	1. Policy annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made; and	Both		
	"	2. Procedures annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made.	Both		
5.2: AT-2	Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):	Both	Agency is responsible for providing annual training prior to any personnel	See 5.2: AT-1

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	1. As part of initial training for new users prior to accessing CJI and annually thereafter; and	Both	accessing CJI along with annual updates to any training programs.	
	"	2. When required by system changes or within 30 days of any security event for individuals involved in the event;	Both		
	"	b. Employ one or more of the following techniques to increase the security and privacy awareness of system users:	Both		
	"	1. Displaying posters			
	"	2. Offering supplies inscribed with security and privacy reminders			
	"	3. Displaying logon screen messages			
	"	4. Generating email advisories or notices from organizational officials			
	"	5. Conducting awareness events			
	"	c. Update literacy training and awareness content annually and following changes in the information system operating environment, when security incidents occur, or when changes are made in the CJIS Security Policy; and	Both		
	"	d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.	Both		
5.2: AT-2 (2)	Literacy Training And Awareness | Insider Threat	Provide literacy training on recognizing and reporting potential indicators of insider threat.	Both	See 5.2: AT-1	See 5.2: AT-1
5.2: AT-2 (3)	Literacy Training And Awareness | Social Engineering And Mining	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.	Both	See 5.2: AT-1	See 5.2: AT-1
5.2: AT-3	Role-Based Training	a. Provide role-based security and privacy training to personnel with the following roles and responsibilities:	Both	See 5.2: AT-1	See 5.2: AT-1
	"	· All individuals with unescorted access to a physically secure location;	Both		
	"	· General User: A user, but not a process, who is authorized to use an information system;	Both		
	"	· Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform:	Both		
	"	1. Before authorizing access to the system, information, or performing assigned duties, and annually thereafter; and	Both		
	"	2. When required by system changes;	Both		
	"	b. Update role-based training content annually and following audits of the CSA and local agencies; changes in the information system operating environment; security incidents; or when changes are made to the CJIS Security Policy;	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training;	Both		
	"	d. Incorporate the minimum following topics into the appropriate role-based training content:	Both		
	"	1. All individuals with unescorted access to a physically secure location:			
	"	a. Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information Penalties	Both		
	"	b. Reporting Security Events	Both		
	"	c. Training	Both		
	"	d. System Use Notification	Both		
	"	e. Physical Access Authorizations	Both		
	"	f. Physical Access Control	Both		
	"	g. Monitoring Physical Access	Both		
	"	h. Visitor Control	Both		
	"	i. Personnel Sanctions	Both		
	"	2. General User: A user, but not a process, who is authorized to use an information system. In addition to AT-3 (d) (1) above, include the following topics:			
	"	a. Criminal Justice Information	Both		
	"	b. Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information	Both		
	"	c. Personally Identifiable Information	Both		
	"	d. Information Handling	Both		
	"	e. Media Storage	Both		
	"	f. Media Access	Both		
	"	g. Audit Monitoring, Analysis, and Reporting	Both		
	"	h. Access Enforcement	Both		
	"	i. Least Privilege	Both		
	"	j. System Access Control	Both		
	"	k. Access Control Criteria	Both		
	"	l. System Use Notification	Both		
	"	m. Session Lock	Both		
	"	n. Personally Owned Information Systems	Both		
	"	o. Password	Both		
	"	p. Access Control for Display Medium	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	q. Encryption	Both		
	"	r. Malicious Code Protection	Both		
	"	s. Spam and Spyware Protection	Both		
	"	t. Cellular Devices	Both		
	"	u. Mobile Device Management	Both		
	"	v. Wireless Device Risk Mitigations	Both		
	"	w. Wireless Device Malicious Code Protection	Both		
	"	x. Literacy Training and Awareness/Social Engineering and Mining	Both		
	"	y. Identification and Authentication (Organizational Users)	Both		
	"	z. Media Protection	Both		
	"	3. Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform. In addition to AT-3 (d) (1) and (2) above, include the following topics:			
	"	a. Access Control	Both		
	"	b. System and Communications Protection and Information Integrity	Both		
	"	c. Patch Management	Both		
	"	d. Data backup and storage—centralized or decentralized approach	Both		
	"	e. Most recent changes to the CJIS Security Policy	Both		
	"	4. Organizational Personnel with Security Responsibilities: Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL. In addition to AT-3 (d) (1), (2), and (3) above, include the following topics:			
	"	a. Local Agency Security Officer Role	Both		
		b. Authorized Recipient Security Officer Role	Both		
	"	c. Additional state/local/tribal/federal agency LASO roles and responsibilities	Both		
	"	d. Summary of audit findings from previous state audits of local agencies	Both		
	"	e. Findings from the last FBI CJIS Division audit	Both		
5.2: AT-3 (5)	Role-Based Training | Processing Personally Identifiable Information	Provide all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI with initial and annual training in the employment and operation of personally identifiable information processing and transparency controls.	Both	See 5.2: AT-1	See 5.2: AT-1

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
5.2: AT-4	Training Records	a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and	Both	See 5.2: AT-1	See 5.2: AT-1
	"	b. Retain individual training records for a minimum of three years.	Both		
CJIS Policy Area: Incident Response					
IR-1	Policy And Procedures	a. Develop, document, and disseminate to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI:	Both	Agency must establish incident response policies related to a security breach within Genasys Cloud Services.	Genasys maintains incident response policies and procedures related to any security breach within the Genasys Cloud Services.
	″	1. Agency-level incident response policy that:	Both		
	"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Both		
	"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Both		
	"	2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;	Both		
	"	b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the incident response policy and procedures; and	Both		
	"	c. Review and update the current incident response:	Both		
	"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Both		
	"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Both		
IR-2	Incident Response Training	a. Provide incident response training to system users consistent with assigned roles and responsibilities:	Both	Agency must establish a response training procedure relating to any data breach of the Genasys Cloud Services.	The Genasys security awareness training for Cloud Services includes security incident response roles and responsibilities, including reporting expectations.
	"	1. Prior to assuming an incident response role or responsibility or acquiring system access;	Both		
	"	2. When required by system changes; and	Both		
	"	3. Annually thereafter; and	Both		
	"	b. Review and update incident response training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Both		
IR-2 (3)	(3) Incident Response Training | Breach	Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.	Both		
IR-3	Incident Response Testing	Control: Test the effectiveness of the incident response capability for the system annually using the following tests: tabletop or walk-through exercises; simulations; or other agency appropriate tests.	Both	Agency must test their Incident Response plans and procedures annually.	Genasys tests its Incident Response plans and procedures annually.

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
IR-3 (2)	(2) Incident Response Testing | Coordination with Related Plans	Coordinate incident response testing with organizational elements responsible for related plans.	Both		
IR-4	Incident Handling	a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;	Both	Agency is responsible for maintaining incident response procedures and plans.	Genasys maintains security incident response procedures and capabilities for Genasys Cloud Services which includes automated procedures
	"	b. Coordinate incident handling activities with contingency planning activities;	Both		
	"	c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and	Both		
	"	d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.	Both		
IR-4 (1)	(1) Incident Handling | Automated Incident Handling Processes	Support the incident handling process using automated mechanisms (e.g., online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.	Both		
IR-5	Incident Monitoring	Control: Track and document incidents.	Both	Agency is responsible for establishing incident response capabilities and tracking and documenting incidents.	Genasys maintains security incident response procedures and capabilities for Genasys Cloud Services. Genasys internally tracks and documents all security incidents to ensure proper remediation.
IR-6	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability immediately but not to exceed one (1) hour after discovery; and	Both	Agency must report to Genasys if they believe an unauthorized third party may be using their account or their content, or if their account information is lost or stolen.	Genasys must report to Agency if we believe an unauthorized third party may be using their account or their content.
	"	b. Report incident information to organizational personnel with incident handling responsibilities, and if confirmed, notify the CSO, SIB Chief, or Interface Agency Official.	Both		
IR-6 (1)	(1) Incident Reporting | Automated Reporting	Report incidents using automated mechanisms.	Both		
IR-6 (3)	(3) Incident Reporting | Supply Chain Coordination	Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.	Both		
IR-7	Incident Response Assistance	Control: Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.	Both	Agency is responsible for establishing their own internal incident support resources.	Genasys establishes and maintains several incident support resources.
IR-7 (1)	(1) Incident Response Assistance | Automation Support for Availability Of Information And Support	Increase the availability of incident response information and support using automated mechanisms described in the discussion.	Both		
	Incident Response Plan	a. Develop an incident response plan that:	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	1. Provides the organization with a roadmap for implementing its incident response capability;	Both	Agency is responsible for establishing and maintaining an Incident Response Plan.	Genasys maintains a detailed Incidence Response Plan approved by executive leadership annually. The Genasys IRP can be provided upon request.
	"	2. Describes the structure and organization of the incident response capability;	Both		
	"	3. Provides a high-level approach for how the incident response capability fits into the overall organization;	Both		
	"	4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;	Both		
	"	5. Defines reportable incidents;	Both		
	"	6. Provides metrics for measuring the incident response capability within the organization;	Both		
IR-8	"	7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;	Both		
	"	8. Addresses the sharing of incident information;	Both		
	"	9. Is reviewed and approved by the organization's/agency's executive leadership annually; and	Both		
	"	10. Explicitly designates responsibility for incident response to organizational personnel with incident reporting responsibilities and CSO or CJIS WAN Official.	Both		
	"	b. Distribute copies of the incident response plan to organizational personnel with incident handling responsibilities;	Both		
	"	c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;	Both		
	"	d. Communicate incident response plan changes to organizational personnel with incident handling responsibilities; and	Both		
	"	e. Protect the incident response plan from unauthorized disclosure and modification.	Both		
IR-8 (1)	(1) Incident Response Plan | Breaches	Include the following in the Incident Response Plan for breaches involving personally identifiable information:	Both		
	"	(a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;	Both		
	"	(b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and	Both		
	"	(c) Identification of applicable privacy requirements.	Both		
CJIS Policy Area: Auditing and Accountability					
AU-1	Policies and Procedures	a. Develop, document, and disseminate to organizational personnel with audit and accountability responsibilities:	TBD	Agency must document and execute their implementation of audit monitoring,	Within the Genasys Cloud Services application, logs are generated and

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	1. Agency and system-level audit and accountability policy that:	TBD	analysis, and reporting. Within the Genasys Cloud Services, detailed usage and access reports are available for agencies to monitor their accounts.	secured that detail all access to evidence data, and robust evidence audit reports are available to customers.
	"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	TBD		
	"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	TBD		
	"	2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;	TBD		
	"	b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and	TBD		
	"	c. Review and update the current audit and accountability:	TBD		
	"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	TBD		
	"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	TBD		
AU-2	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: authentication, file use, user/group management, events sufficient to establish what occurred, the sources of events, outcomes of events, and operational transactions (e.g., NCIC, III);	Service Provider	N/A	In alignment with the Genasys Information Security program, Genasys Cloud Services systems are configured to log all required events and more to a central logging system. Additionally, within the Genasys Cloud Services application, logs are generated and secured that detail all access to evidence data, and robust evidence audit reports are available to customers.
	"	b. Coordinate the event logging function with other organizational entities requiring audit- related information to guide and inform the selection criteria for events to be logged;	Service Provider		
	"	c. Specify the following event types for logging within the system:	Service Provider		
	"	All successful and unsuccessful:	Service Provider		
	"	1. System log-on attempts	Service Provider		
	"	2. Attempts to use:		Within the Genasys Cloud Services, detailed usage and access reports are	In alignment with the Genasys Information Security program, Genasys Cloud Services systems are configured to log all required events and more to a central
	"	a. Access permission on a user account, file, directory, or other system resource;	Service Provider		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	b. Create permission on a user account, file, directory, or other system resource;	Service Provider	available for agencies to monitor their accounts.	logging system. Additionally, within the Genasys Cloud Services application, logs are generated and secured that detail all access to evidence data, and robust evidence audit reports are available to customers.
	"	c. Write permission on a user account, file, directory, or other system resource;	Service Provider		
	"	d. Delete permission on a user account, file, directory, or other system resource;	Service Provider		
	"	e. Change permission on a user account, file, directory, or other system resource.	Service Provider		
	"	3. Attempts to change account passwords	Service Provider	N/A	In alignment with the Genasys Information Security program, Genasys Cloud Services systems are configured to log all required data and activities.
	"	4. Actions by privileged accounts (i.e., root, Oracle, DBA, admin, etc.)	Service Provider		
	"	5. Attempts for users to:	Service Provider		
	"	a. Access the audit log file;	Service Provider		
	"	c. Destroy the audit log file;	Service Provider		
	"	d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and	Service Provider		
	"	e. Review and update the event types selected for logging annually.	Service Provider		
AU-3	Content of Audit Records	Ensure that audit records contain information that establishes the following:	Service Provider	N/A	In alignment with the Genasys Information Security program, Genasys Cloud Services systems are configured to log all required data and activities.
	"	a. What type of event occurred;	Service Provider		
	"	b. When the event occurred;	Service Provider		
	"	c. Where the event occurred;	Service Provider		
	"	d. Source of the event;	Service Provider		
	"	e. Outcome of the event; and	Service Provider		
	"	f. Identity of any individuals, subjects, or objects/entities associated with the event.	Service Provider		
AU-3(1)	(1) Content of Audit Records | Additional Audit Information	Generate audit records containing the following additional information:	Service Provider	N/A	In alignment with the Genasys Information Security program, Genasys Cloud Services systems are configured to log all required data and activities and can provide all data for audit records.
	"	a. Session, connection, transaction, and activity duration;	Service Provider		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	b. Source and destination addresses;	Service Provider		
	"	c. Object or filename involved; and	Service Provider		
	"	d. Number of bytes received and bytes sent (for client-server transactions) in the audit records for audit events identified by type, location, or subject.	Service Provider		
	"	e. The III portion of the log shall clearly identify:	Service Provider		
	"	1. The operator	Agency	Agency must log all required data and activities to provide audit records.	N/A
	"	2. The authorized receiving agency	Agency		
	"	3. The requestor	Agency		
	"	4. The secondary recipient	Agency		
AU-3 (3)	(1) Content of Audit Records | Limit Personally Identifiable Information Elements	Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3).	TBD	N/A	N/A
AU-4	Audit Log Storage Capacity	Allocate audit log storage capacity to accommodate the collection of audit logs to meet retention requirements (AU-11).	TBD	N/A	N/A
AU-5	Response to Audit Logging Process Failures	a. Alert organizational personnel with audit and accountability responsibilities and system/network administrators within one (1) hour in the event of an audit logging process failure; and	Both	Within the Genasys Cloud Services application, detailed usage and access reports are available for agencies to monitor their accounts.	Controls are established to alert Genasys of any log collection or processing failures.
	"	b. Take the following additional actions: restart all audit logging processes and verify system(s) are logging properly.	Both		
AU-6	Audit Record Review, Analysis, and Reporting	a. Review and analyze system audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity;	Both	Agencies must document and execute their implementation of audit monitoring, analysis, and reporting. Within the	Genasys employs advanced detection and analysis capabilities of system events for Genasys Cloud Services.

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	b. Report findings to organizational personnel with audit review, analysis, and reporting responsibilities and organizational personnel with information security and privacy responsibilities; and	Both	Genasys Cloud Services application, detailed usage and access reports are available for agencies to monitor their accounts.	This includes automated detection and alerts for unusual activity or attacks.
	"	c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	Both		
AU-6 (1)	(1) Audit Record Review, Analysis, and Reporting | Automated Process Integration	Integrate audit record review, analysis, and reporting processes using automated mechanisms.	TBD	N/A	N/A
AU-6 (3)	(3) Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.	TBD	N/A	N/A
AU-7	Audit Record Reduction and Report Generation	a. Supports on-demand audit record review, analysis, and reporting requirements and after- the-fact investigations of incidents; and	TBD	N/A	N/A
	"	b. Does not alter the original content or time ordering of audit records.	TBD	N/A	N/A
AU-7 (1)	Audit Record Reduction and Report Generation | Automatic Processing	Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: information included in AU-3.	TBD	N/A	N/A
AU-8	Time Stamps	a. Use internal system clocks to generate time stamps for audit records;	Service Provider	N/A	The Genasys Cloud Services central logging system collects event generation time and event
	"	b. Record time stamps for audit records that meet hundredths of a second (i.e., hh:mm:ss:00) interval and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.	Service Provider		
AU-9	Protection of Audit Information	a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and	Service Provider	N/A	In alignment with the Genasys Information Security program, Genasys Cloud Services systems are configured to log all required events and more to a central logging system. The central logging system protects logs from unauthorized access, modification, and deletion. Additionally, the Genasys Cloud Services platform creates and maintains tamper-proof evidence audit records including the when, who, and what for each evidence file. These records cannot be edited or changed, even by account administrators.
	"	b. Alert organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators upon detection of unauthorized access, modification, or deletion of audit information.	Service Provider		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
AU-9 (4)	Protection of Audit Information | Access by Subset of Privileged Users	Authorize access to management of audit logging functionality to only organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators.	TBD	N/A	N/A
AU-11	Audit Record Retention	Retain audit records for a minimum of one (1) year or until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.	Service Provider	N/A	Genasys Cloud Services system central log data is maintained for at least one (1) year. Evidence and user access logs within Genasys Cloud Services are retained for at least one (1) year, even after evidence deletion.
AU-12	Audit Record Generation	a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on all systems generating required audit logs;	TBD	N/A	N/A
	"	b. Allow organizational personnel with audit record generation responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators to select the event types that are to be logged by specific components of the system; and	TBD	N/A	N/A
	"	c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.	TBD	N/A	N/A
CJIS Policy Area: Access Control					
AC-1	Policy and Procedures	a. Develop, document, and disseminate to: organizational personnel with access control responsibilities	Both	Agency is responsible for implementing this control for their user access into Genasys Cloud Services. Genasys Cloud Services allow for customers to directly administer user accounts.	Genasys maintains account management policies and practices for Genasys Cloud Services systems including at least quarterly account validation. Agency is responsible for implementing this control for their user access into Genasys Cloud Services. Genasys Cloud Services allow for customers to directly administer user accounts.
	"	1. Agency-level access control policy that:	Both		
	"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Both		
	"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Both		
	"	2. Procedures to facilitate the implementation of the access control policy and the associated access controls;	Both		
	"	b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the access control policy and procedures; and	Both		
	"	c. Review and update the current access control:	Both		
	"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Both		
	"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Both		
	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;	Both	Agency is responsible to documenting any internal procedures for assigning	Genasys makes available to Agency a document of the types and access levels

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
				account types within Genasys Cloud Services.	of each role within the Genasys Cloud Services.
	″	b. Assign account managers;	Both	Agency is responsible for assigning users to roles within Genasys Cloud Services.	Executive roles can be assigned on a per user basis within Genasys Cloud Services.
	″	c. Require conditions for group and role membership;	Both	N/A	Roles can be assigned on a per user basis within Genasys Cloud Services.
	″	d. Specify:	Both	N/A	Genasys lists each user and role within the Agency's account within Genasys Cloud Services.
	″	1. Authorized users of the system;	Both		
	″	2. Group and role membership; and	Both		
AC-2	″	3. Access authorizations (i.e., privileges) and attributes listed for each account;	Both	N/A	Provided
	″	Attribute Name	Both	N/A	Provided
	″	Email Address Text	Both	N/A	Provided
	″	Employer Name	Both	N/A	Provided
	″	Federation Id	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	Given Name	Both	N/A	Provided
	″	Identity Provider Id	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	Sur Name	Both	N/A	Provided
	″	Telephone Number	Both	N/A	Provided
	″	Identity Provider Id	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	Unique Subject Id	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	Counter Terrorism Data Self Search Home Privilege Indicator	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	Criminal History Data Self Search Home Privilege Indicator	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	Criminal Intelligence Data Self Search Home Privilege Indicator	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	Criminal Investigative Data Self Search Home Privilege Indicator	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	Display Name	Both	N/A	Provided
	″	Government Data Self Search Home Privilege Indicator	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	Local Id	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	NCIC Certification Indicator	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	NDEx Privilege Indicator	Both	Agency responsibility	Not used within Genasys Cloud Services
		PCII Certification Indicator	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	28 CFR Certification Indicator	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	Employer ORI	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	Employer Organization General Category Code	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	Employer State Code	Both	N/A	Provided
	″	Public Safety Officer Indicator	Both	N/A	Provided as Badge/Employee Number
	″	Sworn Law Enforcement Officer Indicator	Both	N/A	Provided as Badge/Employee Number
	″	Authenticator Assurance Level	Both	N/A	Provided

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	″	Federation Assurance Level	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	Identity Assurance Level	Both	Agency responsibility	Not used within Genasys Cloud Services
	″	Intelligence Analyst Indicator	Both	--	--
	″	e. Require approvals by organizational personnel with account management responsibilities for requests to create accounts;	Both	Agency is responsible for managing user access and any protocol and procedures for access controls for Genasys Cloud Services users.	Genasys does not approve or manage user access within the Agency portal in Genasys Cloud Services.
	″	f. Create, enable, modify, disable, and remove accounts in accordance with agency policy;	Both		
AC-2	″	g. Monitor the use of accounts;	Both		
	″	h. Notify account managers and system/network administrators within:	Both		
	″	1. One day when accounts are no longer required;	Both		
	″	2. One day when users are terminated or transferred; and	Both		
	″	3. One day when system usage or need-to-know changes for an individual;	Both		
	″	i. Authorize access to the system based on:	Both		
	″	1. A valid access authorization;	Both		
	″	2. Intended system usage; and	Both		
	″	3. Attributes as listed in AC-2(d)(3);	Both		
	″	j. Review accounts for compliance with account management requirements at least annually;	Both		
	″	k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and	Both		
	″	l. Align account management processes with personnel termination and transfer processes.	Both		
AC-2(1)	(1) Account Management | Automated System Account Management	Support the management of system accounts using automated mechanisms including email, phone, and text notifications.	Both	N/A	Genasys Cloud Services uses email and text notifications for account management support.
AC-2(2)	(2) Account Management | Automated Temporary And Emergency Account Management	Automatically remove temporary and emergency accounts within 72 hours.	Both	Agency is responsible for managing user accounts within Genasys Cloud Services including account removal.	Genasys is not responsible for managing user accounts within the Agency's Genasys Cloud Services account.
AC-2(3)	(3) Account Management | Disable Accounts	Disable accounts within one (1) week when the accounts:	Both	It is the agency's responsibility to manage their users access within Genasys Cloud Services.	Agency users with the Executive or Management roles can disable or remove users accounts at any time within Genasys Cloud Services.
	"	(a) Have expired;	Both		
	"	(b) Are no longer associated with a user or individual;	Both		
	"	(c) Are in violation of organizational policy; or	Both		
	"	(d) Have been inactive for 90 calendar days.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
AC-2(4)	(4) Account Management | Automated Audit Actions	Automatically audit account creation, modification, enabling, disabling, and removal actions.	Both	Agency can view all user account management activities within Genasys Cloud Services.	Genasys tracks and logs all user account management activities within Genasys Cloud Services.
AC-2(5)	(5) Account Management | Inactivity Logout	Require that users log out when a work period has been completed.	Both	Agency should have policies for logging out of Genasys Cloud Services when work is completed.	Genasys Cloud Services automatically log users out after 30 minutes of inactivity.
AC-2(13)	(13) Account Management | Disable Accounts For High-Risk Individuals	Disable accounts of individuals within 30 minutes of discovery of direct threats to the confidentiality, integrity, or availability of CJI.	Both	Agency is responsible for notifying Genasys of any accounts discovered to compromise data integrity within Genasys Cloud Services.	Genasys will disable any accounts within 30 minutes of discovery of the account compromising the integrity of data within Genasys Cloud Services.
AC-3	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Both	Agency is responsible for implementing this control for their user access into Genasys Cloud Services. Within Genasys Cloud Services roles and permissions are customizable by customers. Default roles are included for customers upon customer tenant creation. These are locked roles and cannot be modified. All other roles are customizable by customers.	Genasys has documented and implemented logical access controls to enforce session control, authorization, multi- factor and remote access requirements. Individuals are assigned unique User IDs when accessing Genasys systems.
AC-3(14)	(14) Access Enforcement | Individual Access	Provide automated or manual processes to enable individuals to have access to elements of their personally identifiable information.	Both		
AC-4	Information Flow Enforcement	Enforce approved authorizations for controlling the flow of information within the system and between connected systems by preventing CJI from being transmitted unencrypted across the public network, blocking outside traffic that claims to be from within the agency, and not passing any web requests to the public network that are not from agency controlled or internal boundary protection devices (e.g., proxies, gateways, firewalls, or routers).	Both	Agency is responsible for any data flow outside of the Genasys Cloud Services.	Genasys requires encryption on all connections to Genasys Cloud Services over public networks. In addition, Genasys maintains a range of capabilities for controlling data flows in Cloud Services, including firewalls, ACLs, proxies, and load balancers.
AC-5	Separation Of Duties	a. Identify and document separation of duties based on specific duties, operations, or information systems, as necessary, to mitigate risk to CJI; and	Both	Agency is responsible for setting the access and authorization levels for each of their users within Genasys Cloud Services.	Agency can control each user's access and authorization level within Genasys Cloud Services to support separation of duties.
	"	b. Define system access authorizations to support separation of duties.	Both		
AC-6	Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	Both	Agency is responsible for implementing this control for their user access into Genasys Cloud Services. Genasys Cloud Services allow for customers to directly administer user accounts.	Genasys account management practices and implementation are designed according to the principle of least privilege.
AC-6(1)	(1) Least Privilege | Authorize Access To Security Functions	Authorize access for personnel including, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information security personnel, maintainers, system programmers, etc.) to:	Both		
	"	(a) Established system accounts, configured access authorizations (i.e., permissions, privileges), set events to be audited, set intrusion detection parameters, and other security functions; and	Both		
	"	(b) Security-relevant information in hardware, software, and firmware.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
AC-6(2)	(2) Least Privilege | Nonprivileged Access For Nonsecurity Functions	Require that users of system accounts (or roles) with access to privileged security functions or security-relevant information (e.g., audit logs), use nonprivileged accounts or roles, when accessing nonsecurity functions.	Both		
AC-6(5)	(5) Least Privilege | Privileged Accounts	Restrict privileged accounts on the system to privileged users.	Both		
AC-6(7)	(7) Least Privilege | Review of User Privileges	a. Reviews annually the privileges assigned to non-privileged and privileged users to validate the need for such privileges; and	Both		
	"	b. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.	Both		
AC-6(9)	(9) Least Privilege | Log Use Of Privileged Functions	Log the execution of privileged functions.	Both		
AC-6(10)	(10) Least Privilege | Prohibit Non-Privileged Users From Executing Privileged Functions	Prevent non-privileged users from executing privileged functions.	Both		
AC-7	Unsuccessful Logon Attempts	a. Enforce a limit of five (5) consecutive invalid logon attempts by a user during a 15-minute time period; and	Both	Agency is required to enforce technical and administrative controls to restrict access to Genasys Cloud Services. Genasys Cloud Services restrict consecutive invalid login attempts as well as account lockout periods in accordance with CJIS Policy requirements. Genasys Cloud Services allow for agency administrators to customize these controls for their tenants.	Genasys Cloud Services access control mechanisms are maintained in compliance with the specific CJIS security requirements and enforce user lockouts or deny attempts from malicious-appearing IPs.
	"	b. Automatically lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.	Both		
AC-8	System Use Notification	a. Display a system use notification message to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:	Both	Agency is required to enforce technical and administrative controls to restrict access to Genasys Cloud Services. Genasys Cloud Services allow agencies the ability to configure and customize the system use notification language.	Genasys Cloud Services systems implements an approved system use notification in compliance with the specific CJIS security requirement.
	"	1. Users are accessing a restricted information system;	Both		
	"	2. System usage may be monitored, recorded, and subject to audit;	Both		
	"	3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and	Both		
	"	4. Use of the system indicates consent to monitoring and recording;	Both		
	"	b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and	Both		
	"	c. For publicly accessible systems:	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	″	1. Display system use information consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines, before granting further access to the publicly accessible system;	Both		
	″	2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and	Both		
	″	3. Include a description of the authorized uses of the system.	Both		
AC-11	Device Lock	a. Prevent further access to the system by initiating a device lock after a maximum of 30 minutes of inactivity and requiring the user to initiate a device lock before leaving the system unattended.	Both	Agency is required to enforce technical and administrative controls to restrict access to Genasys Cloud Services. Genasys Cloud Services allow agencies the ability to configure and customize the inactivity period lockout in accordance with CJIS Policy requirements.	Genasys Cloud Services system access control mechanisms are maintained in compliance with the specific CJIS security requirements. Sessions are terminated after 30 minutes of inactivity and the user is required to reestablish authentication to regain access.
	"	NOTE: In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement.	Both		
	"	b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.	Both		
AC-11(1)	(1) Device Lock | Pattern-Hiding Displays	Conceal, via the device lock, information previously visible on the display with a publicly viewable image.	Both		Upon session termination, the application view is taken to the login screen.
AC-12	Session Termination	Automatically terminate a user session after a user has been logged out.	Both	Agency is responsible for terminating user's sessions on the devices a user is accessing Genasys Cloud Services on.	User sessions at the application level are terminated upon logout.
AC-14	Permitted Actions Without Identification or Authentication	a. Identify any specific user actions that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and	Both	Agency is responsible for identifying and enforcing what access a user has without authentication at the device level.	Users cannot perform any actions without authentication on Genasys Cloud Services application level.
	"	b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.	Both		
AC-17	Remote Access	a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and	Both	Agency is responsible for authorizing and monitoring the methods in which remote access is granted to their tenant within Genasys Cloud Services. Genasys Cloud Services supports several authentication options including multi-factor authentication, Single Sign- On (SSO), and API tokens.	Genasys maintains policies and practices for Genasys Cloud Services that limit remote access to only required individuals and require at least two factors for authentication. All remote access methods are performed through a FIPS-142 certified VPN router and are monitored and logged.
	"	b. Authorize each type of remote access to the system prior to allowing such connections.	Both		
AC-17(1)	(1) Remote Access | Monitoring and Control	Employ automated mechanisms to monitor and control remote access methods.	Both		
AC-17(2)	(2) Remote Access | Protection Of Confidentiality And Integrity Using Encryption	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Both		
AC-17(3)	(3) Remote Access | Managed Access Control Points	Route remote accesses through authorized and managed network access control points.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
AC-17(4)	(4) Remote Access | Privileged Commands and Access	(a) Authorize the execution of privileged commands and access to security relevant information via remote access only in a format that provides assessable evidence and for the following needs: compelling operational needs; and	Both		
	"	(b) Document the rationale for remote access in the security plan for the system.	Both		
AC-18	Wireless Access	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and	Both	Agency is responsible for managing any wireless networks and access points used to access Genasys Cloud Services.	N/A
	"	b. Authorize each type of wireless access to the system prior to allowing such connections.	Both		
AC-18(1)	(1) Wireless Access | Authentication And Encryption	Protect wireless access to the system using authentication of authorized users and agency-controlled devices, and encryption.	Both		
AC-18(3)	(3) Wireless Access | Disable Wireless Networking	Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.	Both		
AC-19	Access Control For Mobile Devices	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and	Both	Agency must address this requirement through appropriate policies and procedures. Genasys Cloud Services provides many security features and capabilities to enable customers to securely manage digital evidence including device-level permission management (for example, allow specific users to use the web-based interface, but not the mobile application) and restrict access to defined IP ranges (limit access to approved office locations).	N/A
	"	b. Authorize the connection of mobile devices to organizational systems.	Both		
AC-19(5)	(5) Access Control For Mobile Devices | Full Device Or Container-Based Encryption	Employ full-device encryption to protect the confidentiality and integrity of information on full- and limited-feature operating system mobile devices authorized to process, store, or transmit CJI.	Both		
AC-20	Use Of External Systems	a. Establish agency-level policies governing the use of external systems consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:	Both	Genasys Cloud Services provides many security features and capabilities to enable customers to securely manage digital evidence and prohibit the usage of personally owned information systems including: • Application permission management (for example, allow specific users to use the web-based interface, but not the mobile application) • Restrict access to defined IP ranges (limit access to approved office locations) Agencies are required to enforce technical and administrative controls to restrict access to Genasys Cloud Services.	Genasys does not allow the use of external systems to access, process, store or transmit any organization-controlled data.
	"	1. Access the system from external systems; and	Both		
	"	2. Process, store, or transmit organization-controlled information using external systems; or	Both		
	″	b. Prohibit the use of personally-owned information systems including mobile devices (i.e., bring your own device [BYOD]) and publicly accessible systems for accessing, processing, storing, or transmitting CJI.	Both		
AC-20(1)	(1) Use Of External Systems | Limits On Authorized Use	Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:	Both		
	"	(a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	(b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.	Both		
AC-20(2)	(2) Use Of External Systems | Portable Storage Devices — Restricted Use	Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.	Both		
AC-21	Information Sharing	a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions as defined in an executed information exchange agreement; and	Both	Agency is responsible for managing information sharing partners, their access and any information exchange agreements necessary.	Genasys allows 'Guest' roles as invited and assigned by the Agency. Guest access is limited to the data access granted by the Agency.
	"	b. Employ attribute-based access control (see AC-2(d)(3)) or manual processes as defined in information exchange agreements to assist users in making information sharing and collaboration decisions.	Both		
AC-22	Publicly Accessible Content	a. Designate individuals authorized to make information publicly accessible;	Both	Agency is responsible for implementing policies and procedures for making information publicly accessible.	Genasys does not allow any information stored in Genasys Cloud Services to be made publicly accessible.
	"	b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;	Both		
	"	c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and	Both		
	"	d. Review the content on the publicly accessible system for nonpublic information quarterly and remove such information, if discovered.	Both		
CJIS Policy Area: Identification and Authentication					
5.6: IA-0	Use of Originating Agency Identifiers in Transactions and Information Exchanges	An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction.	Agency	Agency is responsible for properly identifying and vetting system users prior to granting them access to Genasys Cloud Services through appropriate policies and procedures.	Genasys maintains policies and practices for Genasys Cloud Services for identifying and authenticating users before allowing access.
	"	The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.	Agency		
	"	Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.	Agency		
	"	Agencies assigned a limited access ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.	Agency		
5.6: IA-1	Policy and Procedures	a. Develop, document, and disseminate to authorized personnel:	Agency	Agency is responsible for properly documenting and disseminating	N/A
	"	1. Agency/Entity identification and authentication policy that:	Agency		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Agency	identification and authentication policies prior to granting user's access to Genasys Cloud Services.	
	"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Agency		
	"	2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;	Agency		
	"	b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and	Agency		
	"	c. Review and update the current identification and authentication:	Agency		
	"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Agency		
	"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Agency		
5.6: IA-2	Identification and Authentication (Organizational Users)	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.	Agency	Agency is responsible for identifying and authenticating organizational users.	N/A
5.6: IA-2 (1)	Identification and Authentication (Organizational Users) | Multi-Factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Both	Agency is required to enforce technical and administrative controls to ensure personnel owned information systems are not used to access Genasys Cloud Services and that any information systems used to access Genasys Cloud Services are in compliance with the specific CJIS security requirements for authentication.	Genasys Cloud Services system access control mechanisms are maintained in compliance with the specific CJIS security requirements. Access control to the system is limited to authorized users and uses multiple factors for authentication. Evidence data is encrypted at rest and in transit. Genasys maintains key management practices for managing the encryption keys.
5.6: IA-2 (2)	Identification and Authentication (Organizational Users) | Multi-Factor Authentication to Non-Privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Both		
5.6: IA-2 (8)	Identification and Authentication (Organizational Users) |Access to Accounts - Replay Resistant	Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.	Both		
5.6: IA-2 (12)	Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials	Accept and electronically verify Personal Identity Verification-compliant credentials.	Both		
5.6: IA-3	Device Identification and Authentication	Uniquely identify and authenticate agency devices before establishing all remote and network connections. In the instance of local connection, the device must be approved by the agency and the device must be identified and authenticated prior to connection to an agency asset.	Both	Agency is responsible for identifying and authenticating agency devices prior to granting access to Genasys Cloud Services.	Genasys does not manage the agency devices nor authenticate devices prior to connection to the Genasys Cloud Services. Genasys enforces multi-factor

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
					authentication when a new device has been detected.
5.6: IA-4	Identifier Management	Manage system identifiers by:	Both	Agency is responsible for assigning each user a unique email address prior to granting access to Genasys Cloud Services.	Genasys Cloud Services identifies users by their email address. Email address must be unique across the entire Genasys systems.
	"	a. Receiving authorization from organizational personnel with identifier management responsibilities to assign an individual, group, role, service, or device identifier;	Both		
	"	b. Selecting an identifier that identifies an individual, group, role, service, or device;	Both		
	"	c. Assigning the identifier to the intended individual, group, role, service, or device; and	Both		
	"	d. Preventing reuse of identifiers for one (1) year.	Both		
5.6: IA-4 (4)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as agency or nonagency.	Both	Agency must address this requirement through appropriate policies, procedures, and configurations in how they use Genasys Cloud Services.	Genasys maintains policies and practices for Genasys Cloud Services for Identifier and Authenticator management through Genasys's Information Security Program. Additionally, all users are required to have unique login credentials.
5.6: IA-5	Authenticator Management	Manage system authenticators by:	Both	---	---
	"	a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;	Both	Agency is responsible for assigning proper roles to users within Genasys Cloud Services and managing any authentication requirements for the devices in which users access Genasys Cloud Services from.	Genasys Cloud Services adheres to all authentication requirements listed here.
	"	b. Establishing initial authenticator content for any authenticators issued by the organization;	Both		
	"	c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;	Both		
	"	d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;	Both		
	"	e. Changing default authenticators prior to first use;	Both		
	"	f. Changing or refreshing authenticators annually or when there is evidence of authenticator compromise;	Both		
	"	g. Protecting authenticator content from unauthorized disclosure and modification;	Both		
	"	h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and	Both		
	"	i. Changing authenticators for group or role accounts when membership to those accounts changes.	Both		
	"	j. All credential service providers (CSPs) authenticating claimants at Authenticator Assurance Level 2 (AAL2) SHALL be assessed on the following criteria:			

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	(1) Authentication SHALL occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators.	Both	N/A	Genasys Cloud Services uses multi-factor authenticators and meets the requirements of FIPS 140-1
	"	(2) If the multi-factor authentication process uses a combination of two singlefactor authenticators, then it SHALL include a Memorized Secret authenticator and a possession-based authenticator. (NIST 800-63B, Section 4.2.1)	Both		
	"	(3) Cryptographic authenticators used at AAL2 SHALL use approved cryptography.	Both		
	"	(4) At least one authenticator used at AAL2 SHALL be replay resistant.	Both		
	"	(5) Communication between the claimant and verifier SHALL be via an authenticated protected channel.	Both		
	"	(6) Verifiers operated by government agencies at AAL2 SHALL be validated to meet the requirements of FIPS 140 Level 1.	Both		
	"	(7) Authenticators procured by government agencies SHALL be validated to meet the requirements of FIPS 140 Level 1.	Both		
	"	(8) If a device such as a smartphone is used in the authentication process, then the unlocking of that device (typically done using a PIN or biometric) SHALL NOT be considered one of the authentication factors.	Both	Agency is responsible for managing any device authenticators.	Genasys Cloud Services requires application-level authentication separate from any device authenticators.
	"	(9) If a biometric factor is used in authentication at AAL2, then the performance requirements stated in IA-5 m Biometric Requirements SHALL be met.	Both	Agency is responsible for managing any biometric authentication factors for device access.	Genasys Cloud Services does not use biometric factors for authentication.
	"	(10) Reauthentication of the subscriber SHALL be repeated at least once per 12 hours during an extended usage session.	Both	Agency is responsible for managing any device authenticators.	Genasys Cloud Services will auto-logout users that exceed 30 minutes of application inactivity.
	"	(11) Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer.	Both		
5.6: IA-5	"	(12) The CSP SHALL employ appropriately tailored security controls from the moderate baseline of security controls defined in the CJIS Security Policy.	Both	Agency is responsible for ensuring minimum controls as defines in the CJIS Security Policy for any device-level authenticators.	Genasys Cloud Services adheres to all security control requirements defined in the CJIS Security Policy.
	"	The CSP SHALL ensure that the minimum assurance-related controls for moderateimpact systems are satisfied.	Both		
	"	(13) The CSP SHALL comply with records retention policies in accordance with applicable laws and regulations.	Both		
	"	(14) If the CSP opts to retain records in the absence of any mandatory requirements, then the CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine how long records should be retained and SHALL inform subscribers of that retention policy.	Both		
	"	k. Privacy requirements that apply to all CSPs, verifiers, and RPs.			
	"	(1) The CSP SHALL employ appropriately tailored privacy controls from the CJIS Security Policy.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	(2) If the CSP processes attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively “identity service”), related fraud mitigation, or to comply with law or legal process, then the CSP SHALL implement measures to maintain predictability and manageability commensurate with the associated privacy risk.	Both		
	"	I. General requirements applicable to AAL2 authentication process.		Agency is responsible for ensuring minimum controls as defines in the CJIS Security Policy for any device-level authenticators.	Genasys Cloud Services does not use any physical authentication factors.
	"	(1) CSPs SHALL provide subscriber instructions on how to appropriately protect a physical authenticator against theft or loss.	Both		
	"	(2) The CSP SHALL provide a mechanism to revoke or suspend the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected.	Both		
	"	(3) If required by the authenticator type descriptions in IA-5(1), then the verifier SHALL implement controls to protect against online guessing attacks.	Both		
	"	(4) If required by the authenticator type descriptions in IA-5(1) and the description of a given authenticator does not specify otherwise, then the verifier SHALL limit consecutive failed authentication attempts on a single account to no more than 100.	Both		
	"	(5) If signed attestations are used, then they SHALL be signed using a digital signature that provides at least the minimum security strength specified in the latest revision of 112 bits as of the date of this publication.	Both		
	"	(6) If the verifier and CSP are separate entities (as shown by the dotted line in Figure 8 Digital Identity Model), then communications between the verifier and CSP SHALL occur through a mutually-authenticated secure channel (such as a client authenticated TLS connection).	Both		
5.6: IA-5	"	(7) If the CSP provides the subscriber with a means to report loss, theft, or damage to an authenticator using a backup or alternate authenticator, then that authenticator SHALL be either a memorized secret or a physical authenticator.	Both	Agency is responsible for ensuring minimum controls as defines in the CJIS Security Policy for any device-level authenticators.	Genasys Cloud Services does not use any physical authentication factors.
	"	(8) If the CSP chooses to verify an address of record (i.e., email, telephone, postal) and suspend authenticator(s) reported to have been compromised, then...The suspension SHALL be reversible if the subscriber successfully authenticates to the CSP using a valid (i.e., not suspended) authenticator and requests reactivation of an authenticator suspended in this manner.	Both		
	"	(9) If and when an authenticator expires, it SHALL NOT be usable for authentication.	Both		
	"	(10) The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	(11) CSPs SHALL revoke the binding of authenticators immediately upon notification when an online identity ceases to exist (e.g., subscriber's death, discovery of a fraudulent subscriber), when requested by the subscriber, or when the CSP determines that the subscriber no longer meets its eligibility requirements.	Both		
	"	(12) The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing certified attributes signed by the CSP within five (5) days after revocation or termination takes place.	Both		
	"	m. Biometric Requirements		Agency is responsible for ensuring minimum controls as defines in the CJIS Security Policy for any device-level authenticators.	Genasys Cloud Services does not use any physical authentication factors.
	"	(1) Biometrics SHALL be used only as part of multi-factor authentication with a physical authenticator (something you have).	Both		
	"	(2) An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier SHALL be established.	Both		
	"	(3) The sensor or endpoint SHALL be authenticated prior to capturing the biometric sample from the claimant.	Both		
	"	(4) The biometric system SHALL operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better. This FMR SHALL be achieved under conditions of a conformant attack (i.e., zero-effort impostor attempt) as defined in [ISO/IEC 30107-1].	Both		
	"	(5) The biometric system SHALL allow no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if PAD demonstrating at least 90% resistance to presentation attacks is implemented.	Both	Agency is responsible for ensuring minimum controls as defines in the CJIS Security Policy for any device-level authenticators.	Genasys Cloud Services does not use any physical authentication factors.
	"	(6) Once the limit on authentication failures has been reached, the biometric authenticator SHALL either:	Both		
	"	i. Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt, or	Both		
	"	ii. disable the biometric user authentication and offer another factor (e.g., a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already available.	Both		
	"	(7) The verifier SHALL make a determination of sensor and endpoint performance, integrity, and authenticity.	Both		
5.6: IA-5	"	(8) If biometric comparison is performed centrally, then use of the biometric as an authentication factor SHALL be limited to one or more specific devices that are identified using approved cryptography.	Both		
	"	(9) If biometric comparison is performed centrally, then a separate key SHALL be used for identifying the device.	Both		
	"	(10) If biometric comparison is performed centrally, then biometric revocation, referred to as biometric template protection in ISO/IEC 24745, SHALL be implemented.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	(11) If biometric comparison is performed centrally, all transmission of biometrics SHALL be over the authenticated protected channel.	Both		
	"	(12) Biometric samples and any biometric data derived from the biometric sample such as a probe produced through signal processing SHALL be zeroized immediately after any training or research data has been derived	Both		
	"	n. Authenticator binding refers to the establishment of an association between a specific authenticator and a subscriber's account, enabling the authenticator to be used — possibly in conjunction with other authenticators — to authenticate for that account.		Agency is responsible for binding device-level authenticators to specific user accounts, recording authenticators and ensuring authenticators are in compliance with each AAL.	Genasys Cloud Services is responsible for binding application-level authenticators to specific user accounts, recording authenticators and ensuring authenticators are in compliance with each AAL.
	"	(1) Authenticators SHALL be bound to subscriber accounts by either issuance by the CSP as part of enrollment or associating a subscriber-provided authenticator that is acceptable to the CSP.	Both		
	"	(2) Throughout the digital identity lifecycle, CSPs SHALL maintain a record of all authenticators that are or have been associated with each identity.	Both		
	"	(3) The CSP or verifier SHALL maintain the information required for throttling authentication attempts.	Both		
	"	(4) The CSP SHALL also verify the type of user-provided authenticator so verifiers can determine compliance with requirements at each AAL.	Both		
	"	(5) The record created by the CSP SHALL contain the date and time the authenticator was bound to the account.	Both		
	"	(6) When any new authenticator is bound to a subscriber account, the CSP SHALL ensure that the binding protocol and the protocol for provisioning the associated key(s) are done at AAL2.	Both		
	"	(7) Protocols for key provisioning SHALL use authenticated protected channels or be performed in person to protect against man-in-the- middle attacks.	Both		
	"	(8) Binding of multi-factor authenticators SHALL require multi-factor authentication (or equivalent) at identity proofing.	Both		
	"	(9) At enrollment, the CSP SHALL bind at least one, and SHOULD bind at least two, physical (something you have) authenticators to the subscriber's online identity, in addition to a memorized secret or one or more biometrics.	Both		
	"	(10) At enrollment, authenticators at AAL2 and IAL2 SHALL be bound to the account.	Both		
	"	(11) If the subscriber is authenticated at AAL1, then the CSP SHALL NOT expose personal information, even if self-asserted, to the subscriber.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	(12) If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then the applicant SHALL identify themselves in each new binding transaction by presenting a temporary secret which was either established during a prior transaction, or sent to the applicant's phone number, email address, or postal address of record.	Both	Agency is responsible for ensuring minimum controls as defined in the CJIS Security Policy for any device-level authenticators.	The first step of enrollment in Genasys Cloud Services is to establish an account with a unique email and password. Impeded enrollments can continue upon successful authentication where a protected session is created.
5.6: IA-5	"	(13) If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then long-term authenticator secrets are delivered to the applicant within a protected session.	Both		
	"	(14) If enrollment and binding are being done in person and cannot be completed in a single physical encounter, the applicant SHALL identify themselves in person by either using a secret as described in IA-5 n (12) above, or through use of a biometric that was recorded during a prior encounter.	Both		
	"	(15) If enrollment and binding are being done in person and cannot be completed in a single physical encounter, temporary secrets SHALL NOT be reused.	Both		
	"	(16) If enrollment and binding are being done in person and cannot be completed in a single physical encounter and the CSP issues long-term authenticator secrets during a physical transaction, they SHALL be loaded locally onto a physical device that is issued in person to the applicant or delivered in a manner that confirms the address of record.	Both	Agency is responsible for ensuring minimum controls as defined in the CJIS Security Policy for any device-level authenticators.	Genasys Cloud Services does not use any physical authentication factors.
	"	(17) Before adding a new authenticator to a subscriber's account, the CSP SHALL first require the subscriber to authenticate at AAL2 (or a higher AAL) at which the new authenticator will be used.	Both		Genasys Cloud Services requires application-level re-authentication if any new authenticators are introduced.
	"	(18) If the subscriber's account has only one authentication factor bound to it, the CSP SHALL require the subscriber to authenticate at AAL1 in order to bind an additional authenticator of a different authentication factor.	Both		Genasys Cloud Services always has at least two authentication factors bound to each user.
	"	(19) If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2, that subscriber SHALL repeat the identity proofing process described in IA-12.	Both	Agency is responsible for identity proofing users prior to inviting them into Genasys Cloud Services.	Genasys Cloud Services does not identity proof users beyond their multi-factor authenticators.
	"	(20) If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2 or IAL3, the CSP SHALL require the claimant to authenticate using an authenticator of the remaining factor, if any, to confirm binding to the existing identity.	Both		
	"	(21) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then it requires entry of a confirmation code sent to an address of record.	Both	Agency is responsible for ensuring minimum controls as defined in the CJIS	Genasys Cloud Services does not use any physical authentication factors.

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	(22) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL consist of at least 6 random alphanumeric characters generated by an approved random bit generator [SP 800-90Ar1].	Both	Security Policy for any device-level authenticators.	
	"	(23) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL be valid for a maximum of 7 days but MAY be made valid up to 21 days via an exception process to accommodate addresses outside the direct reach of the U.S. Postal Service. Confirmation codes sent by means other than physical mail SHALL be valid for a maximum of 5 minutes.	Both		
	"	o. Session Management: The following requirements apply to applications where a session is maintained between the subscriber and relying party to allow multiple interactions without repeating the authentication event each time.		Agency is responsible for ensuring minimum controls as defined in the CJIS Security Policy for any device-level session management.	Genasys Cloud Services strictly adheres to all outlined requirements for session management at the application-level.
	"	(1) Session Binding Requirements: A session occurs between the software that a subscriber is running — such as a browser, application, or operating system (i.e., the session subject) — and the RP or CSP that the subscriber is accessing (i.e., the session host).	Both		
5.6: IA-5	"	a. A session is maintained by a session secret which SHALL be shared between the subscriber's software and the service being accessed.	Both		
	"	b. The secret SHALL be presented directly by the subscriber's software or possession of the secret SHALL be proven using a cryptographic mechanism.	Both		
	"	c. The secret used for session binding SHALL be generated by the session host in direct response to an authentication event.	Both		
	"	d. A session SHALL NOT be considered at a higher AAL than the authentication event.	Both		
	"	e. Secrets used for session binding SHALL be generated by the session host during an interaction, typically immediately following authentication.	Both		
	"	f. Secrets used for session binding SHALL be generated by an approved random bit generator [SP 800-90Ar1].	Both		
	"	g. Secrets used for session binding SHALL contain at least 64 bits of entropy.	Both		
	"	h. Secrets used for session binding SHALL be erased or invalidated by the session subject when the subscriber logs out.	Both		
	"	i. Secrets used for session binding SHALL be sent to and received from the device using an authenticated protected channel.	Both		
	"	j. Secrets used for session binding SHALL time out and not be accepted after the times specified in IA-5 j (13) as appropriate for the AAL.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	k. Secrets used for session binding SHALL NOT be available to insecure communications between the host and subscriber's endpoint.	Both		
	"	l. Authenticated sessions SHALL NOT fall back to an insecure transport, such as from https to http, following authentication.	Both		
	"	m. URLs or POST content SHALL contain a session identifier that SHALL be verified by the RP to ensure that actions taken outside the session do not affect the protected session.	Both		
	"	n. Browser cookies SHALL be tagged to be accessible only on secure (HTTPS) sessions.	Both		
	"	o. Browser cookies SHALL be accessible to the minimum practical set of hostnames and paths.	Both		
	"	p. Expiration of browser cookies SHALL NOT be depended upon to enforce session timeouts.	Both		
	"	q. The presence of an OAuth access token SHALL NOT be interpreted by the RP as presence of the subscriber, in the absence of other signals.	Both		
	"	(2) Reauthentication Requirements			
	"	a. Continuity of authenticated sessions SHALL be based upon the possession of a session secret issued by the verifier at the time of authentication and optionally refreshed during the session.	Both	Agency is responsible for ensuring minimum controls as defines in the CJIS Security Policy for any device-level session management.	Genasys Cloud Services strictly adheres to all outlined requirements for session management at the application-level.
	"	b. Session secrets SHALL be non-persistent, i.e., they SHALL NOT be retained across a restart of the associated application or a reboot of the host device.	Both		
	"	c. Periodic reauthentication of sessions (at least every 12 hours per session) SHALL be performed to confirm the continued presence of the subscriber at an authenticated session.	Both		
	"	d. A session SHALL NOT be extended past the guidelines in IA-5 o (2) a – j based on presentation of the session secret alone.	Both		
	"	e. Prior to session expiration, the reauthentication time limit SHALL be extended by prompting the subscriber for the authentication factor(s) of a memorized secret or biometric.	Both		
5.6: IA-5	"	f. If federated authentication is being used, then since the CSP and RP often employ separate session management technologies, there SHALL NOT be any assumption of correlation between these sessions.	Both		
	"	g. An RP requiring reauthentication through a federation protocol SHALL — if possible within the protocol — specify the maximum (see IA-5 j (10)) acceptable authentication age to the CSP.	Both		
	"	h. If federated authentication if being used and an RP has specific authentication age (see IA-5 j (10)) requirements that it has communicated to the CSP, then the CSP SHALL reauthenticate the subscriber if they have not been authenticated within that time period.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	i. If federated authentication is being used, the CSP SHALL communicate the authentication event time to the RP to allow the RP to decide if the assertion is sufficient for reauthentication and to determine the time for the next reauthentication event.	Both		
5.6: IA-5 (1)	Authenticator Management | Authenticator Types	(a) Memorized Secret Authenticators and Verifiers:			
	"	(1) Maintain a list of commonly-used, expected, or compromised passwords and update the list quarterly and when organizational passwords are suspected to have been compromised directly or indirectly;	Both	Agency should maintain a list of commonly-used passwords and prevent them from use on devices that access Genasys Cloud Services.	Genasys Cloud Services maintains a list of commonly-used passwords and prevents them from use as an authenticator.
	"	(2) Require immediate selection of a new password upon account recovery;	Both		Genasys Cloud Services requires a new password is set upon account recovery.
	"	(3) Allow user selection of long passwords and passphrases, including spaces and all printable characters;	Both		Long passwords, spaces and use of all printable characters are allowed for passwords.
	"	(4) Employ automated tools to assist the user in selecting strong password authenticators;	Both		Password strength utilities and recommendations are displayed when a user sets a new password.
	"	(5) Enforce the following composition and complexity rules: when agencies elect to follow basic password standards.	Both	Agency must address this requirement through appropriate policies, procedures, and configurations in how they use Genasys Cloud Services. Genasys Cloud Services provide many security features and capabilities including password strength displays, encryption to protect data in transit, and masking of password in the entry form.	Genasys Cloud Services password complexity requirements are maintained in compliance with the basic password standards.
	"	(a) Not be a proper name.	Both		
	"	(b) Not be the same as the Userid.	Both		
	"	(c) Expire within a maximum of 90 calendar days.	Both		
	"	(d) Not be identical to the previous ten (10) passwords.	Both		
	"	(e) Not be displayed when entered.	Both		
	"	(6) If chosen by the subscriber, memorized secrets SHALL be at least 8 characters in length.	Both		
	"	(7) If chosen by the CSP or verifier using an approved random number generator, memorized secrets SHALL be at least 6 characters in length.	Both		
	"	(8) Truncation of the secret SHALL NOT be performed.	Both		
	"	(9) Memorized secret verifiers SHALL NOT permit the subscriber to store a “hint” that is accessible to an unauthenticated claimant.	Both		Hints are not allowed or stored within Genasys Cloud Services
	"	(10) Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., “What was the name of your first pet?”) when choosing memorized secrets.	Both		Passwords nor multi-factor authenticators use predefined prompts or questions.
	"	(11) When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly used, expected, or compromised.	Both		Genasys Cloud Services password complexity requirements are maintained in compliance with the basic password standards.

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	(12) If a chosen secret is found in the list, the CSP or verifier SHALL advise the subscriber that they need to select a different secret.	Both		Passwords that are found to be commonly used do not meet the minimum password strength requirements for Genasys Cloud Services and are therefore, not allowed.
	"	(13) If a chosen secret is found in the list, the CSP or verifier SHALL provide the reason for rejection.	Both		
	"	(14) If a chosen secret is found in the list, the CSP or verifier SHALL require the subscriber to choose a different value.	Both		
	"	(15) Verifiers SHALL implement a rate-limiting mechanism that effectively limits failed authentication attempts that can be made on the subscriber's account to no more than five.	Both		Genasys Cloud Services strictly adheres to all outlined requirements for authentication management and types at the application-level.
	"	(16) Verifiers SHALL force a change of memorized secret if there is evidence of compromise of the authenticator.	Both		
	"	(17) The verifier SHALL use approved encryption when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.	Both		
	"	(18) The verifier SHALL use an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.	Both		
	"	(19) Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks.	Both		
	"	(20) Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function.	Both		
	"	(21) The salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.	Both		
	"	(22) Both the salt value and the resulting hash SHALL be stored for each subscriber using a memorized secret authenticator	Both		
	"	(23) If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be generated with an approved random bit generator and of sufficient length.	Both		
	"	(24) If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL provide at least the minimum-security strength.	Both		
	"	(25) If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be stored separately from the memorized secrets.	Both		
	"	(b) Look-Up Secret Authenticators and Verifiers			
	"	(1) CSPs creating look-up secret authenticators SHALL use an approved random bit generator to generate the list of secrets.	Both		
	"	(2) Look-up secrets SHALL have at least 20 bits of entropy.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	(3) If look-up secrets are distributed online, then they SHALL be distributed over a secure channel in accordance with the post-enrollment binding requirements in IA-5 n 17 through 25.	Both		
	"	(4) Verifiers of look-up secrets SHALL prompt the claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret.	Both		
	"	(5) A given secret from an authenticator SHALL be used successfully only once.	Both		
	"	(6) If a look-up secret is derived from a grid (bingo) card, then each cell of the grid SHALL be used only once.	Both		
	"	(7) Verifiers SHALL store look-up secrets in a form that is resistant to offline attacks.	Both		
5.6: IA-5 (1)	"	(8) If look-up secrets have at least 112 bits of entropy, then they SHALL be hashed with an approved one-way function	Both		
	"	(9) If look-up secrets have less than 112 bits of entropy, then they SHALL be salted and hashed using a suitable one-way key derivation function.	Both		
	"	(10) If look-up secrets have less than 112 bits of entropy, then the salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.	Both		
	"	(11) If look-up secrets have less than 112 bits of entropy, then both the salt value and the resulting hash SHALL be stored for each look-up secret	Both		
	"	(12) If look-up secrets that have less than 64 bits of entropy, then the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account.	Both		
	"	(13) The verifier SHALL use approved encryption when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.	Both		
	"	(14) The verifier SHALL use an authenticated protected channel when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.	Both		
	"	(c) Out-of-Band Authenticators and Verifiers		Agency is responsible for ensuring minimum controls as defined in the CJIS Security Policy for any device-level out-of-band authenticators.	Genasys Cloud Services strictly adheres to all outlined requirements for out-of-band authenticators at the application-level.
	"	(1) The out-of-band authenticator SHALL establish a separate channel with the verifier in order to retrieve the out-of-band secret or authentication request.	Both		
	"	(2) Communication over the secondary channel SHALL be encrypted unless sent via the public switched telephone network (PSTN).	Both		
	"	(3) Methods that do not prove possession of a specific device, such as voiceover-IP (VOIP) or email, SHALL NOT be used for out-of-band authentication.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	(4) If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL uniquely authenticate itself by establishing an authenticated protected channel with the verifier.	Both		
	"	(5) If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL communicate with the verifier using approved cryptography.	Both		
	"	(6) If PSTN is not being used for out-of-band communication, then the key used to authenticate the out-of-band device SHALL be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE, secure element).	Both		
	"	(7) If the PSTN is used for out-of-band authentication and a secret is sent to the out-of-band device via the PSTN, then the out-of-band authenticator SHALL uniquely authenticate itself to a mobile telephone network using a SIM card or equivalent that uniquely identifies the device.	Both		
	"	(8) If the out-of-band authenticator sends an approval message over the secondary communication channel, it SHALL either accept transfer of a secret from the primary channel to be sent to the verifier via the secondary communications channel, or present a secret received via the secondary channel from the verifier and prompt the claimant to verify the consistency of that secret with the primary channel, prior to accepting a yes/no response from the claimant which it sends to the verifier.	Both		
5.6: IA-5 (1)	"	(9) The verifier SHALL NOT store the identifying key itself, but SHALL use a verification method (e.g., an approved hash function or proof of possession of the identifying key) to uniquely identify the authenticator.	Both		
	"	(10) Depending on the type of out-of-band authenticator, one of the following SHALL take place: transfer of a secret to the primary channel, transfer of a secret to the secondary channel, or verification of secrets by the claimant.	Both		
	"	(11) If the out-of-band authenticator operates by transferring the secret to the primary channel, then the verifier SHALL transmit a random secret to the out-of-band authenticator and then wait for the secret to be returned on the primary communication channel.	Both		
	"	(12) If the out-of-band authenticator operates by transferring the secret to the secondary channel, then the verifier SHALL display a random authentication secret to the claimant via the primary channel and then wait for the secret to be returned on the secondary channel from the claimant’s out-of- band authenticator.	Both		
	"	(13) If the out-of-band authenticator operates by verification of secrets by the claimant, then the verifier SHALL display a random authentication secret to the claimant via the primary channel, send the same secret to the out-of-band authenticator via the secondary	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
		channel for presentation to the claimant, and then wait for an approval (or disapproval) message via the secondary channel.			
	"	(14) The authentication SHALL be considered invalid if not completed within 10 minutes.	Both		
	"	(15) Verifiers SHALL accept a given authentication secret only once during the validity period.	Both		
	"	(16) The verifier SHALL generate random authentication secrets with at least 20 bits of entropy.	Both		
	"	(17) The verifier SHALL generate random authentication secrets using an approved random bit generator.	Both		
	"	(18) If the authentication secret has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 l (3) through (4).	Both		
	"	(19) If out-of-band verification is to be made using the PSTN, then the verifier SHALL verify that the pre-registered telephone number being used is associated with a specific physical device.	Both		
	"	(20) If out-of-band verification is to be made using the PSTN, then changing the pre-registered telephone number is considered to be the binding of a new authenticator and SHALL only occur as described in IA-5 n (17) through (25).	Both		
	"	(21) If PSTN is used for out-of-band authentication, then the CSP SHALL offer subscribers at least one alternate authenticator that is not RESTRICTED and can be used to authenticate at the required AAL.	Both		
	"	(22) If PSTN is used for out-of-band authentication, then the CSP SHALL Provide meaningful notice to subscribers regarding the security risks of the RESTRICTED authenticator and availability of alternative(s) that are not RESTRICTED.	Both		
5.6: IA-5 (1)	"	(23) If PSTN is used for out-of-band authentication, then the CSP SHALL address any additional risk to subscribers in its risk assessment.	Both		
	"	(24) If PSTN is used for out-of-band authentication, then the CSP SHALL develop a migration plan for the possibility that the RESTRICTED authenticator is no longer acceptable at some point in the future and include this migration plan in its digital identity acceptance statement.	Both		
	"	(d) OTP Authenticators and Verifiers			

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	(1) The secret key and its algorithm SHALL provide at least the minimum security strength of 112 bits as of the date of this publication.	Both	Agency is responsible for ensuring minimum controls as defined in the CJIS Security Policy for any OTP authenticators.	Genasys Could Services strictly adheres to the requirements as defined in the CJIS Security Policy for any application-level OTP authenticators.
	"	(2) The nonce SHALL be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.	Both		
	"	(3) OTP authenticators — particularly software-based OTP generators —SHALL NOT facilitate the cloning of the secret key onto multiple devices.	Both		
	"	(4) The authenticator output SHALL have at least 6 decimal digits (approximately 20 bits) of entropy.	Both		
	"	(5) If the nonce used to generate the authenticator output is based on a realtime clock, then the nonce SHALL be changed at least once every 2 minutes.	Both		
	"	(6) The OTP value associated with a given nonce SHALL be accepted only once.	Both		
	"	(7) The symmetric keys used by authenticators are also present in the verifier and SHALL be strongly protected against compromise.	Both		
	"	(8) If a single-factor OTP authenticator is being associated with a subscriber account, then the verifier or associated CSP SHALL use approved cryptography to either generate and exchange or to obtain the secrets required to duplicate the authenticator output.	Both		
	"	(9) The verifier SHALL use approved encryption when collecting the OTP.	Both		
	"	(10) The verifier SHALL use an authenticated protected channel when collecting the OTP.	Both		
	"	(11) If a time-based OTP is used, it SHALL have a defined lifetime (recommended 30 seconds) that is determined by the expected clock drift — in either direction — of the authenticator over its lifetime, plus allowance for network delay and user entry of the OTP.	Both		
	"	(12) Verifiers SHALL accept a given time-based OTP only once during the validity period.	Both		
	"	(13) If the authenticator output has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber’s account as described in IA-5 l (3) through (4).	Both		
	"	(14) If the authenticator is multi-factor, then each use of the authenticator SHALL require the input of the additional factor.	Both		
	"	(15) If the authenticator is multi-factor and a memorized secret is used by the authenticator for activation, then that memorized secret SHALL be a randomly chosen numeric secret at least 6	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
		decimal digits in length or other memorized secret meeting the requirements of IA-5 (1)(a).			
	"	(16) If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 l (3) through (4).	Both		
	Authenticator Management | Authenticator Types (continued)	(17) If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.	Both		
	"	(18) If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an OTP has been generated.	Both		
	"	(19) If the authenticator is multi-factor, the verifier or CSP SHALL establish, via the authenticator source, that the authenticator is a multi-factor device.	Both		
	"	(20) In the absence of a trusted statement that it is a multi-factor device, the verifier SHALL treat the authenticator as single-factor, in accordance with IA-5 (1) (d) (1) through (13).	Both		
5.6: IA-5 (1)	"	(e) Cryptographic Authenticators and Verifiers (including single- and multi-factor cryptographic authenticators, both hardware- and software-based)		Agency is responsible for ensuring minimum controls as defined in the CJIS Security Policy for any cryptographic authenticators.	Genasys Cloud Services strictly adheres to the requirements as defined in the CJIS Security Policy for any cryptographic authenticators.
	"	(1) If the cryptographic authenticator is software based, the key SHALL be stored in suitably secure storage available to the authenticator application.	Both		
	"	(2) If the cryptographic authenticator is software based, the key SHALL be strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access.	Both		
	"	(3) If the cryptographic authenticator is software based, it SHALL NOT facilitate the cloning of the secret key onto multiple devices.	Both		
	"	(4) If the authenticator is single-factor and hardware-based, secret keys unique to the device SHALL NOT be exportable (i.e., cannot be removed from the device).	Both		
	"	(5) If the authenticator is hardware-based, the secret key and its algorithm SHALL provide at least the minimum-security length of 112 bits as of the date of this publication.	Both		
	"	(6) If the authenticator is hardware-based, the challenge nonce SHALL be at least 64 bits in length.	Both		
	"	(7) If the authenticator is hardware-based, approved cryptography SHALL be used.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	(8) Cryptographic keys stored by the verifier SHALL be protected against modification.	Both		
	"	(9) If symmetric keys are used, cryptographic keys stored by the verifier SHALL be protected against disclosure.	Both		
	"	(10) The challenge nonce SHALL be at least 64 bits in length.	Both		
	"	(11) The challenge nonce SHALL either be unique over the authenticator's lifetime or statistically unique (i.e., generated using an approved random bit generator).	Both		
	"	(12) The verification operation SHALL use approved cryptography.	Both		
	"	(13) If a multi-factor cryptographic software authenticator is being used, then each authentication requires the presentation of the activation factor.	Both		
	"	(14) If the authenticator is multi-factor, then any memorized secret used by the authenticator for activation SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1) (a).	Both		
5.6: IA-5 (1)	"	(15) If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 l (3) through (4).	Both		
	"	(16) If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.	Both		
	"	(17) If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an authentication transaction has taken place.	Both		
5.6: IA-5 (2)	Authenticator Management | Public Key Based Authentication	(a) For public key-based authentication:		Agency must address this requirement through appropriate policies, procedures, and configurations in how they use Genasys Cloud Services.	Genasys Cloud Services does not use any public key-based authenticators.
	"	(1) Enforce authorized access to the corresponding private key; and	Both		
	"	(2) Map the authenticated identity to the account of the individual or group; and	Both		
	"	(b) When public key infrastructure (PKI) is used:	Both		
	"	(1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and	Both		
	"	(2) Implement a local cache of revocation data to support path discovery and validation.	Both		
5.6: IA-5 (6)	Authenticator Management | Protection of Authenticators	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	Both		Genasys Cloud Services encrypts and protects all used authenticators.

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
5.6: IA-6	Authentication Feedback	Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.	Both		
5.6: IA-7	Cryptographic Module Authentication	Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.	Both		
5.6: IA-8	Identification and Authentication (Non-Organizational Users)	Control: Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.	Both		N/A
5.6: IA-8 (1)	Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from Other Agencies	Accept and electronically verify Personal Identity Verification-compliant credentials from other federal, state, local, tribal, or territorial (SLTT) agencies.	Both		Genasys Cloud Services does not verify PIV credentials. It is the responsibility of the agency to verify this prior to inviting a user into Genasys Cloud Services.
5.6: IA-8 (2)	Identification and Authentication (Non-Organizational Users) | Acceptance of External Authenticators	(a) Accept only external authenticators that are NIST-compliant; and	Both		Any external authenticators used by Genasys Cloud Services are fully compliant with 800-63C's identity federation and assertion recommendations.
	"	(b) Document and maintain a list of accepted external authenticators.	Both		
5.6: IA-8 (4)	Identification and Authentication (Non-Organizational Users) | Use of Defined Profiles	Conform to the following profiles for identity management: Security Assertion Markup Language (SAML) or OpenID Connect.	Both		Genasys Cloud Services has the option to use either SAML or OpenID standards.
5.6: IA-11	Re-Authentication	Require users to re-authenticate when: roles, authenticators, or credentials change, security categories of systems change, the execution of privileged functions occur, or every 12 hours.	Both		Users within Genasys Cloud Services are required to re-authenticate as defined in the CJIS Security Policy.
5.6: IA-12	Identity Proofing	a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;	Both	Agency is responsible for identity proofing users prior to inviting and giving access to Genasys Cloud Services.	Genasys identity proofs internal personnel who have access to production systems and environments. Genasys does not identity proof subscribers to Genasys Cloud Services.
	"	b. Resolve user identities to a unique individual; and	Both		
	"	c. Collect, validate, and verify identity evidence.	Both		
5.6: IA-12 (2)	Identity Proofing | Identity Evidence	Require evidence of individual identification be presented to the registration authority.	Both		
5.6: IA-12 (3)	Identity Proofing | Identity Evidence Validation and Verification	a. Require that the presented identity evidence be validated and verified through agency defined resolution, validation, and verification methods.	Both		
	"	b. Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits.	Both		
	"	c. 1. Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity in a given context.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	2. Collection of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation, and verification.	Both		
	"	d. The CSP SHALL provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes.	Both		
	"	e. If CSPs process attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively “identity service”), related fraud mitigation, or to comply with law or legal process, then CSPs SHALL implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing.	Both		
	"	f. If the CSP employs consent as part of its measures to maintain predictability and manageability, …then it SHALL NOT make consent for the additional processing a condition of the identity service.	Both		
	"	g. The CSP SHALL provide mechanisms for redress of applicant complaints or problems arising from the identity proofing.	Both		
	"	These [redress] mechanisms SHALL be easy for applicants to find and use.	Both		
	"	h. The CSP SHALL assess the [redress] mechanisms for their efficacy in achieving resolution of complaints or problems.	Both		
	"	i. The identity proofing and enrollment processes SHALL be performed according to an applicable written policy or *practice statement* that specifies the particular steps taken to verify identities.	Both		
	"	j. The *practice statement* SHALL include control information detailing how the CSP handles proofing errors that result in an applicant not being successfully enrolled.	Both		
	"	k. The CSP SHALL maintain a record, including audit logs, of all steps taken to verify the identity of the applicant as long as the identity exists in the information system.	Both		
	"	l. The CSP SHALL record the types of identity evidence presented in the proofing process.	Both		
	"	m. The CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine:	Both		
	"	1. Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein;	Both		
5.6: IA-12 (3)	"	2. The PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing (Note: Specific federal requirements may apply); and	Both	Agency is responsible for identity proofing users prior to inviting and giving access to Genasys Cloud Services.	Genasys identity proofs internal personnel who have access to production systems and environments. Genasys

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	3. The schedule of retention for these records (Note: CSPs may be subject to specific retention policies in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply).	Both		does not identity proof subscribers to Genasys Cloud Services.
	"	n. All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source.	Both		
	"	o. "The entire proofing transaction, including transactions that involve a third party, SHALL occur over authenticated protected channels. "	Both		
	"	p. "If the CSP uses fraud mitigation measures, then the CSP SHALL conduct a privacy risk assessment for these mitigation measures. "	Both		
	"	Such assessments SHALL include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per requirement IA-12(3) k – m above.	Both		
	"	q. In the event a CSP ceases to conduct identity proofing and enrollment processes, then the CSP SHALL be responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention.	Both		
	"	r. Regardless of whether the CSP is a federal agency or non- federal entity, the following requirements apply to the federal agency offering or using the proofing service:	Both		
	"	1. The agency SHALL consult with their Senior Agency Official for Privacy (SAOP) to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers Privacy Act requirements.	Both		
	"	2. The agency SHALL publish a System of Records Notice (SORN) to cover such collection, as applicable.	Both		
	"	3. The agency SHALL consult with their SAOP to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers E-Government Act of 2002 requirements.	Both		
	"	4. The agency SHALL publish a Privacy Impact Assessment (PIA) to cover such collection, as applicable.	Both		
	"	s. An enrollment code SHALL be comprised of one of the following:	Both		
	"	1. Minimally, a random six character alphanumeric or equivalent entropy. For example, a code generated using an approved random number generator or a serial number for a physical hardware authenticator; OR	Both		
	"	2. A machine-readable optical label, such as a QR Code, that contains data of similar or higher entropy as a random six character alphanumeric.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	t. Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP.	Both		
	"	u. This criterion applies to CSPs that provide identity proofing and enrollment services to minors (under the age of 18):	Both		
	Identity Proofing | Identity Evidence Validation and Verification (continued)	If the CSP provides identity proofing and enrollment services to minors (under the age of 18), then…the CSP SHALL give special consideration to the legal restrictions of interacting with minors unable to meet the evidence requirements of identity proofing [to ensure compliance with the Children's Online Privacy Protection Act of 1998 (COPPA), and other laws, as applicable]. "	Both	Agency is responsible for identity proofing users prior to inviting and giving access to Genasys Cloud Services.	Genasys does not provide identity proofing to minors.
	"	Requirements v and w apply to the collection of biometric characteristics for in-person (physical or supervised remote) identity proofing and are mandatory at IAL3. These criteria also apply to CSPs that optionally choose to collect biometric characteristics through in-person identity-proofing identity proofing and enrollment at IAL2.		Agency is responsible for managing any biometric authentication for any devices used to access Genasys Cloud Services.	Genasys Cloud Services does not use biometrics as an authenticator.
	"	v. The CSP SHALL have the operator view the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.	Both		
	"	w. The CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject. All biometric performance requirements in IA-5 m (1) through (12) apply.	Both		
	"	x. The CSP SHALL support in-person or remote identity proofing, or both.	Both		
	"	y. The CSP SHALL collect the following from the applicant:	Both		
	"	1. One piece of SUPERIOR or STRONG evidence if the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source; OR	Both		
	"	2. Two pieces of STRONG evidence; OR	Both		
	"	3. One piece of STRONG evidence plus two pieces of FAIR evidence	Both		
	"	z. The CSP SHALL validate each piece of evidence with a process that can achieve the same strength as the evidence presented (see 'z' above). For example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of STRONG.	Both		
	"	aa. The CSP SHALL verify identity evidence as follows:	Both		
	"	At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of STRONG.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	bb. For IAL2 remote proofing: The collection of biometric characteristics for physical or biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity performed remotely SHALL adhere to all requirements as specified in IA-5 m.	Both		
	"	cc. Knowledge-based verification (KBV) SHALL NOT be used for in-person (physical or supervised remote) identity verification.	Both		
	"	dd. The CSP SHALL employ appropriately tailored security controls, to include control enhancements, from the moderate or high baseline of security controls defined in the CJIS Security Policy.	Both		
	"	The CSP SHALL ensure that the minimum assurance-related controls for moderate impact systems are satisfied.	Both		
5.6: IA-12 (3)	Identity Proofing | Identity Evidence Validation and Verification (continued)	ee. Supervised Remote Identity Proofing: Supervised remote identity proofing is intended to provide controls for comparable levels of confidence and security to in-person IAL3 identity proofing for identity proofing processes that are performed remotely. Supervised remote identity proofing is optional for CSPs; that is, if a CSP chooses to use supervised remote identity proofing, then the following requirements, (1) through (8), would apply. It should be noted that the term “supervised remote identity proofing” has specialized meaning and is used only to refer to the specialized equipment and the following control requirements, (1) through (8). In addition to those requirements presented in this document, as well as the applicable identity validation and verification requirements, CSPs that provide supervised remote identity proofing services must demonstrate conformance with the requirements contained in this section. The following requirements for supervised remote proofing apply specifically to IAL3. If the equipment/facilities used for supervised remote proofing are used for IAL2 identity proofing, the following requirements, (1) through (8), for supervised remote proofing do not apply. In this case, the requirements for conventional remote identity proofing are applicable.	Both	Agency is responsible for identity proofing users prior to inviting and giving access to Genasys Cloud Services.	Genasys does not provide identity proofing.
	"	(1) Supervised remote identity proofing and enrollment transactions SHALL meet the following requirements, in addition to the IAL3 validation and verification requirements specified in Section 4.6 .	Both		
	"	(2) The CSP SHALL monitor the entire identity proofing session, from which the applicant SHALL NOT depart — for example, by a continuous high-resolution video transmission of the applicant.	Both		
	"	(3) The CSP SHALL have a live operator participate remotely with the applicant for the entirety of the identity proofing session.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	(4) The CSP SHALL require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator.	Both		
	"	(5) The CSP SHALL require that all digital validation of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors.	Both		
	"	(6) The CSP SHALL require operators to have undergone a training program to detect potential fraud and to properly perform a supervised remote proofing session.	Both		
	"	(7) The CSP SHALL employ physical tamper detection and resistance features appropriate for the environment in which it is located.	Both		
	"	(8) The CSP SHALL ensure that all communications occur over a mutually authenticated protected channel.	Both		
	"	ff. Trusted Referee: The use of trusted referees is optional for CSPs; that is, if a CSP chooses to use trusted referees for identity proofing and enrollment, then the following requirements, (1) through (3) would apply. The use of trusted referees is intended to assist in the identity proofing and enrollment for populations that are unable to meet IAL2 identity proofing requirements, or otherwise would be challenged to perform identity proofing and enrollment process requirements. Such populations may include, but are not limited to:	Both		
	"	· disabled individuals;	Both		
	"	· elderly individuals;	Both		
	"	· homeless individuals,	Both		
	"	· individuals with little or no access to online services or computing devices;	Both		
	"	· unbanked and individuals with little or no credit history;	Both		
	"	· victims of identity theft;	Both		
	"	· children under 18; and	Both		
	"	· immigrants.	Both		
	"	In addition to those requirements presented in the General section of this document, as well as the applicable IAL requirements, CSPs that use trusted referees in their identity proofing services must demonstrate conformance with the requirements contained in this section.		Agency is responsible for identity proofing users prior to inviting and giving access to Genasys Cloud Services.	Genasys does not provide identity proofing.
	"	(1) If the CSP uses trusted referees, then…The CSP SHALL establish written policy and procedures as to how a trusted referee is determined and the lifecycle by which the trusted referee retains their status as a valid referee, to include any restrictions, as well as any revocation and suspension requirements.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	(2) If the CSP uses trusted referees, then…The CSP SHALL proof the trusted referee at the same IAL as the applicant proofing.	Both		
	"	(3) If the CSP uses trusted referees, then…The CSP SHALL determine the minimum evidence required to bind the relationship between the trusted referee and the applicant.	Both		
5.6: IA-12 (5)	(5) Identity Proofing | Address Confirmation	a. Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record.	Both		
	"	b. The CSP SHALL confirm address of record.	Both		
	"	c. Valid records to confirm address SHALL be issuing source(s) or authoritative source(s).	Both		
	"	Self-asserted address data that has not been confirmed in records SHALL NOT be used for confirmation.	Both		
	"	d. Note that IAL2-7 applies only to in-person proofing at IAL2.	Both		
	"	If the CSP performs in-person proofing for IAL2 and provides an enrollment code directly to the subscriber for binding to an authenticator at a later time, then the enrollment code…SHALL be valid for a maximum of seven (7) days.	Both		
	"	e. For remote identity proofing at IAL2:	Both		
	"	The CSP SHALL send an enrollment code to a confirmed address of record for the applicant.	Both		
	"	f. For remote identity proofing at IAL2:	Both		
	"	The applicant SHALL present a valid enrollment code to complete the identity proofing process.	Both		
	"	g. Note that the following enrollment code validity periods apply to enrollment codes sent to confirmed addresses of record for IAL2 remote in-person proofing only.	Both		
	"	Enrollment codes shall have the following maximum validities:	Both		
	"	i. 10 days, when sent to a postal address of record within the contiguous United States;	Both		
	"	ii. 30 days, when sent to a postal address of record outside the contiguous United States;	Both		
	"	iii. 10 minutes, when sent to a telephone of record (SMS or voice);	Both		
	"	iv. 24 hours, when sent to an email address of record.	Both		
	"	h. If the enrollment code sent to the confirmed address of record as part of the remote identity proofing process at IAL2 is also intended to be an authentication factor, then…it SHALL be reset upon first use.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	i. If the CSP performs remote proofing at IAL2 and optionally sends notification of proofing in addition to sending the required enrollment code, then…The CSP SHALL ensure the enrollment code and notification of proofing are sent to different addresses of record.	Both		
CJIS Policy Area: Configuration Management					
CM-1	Policy and Procedures	Develop, document, and disseminate to organizational personnel with configuration management responsibilities:	TBD	N/A	N/A
	"	1. Agency-level configuration management policy that:	TBD	N/A	N/A
	"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	TBD	N/A	N/A
	"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	TBD	N/A	N/A
	"	2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;	TBD	N/A	N/A
	"	b. Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the configuration management policy and procedures; and	TBD	N/A	N/A
	"	c. Review and update the current configuration management:	TBD	N/A	N/A
	"	1. Policy annually and following any hardware or software changes to systems which process, store, or transmit CJI; and	TBD	N/A	N/A
	"	2. Procedures annually and following any hardware or software changes to systems which process, store, or transmit CJI.	TBD	N/A	N/A
CM-2	Baseline Configuration	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system;	TBD	Agency is responsible for maintaining their own system diagram that contains the Genasys Cloud Services connection.	Genasys maintains a current system diagram for Genasys Cloud Services.
	"	b. Develop, document, and maintain a current and complete topological drawing depicting the interconnectivity of the agency network to criminal justice information systems and services; and	Both		
	"	c. Review and update the baseline configuration and topological drawing of the system:	Both		
	"	1. At least annually;	Both		
	"	2. When required due to security-relevant changes to the system and/or security incidents occur; and	Both		
	"	3. When system components are installed or upgraded.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
CM-2(2)	(2) Baseline Configuration | Automation Support for Accuracy and Currency	Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms such as configuration management tools, hardware, software, firmware inventory tools, and network management tools.	TBD	N/A	N/A
CM-2(3)	(3) Baseline Configuration | Retention of Previous Configurations	Retain at least one (1) of previous versions of baseline configurations of the system to support rollback.	TBD	N/A	N/A
CM-2(7)	(7) Baseline Configuration | Configure System and Components for High-Risk Areas	a. Issue devices (e.g., mobile devices) with CJISSECPOL compliant configurations to individuals traveling to locations that the organization deems to be of significant risk; and	TBD	N/A	N/A
	"	b. Apply the following controls to the systems or components when the individuals return from travel: examine the device for signs of physical tampering, purge and reimage disk drives and/or devices as required, and ensure all security controls are in place and functional	Agency	Agency must address this requirement through appropriate policies and procedures.	N/A
CM-3	Configuration Change Control	a. Determine and document the types of changes to the system that are configuration-controlled;	TBD	N/A	N/A
	"	b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;	TBD	N/A	N/A
	"	c. Document configuration change decisions associated with the system;	TBD	N/A	N/A
	"	d. Implement approved configuration-controlled changes to the system;	TBD	N/A	N/A
	"	e. Retain records of configuration-controlled changes to the system for two (2) years;	TBD	N/A	N/A
	"	f. Monitor and review activities associated with configuration-controlled changes to the system; and	TBD	N/A	N/A
	"	g. Coordinate and provide oversight for configuration change control activities through personnel with configuration management responsibilities, a Configuration Control Board, or Change Advisory Board that convenes regularly or when hardware or software changes (i.e., updates, upgrades, replacements, etc.) to the information system are required.	TBD	N/A	N/A
CM-3(2)	(2) Configuration Change Control | Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.	TBD	N/A	N/A
CM-3(4)	(4) Configuration Change Control | Testing, Validation, and Documentation of Changes	Require organizational personnel with information security and privacy responsibilities to be members of the Configuration Control Board or Change Advisory Board.	TBD	N/A	N/A
CM-4	Impact Analyses	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.	TBD	N/A	N/A

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
CM-4(2)	(2) Impact Analyses | Verification of Controls	After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.	TBD	N/A	N/A
CM-5	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	Both	Agency is responsible for restricting and controlling access to system configuration documentation.	Genasys system configuration documentation is classified as confidential and protected according to Genasys's internal classification and detailed within Genasys's Information Security Policy.
CM-6	Configuration Settings	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using established best practices and guidelines such as Defense Information Systems Agency (DISA) Secure Technical Implementation Guidelines (STIGs), Center for Internet Security (CIS) Benchmarks, or Federal Information Processing Standards;	TBD	N/A	N/A
	"	b. Implement the configuration settings;	TBD	N/A	N/A
	"	c. Identify, document, and approve any deviations from established configuration settings for system components that store, process, or transmit CJI based on operational requirements; and	TBD	N/A	N/A
	"	d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.	TBD	N/A	N/A
CM-7	Least Functionality	a. Configure the system to provide only essential capabilities to meet operational requirements; and	TBD	N/A	N/A
	"	b. Prohibit or restrict the use of specified functions, ports, protocols, software, and/or services: which are not required.	Both	Agency is responsible for restricting and controlling changes made by agency personnel to their Genasys Cloud Services.	Genasys designs and maintains the Genasys Cloud Services infrastructure under the principle of least functionality.
CM-7(1)	(1) Least Functionality | Periodic Review	a. Review the system annually, as the system changes, or incidents occur to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and	Both		
		b. Disable or remove functions, ports, protocols, software, and/or services within the system deemed to be unnecessary and/or unsecure.	TBD	N/A	N/A
CM-7(2)	(2) Least Functionality | Prevent Program Execution	Prevent program execution in accordance with rules of behavior and/or rules authorizing the terms and conditions of software program usage.	TBD	N/A	N/A
CM-7(5)	(5) Least Functionality | Authorized Software – Allow-By-Exception	a. Identify software programs authorized to execute on the system;	TBD	N/A	N/A
	"	b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and	TBD	N/A	N/A

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	c. Review and update the list of authorized software programs annually.	TBD	N/A	N/A
CM-8	System Component Inventory	a. Develop and document an inventory of system components that:	TBD	N/A	N/A
	"	1. Accurately reflects the system;	TBD	N/A	N/A
	"	2. Includes all components within the system;	TBD	N/A	N/A
	"	3. Does not include duplicate accounting of components or components assigned to any other system;	TBD	N/A	
	"	4. Is at the level of granularity deemed necessary for tracking and reporting; and	TBD	N/A	N/A
	"	5. Includes the following minimum information to achieve system component accountability: date of installation, model, serial number, manufacturer, supplier information, component type, software owner, software version number, software license information, and hardware and physical location; and	TBD	N/A	N/A
	"	b. Review and update the system component inventory annually.	TBD	N/A	N/A
CM-8(1)	(1) System Component Inventory | Updates During Installation and Removal	Update the inventory of system components as part of component installations, removals, and system updates.	TBD	N/A	N/A
CM-8(3)	(3) System Component Inventory | Automated Unauthorized Component Detection	a. Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms continuously or at least weekly; and	TBD	N/A	N/A
	"	b. Take the following actions when unauthorized components are detected: disable or isolate the unauthorized components and notify organizational personnel with security responsibilities.	TBD	N/A	N/A
CM-9	Configuration Management Plan	Develop, document, and implement a configuration management plan for the system that:	TBD	N/A	N/A
	"	a. Addresses roles, responsibilities, and configuration management processes and procedures;	TBD	N/A	N/A
	"	b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;	TBD	N/A	N/A
	"	c. Defines the configuration items for the system and places the configuration items under configuration management;	TBD	N/A	N/A
	"	d. Is reviewed and approved by organizational personnel with information security responsibilities and organizational personnel with configuration management responsibilities; and	TBD	N/A	N/A
	"	e. Protects the configuration management plan from unauthorized disclosure and modification.	TBD	N/A	N/A

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
CM-10	Software Usage Restrictions	a. Use software and associated documentation in accordance with contract agreements and copyright laws;	TBD	N/A	N/A
	"	b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and	TBD	N/A	N/A
	"	c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	TBD	N/A	N/A
CM-11	User-Installed Software	a. Establish agency-level policies governing the installation of software by users;	TBD	N/A	N/A
	"	b. Enforce software installation policies through automated methods; and	TBD	N/A	N/A
	"	c. Monitor policy compliance through automated methods at least weekly.	TBD	N/A	N/A
CM-12	Information Location	a. Identify and document the location of CJI and the specific system components on which the information is processed, and stored, or transmitted;	TBD	N/A	N/A
	"	b. Identify and document the users who have access to the system and system components where the information is processed and stored; and	TBD	N/A	N/A
	"	c. Document changes to the location (i.e., system or system components) where the information is processed and stored.	TBD	N/A	N/A
CM-12(1)	Information Location | Automated Tools to Support Information Location	Use automated tools to identify CJI on software and hardware system components to ensure controls are in place to protect organizational information and individual privacy.	TBD	N/A	N/A
CJIS Policy Area: Media Protection					
5.8: MP-1	Policy and Procedures	a. Develop, document, and disseminate to authorized individuals:	Agency	Agency is responsible for documenting and implementing policies regarding secure handling of media.	
	"	1. Agency-level media protection policy that:	Agency		
	"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and	Agency		
	"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Agency		
	"	2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;	Agency		
	"	b. Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policy and procedures; and	Agency		
	"	c. Review and update the current media protection:	Agency		
	"	1. Policy at least annually and following any security incidents involving digital and/or non-digital media; and	Agency		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	2. Procedures at least annually and following any security incidents involving digital and/or non-digital media.	Agency		
5.8: MP-2	Media Access	Restrict access to digital and non-digital media to authorized individuals.	Both	Agency is responsible for documenting and implementing policies regarding secure handling of media.	Genasys ensures digital media in Genasys Cloud Services is stored in physically secure and controlled locations.
~~5.8: MP-3~~	~~Media Marking~~	~~a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and~~			
	N/A~~"~~	~~b. Exempt digital and non-digital media containing CJI from marking if the media remain within physically secure locations and controlled areas.~~			
5.8: MP-4	Media Storage	a. Physically control and securely store digital and non-digital media within physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible; and	Both	Agency is responsible for documenting and implementing policies regarding secure storage of media.	Genasys maintains policies and practices for Genasys Cloud Services for securely handling media. Sensitive communications and data that traverse public networks are encrypted. Data is encrypted in transit over public networks using a robust TLS 1.2 implementation with 256 Bit Perfect Forward Secrecy.
	"	b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	Both		
5.8: MP-5	Media Transport	a. Protect and control digital and non-digital media to help prevent compromise of the data during transport outside of the physically secure locations or controlled areas using encryption, as defined in Section 5.10.1.2 of this Policy. Physical media will be protected at the same level as the information would be protected in electronic form. Restrict the activities associated with transport of electronic and physical media to authorized personnel;	Both	Agency is responsible for protecting any information from Genasys Cloud Services put into physical form in the same manner as in electronic form.	Genasys maintains policy and procedures for Genasys Cloud Services for the protection of any physical media during transport.
	"	b. Maintain accountability for system media during transport outside of the physically secure location or controlled areas;	Both		
	"	c. Document activities associated with the transport of system media; and	Both		
	"	d. Restrict the activities associated with the transport of system media to authorized personnel.	Both		
5.8: MP-6	Media Sanitization	a. Sanitize or destroy digital and non-digital media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration; and	Both	Agency is responsible for documenting and implementing policies regarding electronic media sanitization and disposal of data outside of Genasys Cloud Services.	Genasys maintains practices for sanitizing and disposing of electronic media. Including: . Data destruction and removal activities should be logged in an auditable format to ensure important devices are not missed. 2. The transfer of a workstation to a new owner requires full wiping of the previous owner's data.
	"	b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
					3. Data storage devices must be fully wiped or destroyed before disposal. Data destruction and wiping techniques must ensure that a determined attacker with moderate capabilities cannot recover the data.
5.8: MP-7	Media Use	a. Restrict the use of digital and non-digital media on agency-owned systems that have been approved for use in the storage, processing, or transmission of criminal justice information by using technical, physical, or administrative controls (examples below); and	Both	Agency is responsible for documenting and implementing policies regarding media use and the use of personally owned digital media devices.	Genasys maintains practices and policies for restricting the use of digital media in Genasys Cloud Services. Genasys employs strict technical, physical and administrative controls over access to any systems used in the storage, processing and transmission of media and prohibits any use of personal digital media devices.
	"	b. Prohibit the use of personally-owned digital media devices on all agency-owned or controlled systems that store, process, or transmit criminal justice information; and	Both		
	"	c. Prohibit the use of digital media devices on all agency-owned or controlled systems that store, process, or transmit criminal justice information when such devices have no identifiable owner.	Both		
CJIS Policy Area: Physical Protection					
5.9	Physical Protection	Physical protection policy and procedures **shall** be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.	Both	Agency is responsible for documenting and implementing policies regarding physical protection.	Genasys maintains policies and practices for Genasys Cloud Services related to physical protection.
5.9.1.1	Security Perimeter	The perimeter of physically secure location **shall** be prominently posted and separated from non-secure locations by physical controls.	Both	Agency is responsible for maintaining a secure physical perimeter.	Genasys defines and controls the physically secure perimeter for Genasys facilities.
	"	Security perimeters **shall** be defined, controlled and secured in a manner acceptable to the CSA or SIB.	Both		
5.9.1.2	Physical Access Authorizations	The agency **shall** develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or…	Both	Agency is responsible for restricting and controlling physical access to secure locations, as determined and managed by Agency, to support the use of Genasys Cloud Services.	Genasys ensures physical access to secure locations is limited to authorized personnel.
	"	...or **shall** issue credentials to authorized personnel.	Both		
5.9.1.3	Physical Access Control	The agency **shall** control all physical access points (except for those areas within the facility officially designated as publicly accessible) and…	Both	Agency is responsible for restricting and controlling physical access to physical access points.	Genasys regularly reviews the specific security practices and audit results documented by underlying infrastructure providers to ensure the highest standards are met. Genasys ensures physical access is limited to authorized personnel.
	"	...and **shall** verify individual access authorizations before granting access.	Both		
5.9.1.4	Access Control for Transmission Medium	The agency **shall** control physical access to information system distribution and transmission lines within the physically secure location.	Both	Agency is responsible for restricting and monitoring access to transmission lines within physically secure locations, as determined and managed by agencies, to support the use of Genasys Cloud Services.	Genasys restricts and monitors access to transmission lines within the physically secure locations used to deliver Genasys Cloud Services.

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
5.9.1.5	Access Control for Display Medium	The agency **shall** control physical access to information system devices that display CJI and…	Both	Agency should maintain policy and procedure surrounding the devices used to access Genasys Cloud Services.	Genasys maintains policy and procedure surrounding the devices used to administer Genasys Cloud Services.
	"	...and **shall** position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.	Both		
5.9.1.6	Monitoring Physical Access	The agency **shall** monitor physical access to the information system to detect and respond to physical security incidents.	Both	Agency is responsible for restricting and controlling physical access to locations managed by agencies to support the use of Genasys Cloud Services.	Genasys maintains policies and practices for monitoring physical access and responding to suspicious events.
5.9.1.7	Visitor Control	The agency **shall** control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible).	Both	Agency is responsible for restricting and controlling physical access. This includes monitoring and escorting visitors to physically secure locations as determined and managed by agencies to support the use of Genasys Cloud Services.	Genasys maintains policies and practices for controlling visitors to Genasys facilities. Visitors are identified with a unique badge only valid for the day of visit. In addition, the purpose of the visit is recorded with reception.
	"	The agency **shall** escort visitors at all times and monitor visitor activity.	Both		
5.9.1.8	Delivery and Removal	The agency **shall** authorize and control information system-related items entering and exiting the physically secure location.	Both	Agency is responsible for authorizing and monitoring information system related items entering and leaving physically secure locations, as determined and managed by agencies, to support the use of Genasys Cloud Services.	Genasys maintains policies and practices for controlling information-system-related items.
5.9.2	Controlled Area	If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency **shall** designate an area, a room, or a storage container, as a “controlled area” for the purpose of day-to-day CJI access or storage.	Both	Agency is responsible for documenting and implementing policies and practices related to physical protection.	Genasys maintains policies and practices for Genasys Cloud Services related to physical protection.
	"	The agency **shall**, at a minimum:			
	"	1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.	Both		
	"	2. Lock the area, room, or storage container when unattended.	Both		
	"	3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.	Both		
	"	4. Follow the encryption requirements found in section 5.10.1.1.2 for electronic storage (i.e. data “at rest”) of CJI.	Both		
CJIS Policy Area: Systems and Communications Protection and Information Integrity					
5.10.1	Information Flow Enforcement	The network infrastructure **shall** control the flow of information between interconnected systems.	Service Provider	N/A	Genasys requires encryption on all connections to Genasys Cloud Services over public networks. In addition, Genasys maintains a range of capabilities for controlling data flows in Cloud Services, including firewalls, ACLs, proxies, and load balancers.

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
5.10.1.1	Boundary Protection	The agency **shall**:		N/A	Genasys maintains controls to protect and monitor the boundaries of Genasys Cloud Services. These include firewalls, ACLs, network segmentation, proxies, and intrusion detection systems. Changes to computing resources are detected and monitored. An advanced anti-malware solution is deployed for malware protection on Genasys Cloud Services hosts and a host-based IDS/IPS solution is deployed. A web application firewall is deployed on each Genasys Cloud Services web servers. Additionally, vulnerability scans are performed on at least monthly basis, and penetration tests are performed regularly.
	"	1. Control access to networks processing CJI.	Service Provider		
	"	2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.	Service Provider		
	"	3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.10.4.4 for guidance on personal firewalls.	Service Provider		
	"	4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.	Service Provider		
	"	5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device “fails closed” vs. “fails open”).	Service Provider		
	"	6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host **shall** follow the guidance in section 5.10.3.2 to achieve separation.	Service Provider		
5.10.1.2.1	Encryption for CJI in Transit	When CJI is transmitted outside the boundary of the physically secure location, the data **shall** be immediately protected via encryption.	Service Provider	N/A	Data transmitted in Genasys Cloud Services is encrypted with 128 bits or stronger. Genasys's Cryptographic Module that provides for protection of data in transit is FIPS 140-2 validated: https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2878. Genasys maintains policies and practices for Genasys Cloud Services for encryption key and certificate management.
	"	When encryption is employed, the cryptographic module used **shall** be FIPS 140-2 certified and …	Service Provider		
	"	… and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.	Service Provider		
	"	2. Encryption **shall not** be required if the transmission medium meets all of the following requirements:			
	"	a. The agency owns, operates, manages, or protects the medium.	Agency		
	"	b. Medium terminates within physically secure locations at both ends with no interconnections between.	Agency		
	"	c. Physical access to the medium is controlled by the agency using the requirements in Section 5.9.1 and 5.12.	Agency		
	"	d. Protection includes safeguards (e.g. acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g. alarms, notifications) to permit its use for the tranmission of unencrypted information through an area of lesser classification or control.	Agency		
	"	e. With approval of the CSO.	Agency		
5.10.1.2.2	Encryption for CJI at Rest	When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data **shall** be protected via encryption.	Service Provider	N/A	Evidence data stored in Genasys Cloud Services is encrypted with AES 256. Genasys maintains policies and practices for Genasys Cloud Services for encryption key and certificate management.
	"	When encryption is employed, agencies **shall** either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or …	Service Provider		
	"	… or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.	Service Provider		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	1. When agencies implement encryption on CJI at rest, the passphrase to unlock the cipher **shall** meet the following requirements:			
	"	a. Be at least 10 characters	Service Provider		
	"	b. Not be a dictionary word	Service Provider		
	"	c. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character	Service Provider		
	"	d. Be changed when previously authorized personnel no longer require access	Service Provider		
	"	2. Multiple files maintained in the same unencrypted folder **shall** have separate and distinct passphrases.	Service Provider		
	"	2. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) **shall** be applied.	Service Provider		
5.10.1.2.3	Public Key Infrastructure (PKI) Technology	For agencies using public key infrastructure (PKI) technology, the agency **shall** develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.	Service Provider		Genasys uses PKI to provide server authentication to clients interacting with Genasys Cloud
	"	Registration to receive a public key certificate **shall**:			
	"	1. Include authorization by a supervisor or a responsible official.	Service Provider		
	"	2. Be accomplished by a secure process that verifies the identity of the certificate holder.	Service Provider		
	"	3. Ensure the certificate is issued to the intended party.	Service Provider		
5.10.1.3	Voice over Internet Protocol	In addition to the security controls described in this document, the following additional controls **shall** be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:		N/A	Not applicable to Genasys Cloud Services security practices. VOIP is not used within Genasys Cloud Services.
	"	1. Establish usage restrictions and implementation guidance for VoIP technologies.	Service Provider		
	"	2. Change the default administrative password on the IP phones and VoIP switches.	Service Provider		
	"	3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.	Service Provider		
5.10.1.4	Cloud Computing	The storage of CJI, regardless of encryption status, **shall** only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e. U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).	Service Provider	N/A	Genasys ensures that all CJI data and metadata in Genasys Cloud Services remains within the United States, including, without limitation, all backup data, replication sites, and disaster recovery sites. Metadata derived from any CJI data is protected in the same manner as CJI data within Genasys Cloud Services. Permitted use of stored CJI data and metadata is defined within
	"	Metadata derived from unencrypted CJI **shall** be protected in the same manner as CJI and…	Service Provider		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	...and **shall not** be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.	Service Provider		agreements between agencies and Genasys.
5.10.2	Facsimile Transmission of CJI	CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, **shall** meet the encryption requirements for CJI in transit as defined in Section 5.10.	Service Provider	N/A	Not applicable to Genasys Cloud Services security practices. Facsimile transmission is not used within Genasys Cloud Services.
5.10.3.1	Partitioning	The application, service, or information system **shall** separate user functionality (including user interface services) from information system management functionality.	Service Provider	N/A	Genasys Cloud Services uses many partitioning and segmentation methods for security purposes. These include network segmentation, OS separation, firewalls, and logical access separation.
	"	The application, service, or information system **shall** physically or logically separate user interface services (e.g. public Web pages) from information storage and management services (e.g. database management).	Service Provider		
5.10.3.2	Virtualization	In addition to the security controls described in this policy, the following additional controls **shall** be implemented in a virtual environment:		N/A	Genasys Cloud Services is deployed in a multi-tenant architecture, where customers leverage a shared application and underlying infrastructure. Customers are logically segmented within Genasys Cloud Services and cannot access other customers' data. Application security controls and session management controls within the application prevent a customer from accessing data not associated with their account or agency. Genasys leverages technologies and services provided by Infrastructure as a Service (IaaS) partners to deliver Genasys Cloud Services. Genasys deploys and manages virtualized servers on IaaS compute resources and leverages and manages additional IaaS services including object storage, networking, and resiliency capabilities.
	"	1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.	Service Provider		
	"	2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.	Service Provider		
	"	3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) **shall** be physically separate from Virtual Machines that process CJI internally or be separated by a virtual firewall.	Service Provider		
	"	4. Drivers that serve critical functions **shall** be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system - secured as independently as possible.	Service Provider		
	"	The following additional technical security controls **shall** be applied in virtual environments where CJI is comingled with non-CJI:			
	"	1. Encrypt CJI when stored in a virtualized environment where CJI is comingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.	Service Provider		
	"	2. Encrypt network traffic within the virtual environment.	Service Provider		
5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	The CJIS Audit Unit (CAU) **shall** conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies.	CJIS/CSO	Agency is required to schedule and execute audits of Genasys Cloud Services in compliance with the CJIS Security Policy.	Genasys is committed to undergoing formal audits with the FBI, state CSAs, or local agencies.
	"	This audit **shall** include a sample of CJAs and, in coordination with the SIB, the NCJAs.	CJIS/CSO		
	"	The FBI CJIS Division **shall** also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.	CJIS/CSO		
5.11.1.2	Triennial Security Audits by the FBI CJIS Division	This audit **shall** include a sample of CJAs and NCJAs.	CJIS/CSO	Agency is required to schedule and execute audits of Genasys Cloud Services in compliance with the CJIS	Genasys is committed to undergoing formal audits with the FBI, state CSAs, or local agencies.

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
				Security Policy.	
5.11.2	Audits by the CSA	Each CSA **shall**:		Agency is required to schedule and execute audits of Genasys Cloud Services in compliance with the CJIS Security Policy.	Genasys is committed to undergoing formal audits with the FBI, state CSAs, or local agencies.
	"	1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.	CJIS/CSO		
	"	2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.	CJIS/CSO		
	"	3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.	CJIS/CSO		
	"	4. Have the authority, on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.	CJIS/CSO		
5.11.3	Special Security Inquiries and Audits	All agencies having access to CJI **shall** permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations.	CJIS/CSO	Agency is required to schedule and execute audits of Genasys Cloud Services in compliance with the CJIS Security Policy.	Genasys is committed to undergoing formal audits with the FBI, state CSAs, or local agencies.
	"	The inspection team **shall** be appointed by the APB and…	CJIS/CSO		
	"	...and **shall** include at least one representative of the CJIS Division.	CJIS/CSO		
	"	All results of the inquiry and audit **shall** be reported to the APB with appropriate recommendations.	CJIS/CSO		
CJIS Policy Area: Personnel Security					
5.12.1	Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI	1. To verify identification, state of residency and national fingerprint-based record checks **shall** be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing).	Agency	Agency must address this control for users to whom they grant access to their instance of Genasys Cloud Services.	Genasys conducts national background checks for all employees. When necessary, Genasys employees that work on Genasys Cloud Services are available for a fingerprint-based national record check and state- level validations.
	"	However, if the person resides in a different state than that of the assigned agency, the agency **shall** conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances.	Agency		
	"	When appropriate, the screening **shall** be consistent with:	Agency		
	"	a. 5 CFR 731.106; and/or	Agency		
	"	b. Office of Personnel Management policy, regulations, and guidance; and/or	Agency		
	"	c. agency policy, regulations, and guidance.	Agency		
	"	2. All requests for access **shall** be made as specified by the CSO.	Agency		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	All CSO designees **shall** be from an authorized criminal justice agency.	Agency		
	"	3. If a record of any kind exists, access to CJI **shall not** be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.	Agency		
	"	a. If a felony conviction of any kind exists, the Interface Agency **shall** deny access to CJI. However, the Interface Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.	Agency		
	"	c. If a record of any kind is found on a contractor, the CGA **shall** be formally notified and system access shall be delayed pending review of the criminal history record information.	Agency		
	"	c. (cont) The CGA **shall** in turn notify the contractor's security officer.	Agency		
	"	4. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee **shall** review the matter to determine if access to CJI is appropriate.	Agency		
	"	5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI **shall** be determined by the CSO.	Agency		
	"	6. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access **shall** be denied and…	Agency		
	"	...and the person's appointing authority **shall** be notified in writing of the access denial.	Agency		
	"	7. The granting agency **shall** maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and...	Agency		
	"	...and **shall**, upon request, provide a current copy of the access list to the CSO.	Agency		
5.12.2	Personnel Termination	Upon termination of personnel by an interface agency, the agency **shall** immediately terminate access to local agency systems with access to CJI.	Both	Agency must address this control for users to whom they grant access to their instance of Genasys Cloud Services.	Genasys maintains policies and practices for access management related to termination or transfer of employees.
	"	Furthermore, the interface agency **shall** provide notification or other action to ensure access to state and other agency systems is terminated.	Both		
	"	If the employee is an employee of a NCJA or a Contractor, the employer **shall** notify all Interface Agencies that may be affected by the personnel change.	Both		
5.12.3	Personnel Transfer	The agency **shall** review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.	Both	Agency must address this control for users to whom they grant access to their instance of Genasys Cloud Services.	Genasys maintains policies and practices for access management related to termination or transfer of employees.
5.12.4	Personnel Sanctions	The agency **shall** employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.	Both	Agency must address this control for users to whom they grant access to their instance of Genasys Cloud	Genasys maintains a formal sanction process for employees failing to comply

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
				Services.	with established security policies and practices.
CJIS Policy Area: Mobile Devices					
5.13	Mobile Devices	The agency **shall**:		Agency must address this requirement through appropriate policies and procedures. Genasys Cloud Services provides many security features and capabilities to enable customers to securely manage digital evidence including device-level permission management (for example, allow specific users to use the web-based interface, but not the mobile application) and restrict access to defined IP ranges (limit access to approved office locations).	N/A
	"	(i) establish usage restrictions and implementation guidance for mobile devices;	Agency		
	"	(ii) authorize, monitor, control wireless access to the information system.	Agency		
5.13.1.1	802.11 Wireless Protocols	Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-80.11i protocols, do not meet the requirements for FIPS 140-2 and **shall not** be used.	Agency	Agency must address this requirement through appropriate policies and procedures.	N/A
	"	Agencies **shall** implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:			
	"	1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.	Agency		
	"	2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.	Agency		
	"	3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.	Agency		
	"	4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.	Agency		
	"	5. Enable user authentication and encryption mechanisms for the management interface of the AP.	Agency		
	"	6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with section 5.6.3.1.	Agency		
	"	7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.	Agency		
	"	8. Change the default service set identifier (SSID) in the APs.	Agency		
	"	Disable the broadcast SSID feature so that the client SSID must match that of the AP.	Agency		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.	Agency		
	"	9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features.	Agency		
	"	10. Ensure that encryption key sizes are at least 128-bits and…	Agency		
	"	...and the default shared keys are replaced by unique keys.	Agency		
	"	11. Ensure that the ad hoc mode has been disabled.	Agency		
	"	12. Disable all nonessential management protocols on the APs. Disable non-FIPS compliant secure access to the management interface.	Agency		
	"	13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.	Agency		
	"	14. Enable logging (if supported) and…	Agency		
	"	...and review the logs on a recurring basis per local policy.	Agency		
	"	At a minimum logs **shall** be reviewed monthly.	Agency		
	"	15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure.	Agency		
	"	16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.	Agency		
5.13.1.2.1	Cellular Service Abroad	When devices are authorized to access CJI outside the U.S., agencies **shall** perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency's policies prior to and after deployment outside of the U.S.	Agency	Agency must address this requirement through appropriate policies and procedures.	N/A
5.13.1.3	Bluetooth	Organizational security policy **shall** be used to dictate the use of Bluetooth and its associated devices based on the agency's operational and business processes.	Agency	Agency must address this requirement through appropriate policies and procedures.	N/A
5.13.1.4	Mobile Hotspots	When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they **shall** be configured:		Agency must address this requirement through appropriate policies and procedures.	N/A
	"	1. Enable encryption on the hotspot	Agency		
	"	2. Change the hotspot's default SSID	Agency		
	"	a. Ensure the hotspot SSID does not identify the device make/model or agency ownership	Agency		
	"	3. Create a wireless network password (Pre-shared key)	Agency		
	"	4. Enable the hotspot’s port filtering/blocking features if present	Agency		
	"	5. Only allow connections from agency controlled devices	Agency		
	"	OR 1. Have a MDM solution to provide the same security as identified in 1 - 5 above.	Agency		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
5.13.2	Mobile Device Management (MDM)	Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) **shall not** be used to process, store, or transmit CJI at any time.	Agency	Agency must address this requirement through appropriate policies and procedures.	N/A
	"	User agencies **shall** implement the following controls when directly accessing CJI from devices running limited feature operating system:			
	"	1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.	Agency		
	"	2. MDM with centralized administration configured and implemented to perform at least the following controls:	Agency		
	"	a. Remote locking of the device	Agency		
	"	b. Remote wiping of the device	Agency		
	"	c. Setting and locking device configuration	Agency		
	"	d. Detection of "rooted" and "jailbroken" devices	Agency		
	"	e. Enforcement of folder or disk level encryption	Agency		
	"	f. Application of mandatory policy settings on the device	Agency		
	"	g. Detection of unauthorized configurations	Agency		
	"	h. Detection of unauthorized software or applications	Agency		
	"	i. Ability to determine location of agency controlled devices	Agency		
	"	j. Prevention of unpatched devices from accessing CJI or CJI systems	Agency		
	"	k. Automatic device wiping after a specified number of failed access attempts	Agency		
5.13.3	Wireless Device Risk Mitigations	Organizations **shall**, as a minimum, ensure that wireless devices:		Agency must address this requirement through appropriate policies and procedures.	N/A
	"	1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.	Agency		
	"	2. Are configured for local device authentication (see Section 5.13.8.1).	Agency		
	"	3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.	Agency	Agency must address this requirement through appropriate policies and procedures	N/A
	"	4. Encrypt all CJI resident on the device.	Agency		
	"	5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.	Agency		
	"	6. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.	Agency		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	7. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.	Agency		
5.13.4.1	Patching/Updates	Agencies **shall** monitor mobile devices to ensure their patch and update state is current.	Agency	Agency must address this requirement through appropriate policies and procedures	N/A
5.13.4.2	Malicious Code Protection	Agencies that allow smartphones and tablets to access CJI **shall** have a process to approve the use of specific software or applications on the devices.	Agency	Agency must address this requirement through appropriate policies and procedures	N/A
5.13.4.3	Personal Firewall	A personal firewall **shall** be employed on all devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems).	Agency	Agency must address this requirement through appropriate policies and procedures	N/A
	"	At a minimum, the personal firewall **shall** perform the following activities:			
	"	1. Manage program access to the Internet.	Agency		
	"	2. Block unsolicited requests to connect to the PC.	Agency		
	"	3. Filter Incoming traffic by IP address or protocol.	Agency		
	"	4. Filter Incoming traffic by destination ports.	Agency		
	"	5. Maintain an IP traffic log.	Agency		
5.13.5	Incident Response	In addition to the requirements in Section 5.3 Incident Response, agencies **shall** develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios.	Agency	Agency must address this requirement through appropriate policies and procedures	N/A
	"	Special reporting procedures for mobile devices **shall** apply in any of the following situations:			
	"	1. Loss of device control. For example:	Agency		
	"	a. Device known to be locked, minimal duration of loss			
	"	b. Device lock state unknown, minimal duration of loss			
	"	c. Device lock state unknown, extended duration of loss			
	"	d. Device known to be unlocked, more than momentary duration of loss			
	"	2. Total loss of device	Agency		
	"	3. Device compromise	Agency		
	"	4. Device loss or compromise outside the United States	Agency		
5.13.6	Access Control	Access control (Section 5.5 Access Control) **shall** be accomplished by the application that accesses CJI.	Agency	Agency must address this requirement through appropriate policies and procedures	N/A
5.13.7.1	Local Device Authentication	When mobile devices are authorized for use in accessing CJI, local device authentication **shall** be used to unlock the device for use.	Agency		N/A

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	The authenticator used **shall** meet the requirements in section 5.6.2.1 Standard Authenticators.	Agency	Agency must address this requirement through appropriate policies and procedures	
5.13.7.2	Advanced Authentication	When accessing CJI from an authorized mobile device, advanced authentication **shall** be used by the authorized user unless the access to CJI is indirect as described in Section 5.6.2.2.1. If access in indirect, then AA is not required.	Agency	Agency must address this requirement through appropriate policies and procedures	N/A
5.13.7.2.1	Compensating Controls	Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) **shall** be implemented per Section 5.13.2.	Agency	Agency must address this requirement through appropriate policies and procedures	N/A
	"	The compensating controls **shall:**			
	"	1. Meet the intent of the CJIS Security Policy AA requirement	Agency		
	"	2. Provide a similar level of protection or security as the original AA requirement	Agency		
	"	3. Not rely upon the existing requirements for AA as compensating controls	Agency		
	"	4. Expire upon the CSO approved date or when a compliant AA solution is implemented.	Agency		
	"	The following minimum controls **shall** be implemented as a part of the CSO approved compensating controls:			
	"	Possession and registration of an agency-issued smartphone or tablet as an indication it is the authorized user	Agency		
	"	Use of device certificates as per Section 5.13.7.3 Device Certificates	Agency		
	"	Implemented CJIS Security Policy compliant standard authenticator protection on the secure location where CJI is stored	Agency		
5.13.7.3	Device Certificates	When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they **shall** be:		Agency must address this requirement through appropriate policies and procedures	N/A
	"	1. Protected against being extracted from the device	Agency		
	"	2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts	Agency		
	"	3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use	Agency		
CJIS Policy Area: System and Services Acquisition					
5.14: SA-22	Unsupported System Components	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or	Both	Agency is responsible for supporting and maintaining any devices that are used to access Genasys Cloud Services.	Genasys provides backwards compatibility for any altered or removed features.
	"	b. Provide the following option for alternative sources for continued support for unsupported components: original manufacturer support, or original contracted vendor support.	Both		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
CJIS Policy Area: System and Information Integrity					
5.15: SI-1	Policy and Procedures	a. Develop, document, and disseminate to all organizational personnel with system and information integrity responsibilities and information system owners:	Agency	Agency must address this requirement through appropriate policies and procedures	N/A
	"	1. Agency-level system and information integrity policy that:	Agency		
	"	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Agency		
	"	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Agency		
	"	2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;	Agency		
	"	b. Designate organizational personnel with system and information integrity responsibilities to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and	Agency		
	"	c. Review and update the current system and information integrity:	Agency		
	"	1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and	Agency		
	"	2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.	Agency		
5.15: SI-2	Flaw Remediation	a. Identify, report, and correct system flaws;	Service Provider	N/A	System flaws are logged, reported and corrected in accordance with the Genasys change management process.
	"	b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;	Service Provider		
	"	c. Install security-relevant software and firmware updates within the number of days listed after the release of the updates;	Service Provider		
	"	• Critical – 15 days	Service Provider		
	"	• High – 30 days	Service Provider		
	"	• Medium – 60 days	Service Provider		
	"	• Low – 90 days; and	Service Provider		
	"	d. Incorporate flaw remediation into the organizational configuration management process.	Service Provider		
	"	Determine if system components have applicable security-relevant software and firmware updates installed using vulnerability scanning tools as least quarterly or following any security incidents involving CJI or systems used to process, store, or transmit CJI.	Service Provider	N/A	Genasys uses a vulnerability management service that scans workloads for software vulnerabilities and unintended network exposure.
5.15: SI-3	Malicious Code Protection	a. Implement signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;	Service Provider	N/A	Genasys uses malware scanning and protection for instances and container workloads.

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;	Service Provider		
	"	c. Configure malicious code protection mechanisms to:			
	"	1. Perform periodic scans of the system at least daily and real-time scans of files from external sources at network entry and exit points and on all servers and endpoint devices as the files are downloaded, opened, or executed in accordance with organizational policy; and	Service Provider		
	"	2. Block or quarantine malicious code, take mitigating action(s), and when necessary, implement incident response procedures; and send alert to system/network administrators and/or organizational personnel with information security responsibilities in response to malicious code detection; and	Service Provider		
	"	d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Service Provider		
5.15: SI-4	System Monitoring	a. Monitor the system to detect:	Service Provider	N/A	Genasys Cloud Services are monitored in real-time for attacks, intrusions, and any other abnormal network activity. Genasys Cloud Services operate on AWS GovCloud where system level monitoring is managed. Learn more here
	"	1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives:	Service Provider		
	"	a. Intrusion detection and prevention	Service Provider		
	"	b. Malicious code protection	Service Provider		
	"	c. Vulnerability scanning	Service Provider		
	"	d. Audit record monitoring	Service Provider		
	"	e. Network monitoring	Service Provider		
	"	f. Firewall monitoring;	Service Provider		
	"	2. Unauthorized local, network, and remote connections;	Service Provider		
	"	b. Identify unauthorized use of the system through the following techniques and methods: event logging (ref. 5.4 Audit and Accountability);	Service Provider		
	"	c. Invoke internal monitoring capabilities or deploy monitoring devices:	Service Provider		
	"	1. Strategically within the system to collect organization-determined essential information; and	Service Provider		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	"	2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;	Service Provider		
	"	d. Analyze detected events and anomalies;	Service Provider		
	"	e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;	Service Provider		
	"	f. Obtain legal opinion regarding system monitoring activities; and	Service Provider		
	"	g. Provide intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring, and firewall monitoring software logs to organizational personnel with information security responsibilities weekly.	Service Provider		
5.15: SI-4 (2)	(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis	Employ automated tools and mechanisms to support near-real-time analysis of events.	Service Provider	N/A	Genasys Cloud Services operate on AWS GovCloud where system level monitoring is managed. Learn more here
5.15: SI-4 (4)	(4) System Monitoring | Inbound and Outbound Communications Traffic	a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;	Service Provider	N/A	Genasys Cloud Services operate on AWS GovCloud where system level monitoring is managed. Learn more here
	"	b. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions such as: the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information.	Service Provider		
5.15: SI-4 (5)	(5) System Monitoring | System-Generated Alerts	Alert organizational personnel with system monitoring responsibilities when the following system-generated indications of compromise or potential compromise occur: inappropriate or unusual activities with security or privacy implications.	Service Provider	N/A	Genasys Cloud Services are monitored in real-time for attacks, intrusions, and any other abnormal network activity.
5.12: SI-5	Security Alerts, Advisories, And Directives	a. Receive system security alerts, advisories, and directives from external source(s) (e.g., CISA, Multi-State Information Sharing & Analysis Center [MS-ISAC], U.S. Computer Emergency Readiness Team [USCERT], hardware/software providers, federal/state advisories, etc.) on an ongoing basis;	Service Provider		Genasys Cloud Services operate on AWS GovCloud where system level security addresses all U.S. government security requirements. Learn more here
	"	b. Generate internal security alerts, advisories, and directives as deemed necessary;	Service Provider		
	"	c. Issue security alerts, advisories, and directives to: organizational personnel implementing, operating, maintaining, and using the system; and	Service Provider		
	"	d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.	Service Provider		

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
5.15: SI-7	Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to software, firmware, and information systems that contain or process CJI; and	Service Provider	N/A	Genasys Cloud Services operate on AWS GovCloud where the firmware and operating system level services address all U.S. government security requirements. Learn more here
	"	b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: notify organizational personnel responsible for software, firmware, and/or information integrity and implement incident response procedures as appropriate.	Service Provider		
	(1) Software, Firmware, and Information Integrity | Integrity Checks	Perform an integrity check of software, firmware, and information systems that contain or process CJI at agency-defined transitional states or security relevant events at least weekly or in an automated fashion.	Service Provider		
	(7) Software, Firmware, And Information Integrity | Integration Of Detection and Response	Incorporate the detection of the following unauthorized changes into the organizational incident response capability: unauthorized changes to established configuration setting or the unauthorized elevation of system privileges.	Service Provider		
5.15: SI-8	Spam Protection	a. Employ spam protection mechanisms at system entry points to detect and act on unsolicited messages; and	Service Provider	N/A	N/A
	"	b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	Service Provider		
5.15: SI-8 (2)	(2) Spam Protection | Automatic Updates	Automatically update spam protection mechanisms at least daily.	Service Provider	N/A	N/A
5.15: SI-10	Information Input Validation	Check the validity of the following information inputs: all inputs to web/application servers, database servers, and any system or application input that might receive or process CJI.	Service Provider	N/A	Data inputs are sanitized and verified prior to insertion into a Genasys Cloud Services data store.
5.15: SI-11	Error Handling	a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and	Service Provider	N/A	Errors are logged with system and application-level information accessible by information security personnel only.
	"	b. Reveal error messages only to organizational personnel with information security responsibilities.	Service Provider		
5.15: SI-12	INFORMATION MANAGEMENT AND RETENTION	Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.	Service Provider	N/A	Data is retained within Genasys Cloud Services in accordance with the data retention policies of the Agency.
5.15: SI-16	(1) INFORMATION MANAGEMENT AND RETENTION | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	Limit personally identifiable information being processed in the information life cycle to the minimum PII necessary to achieve the purpose for which it is collected (see Section 4.3).	Service Provider	N/A	All data within Genasys Cloud Services is processed as if it is PII or CJI and follows the guidelines accordingly.

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details
	(2) INFORMATION MANAGEMENT AND RETENTION | MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: data obfuscation, randomization, anonymization, or use of synthetic data.	Service Provider	N/A	No production or live data from Genasys Cloud Services is used for research, testing or training.
	(3) INFORMATION MANAGEMENT AND RETENTION | INFORMATION DISPOSAL	Use the following techniques to dispose of, destroy, or erase information following the retention period: as defined in MP-6.	Service Provider	N/A	Data within Genasys Cloud Services is disposed of in accordance with the guidelines defined in section MP-6 after the retention period or upon written request by the Agency.
	MEMORY PROTECTION	Implement the following controls to protect the system memory from unauthorized code execution: data execution prevention and address space layout randomization.	Service Provider	N/A	Genasys Cloud Services are containerized and operate on up-to-date Linux operating systems with Nitro Enclave enabled.

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details

CJIS SECURITY POLICY 5.9.3: Genasys Evertel Cloud Services Compliance Details

Security Policy Appendix G.3 Cloud Computing

As stated in the CJIS Security Policy, the following questions can help frame the process of determining compliance (of a cloud provider) with the existing requirements of the CJIS Security Policy. The following outlines Genasys's response to the questions.

Appendix G.3 Questions	**Genasys Cloud Services Policies, Practices, and Standards**
Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)	Genasys maintains policies and practices for Genasys Cloud Services that limit remote access to only required individuals, via managed VPN connections requiring at least 2-factor authentication.
Will advanced authentication (AA) be required for access to CJI within a cloud environment? (5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale)	Genasys Cloud Services require at least 2-factor authentication for all system administration access. 2-factor authentication is available for individual customer accounts.
Does/do any cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9.1 Physically Secure Location)	Genasys regularly reviews the specific security practices and audit results documented by Infrastructure as a Service (IaaS) partners to ensure they meet the relevant portions of the CJIS Security Policy.
Are the encryption requirements being met? (5.10.1.2 Encryption) Who will be providing the encryption as required in the CJIS Security Policy (client or cloud service provider)? Note: individuals with access to the keys can decrypt the stored files and therefore have access to unencrypted CJI. Is the data encrypted while at rest and in transit?	Data transmitted and stored in Genasys Cloud Services is encrypted with 128 bits or stronger. FIPS 140-2 approved encryption ciphers (or stronger) are used, including AES 256, and RSA 2048. Genasys maintains policies and practices for Genasys Cloud Services for encryption key and certificate management.
What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response) Will the cloud subscriber be notified of any incident? If CJI is compromised, what are the notification and response procedures?	Genasys maintains comprehensive security incident response plans for Genasys Cloud Services including reporting to appropriate parties.
Is the cloud service provider a private contractor/vendor? If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI? (5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors)	Genasys acknowledges and abides by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is included by reference in the Genasys MSPA which contractually commits Genasys to the CJIS Security Policy requirements. CJIS Security Addendum Certification pages are maintained for each authorized Genasys employee and are available to customers. Genasys maintains policies and practices for ensuring all Genasys Cloud Services personnel are trustworthy and competent to handle sensitive data and systems. Authorized Genasys personnel are available for state of residence and national fingerprint-based record checks at either the state or local level.

Control Number	Title	Shall Statement / Requirement	SaaS Model Responsibility	Agency Details	Genasys Details

Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? Note: Cloud facilities such as datacenters in which CJI will be stored or processed should be audited as would any other datacenter housing and processing CJI.(5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)	Genasys adheres to the audit requirements of the FBI CJIS Security Policy.
How will event and content logging be handled? (5.4 Policy Area 4, Auditing and Accountability) Will the cloud service provider handle the events and content logging required by the CJIS Security Policy and provide that upon request? What are the cloud service provider's responsibilities with regard to media protection and destruction? (5.8 Policy Area 8: Media Protection)	Genasys Cloud Services systems are configured to log all required events from Policy Area 4, and more, to a central logging system.