Appendix A. Cloud Control Catalog

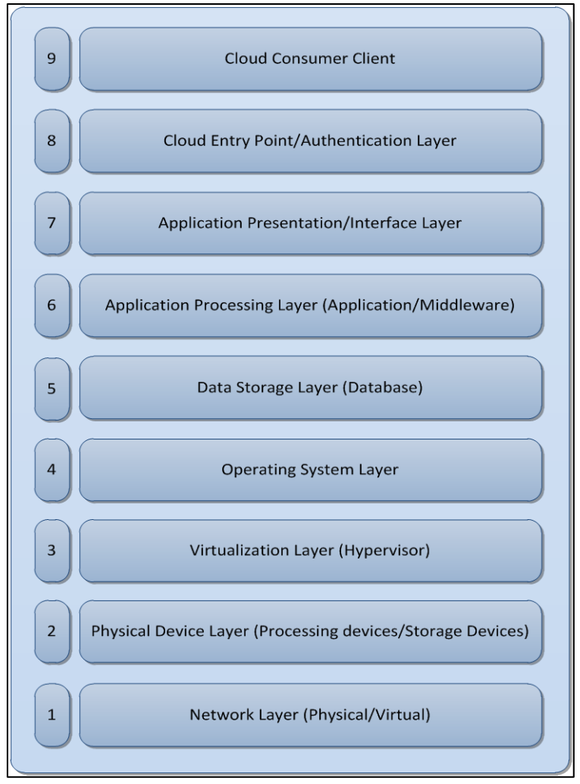
CJIS Control Catalog Instructions

The CJIS Control Catalog contains the security control requirements from the CJIS Security Policy and addendums to each control applicable to either the agency obtaining cloud computer services or the cloud computing provider. This catalog is utilized to conduct step 4.1 from the Cloud Deployment Evaluation Process and is based on the Cloud Infrastructure Evaluation Model (CIEM) described in the CJIS Security Policy Cloud Computing Addendum.

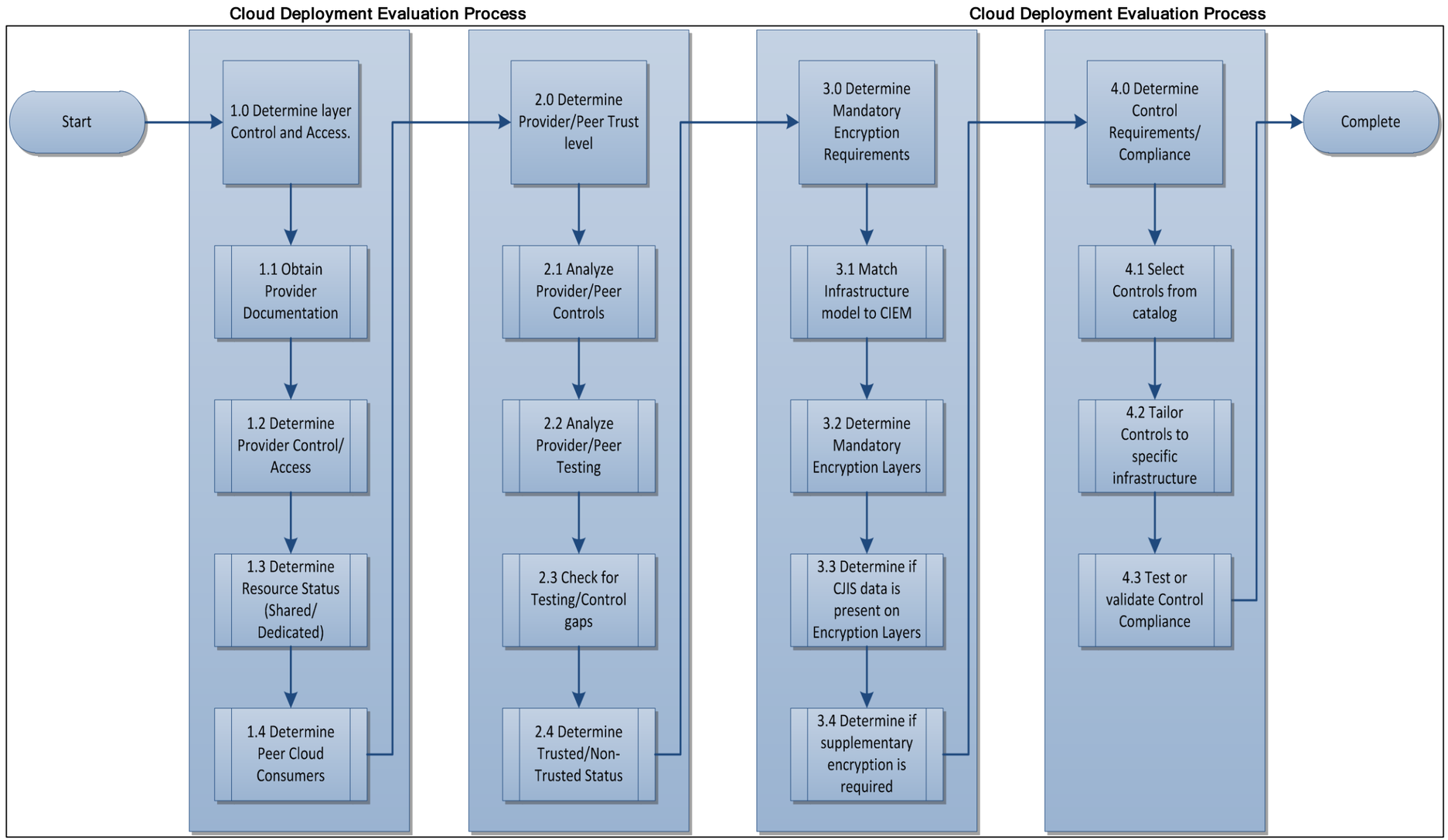
The catalog contains nine columns labeled L1-L9. These columns correspond to the layers of the CIEM. Security controls without specific layer entries in these columns are applied to the overall supported agency CJIS data structure, both inside and outside a cloud computing environment, and have no special requirements specific to cloud computing deployments. Columns containing a 'P' are mandatory controls that must be applied to identified layers if the layer is controlled or accesses by the cloud provider. The cloud provider can only be considered a 'Trusted' cloud provider for any particular layer if they meet all the mandatory controls for that layer. Layers marked with a 'C' will have the corresponding control applied by the CJIS Cloud Consumer for that layer if the Cloud Consumer has control of the layer. Controls marked 'PC' are mandatory for marked layers for whomever (Cloud Provider or Cloud Consumer) has control of that layer. In all cases, controls with mandatory layer markings must be explicitly addressed for each marked layer within the security documentation and testing of the overall system or application.

Cloud Infrastructure Evaluation Model (CIEM)

Cloud Infrastructure Evaluation Model (CIEM)



Appendix A. Cloud Control Catalog



Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.1	5.1	Policy Area 1: Information Exchange Agreements	The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.												
5.1	5.1.1	Information Exchange	Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI. Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. 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. Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements. There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. See Section 5.1.3 for secondary dissemination guidance.												

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.1	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. Using the requirements in this policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange. The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including – but not limited to - employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.												
5.1	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. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA or SIB Chief, each Interface Agency shall also allow the FBI to periodically test 2/09/2011 CJISD-ITS-DOC-08140-5.0 15 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. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.												

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.1	5.1.1.3	Criminal Justice Agency User Agreements	Any CJA receiving access to FBI CJIS data shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. 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. These agreements shall include: 1. Audit. 2. Dissemination. 3. Hit confirmation. 4. Logging. 5. Quality Assurance (QA). 6. Screening (Pre-Employment). 7. Security. 8. Timeliness. 9. Training. 10. Use of the system. 11. Validation.	P	P	P	P	P	P	P	P			Provider documentation and testing must cover all items listed and provide contractual or binding guarantee's that the provider will fulfill all requirements specified by the provider documentation	Same as control
5.1	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. Access shall be permitted when such designation is authorized pursuant to Executive Order, statute, regulation, or inter-agency agreement. 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. The MCA may be a separate document or included with the language of an inter-agency agreement. An example of an NCJA (government) is a city IT department.												

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.1	5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum	The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require. Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI. 1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible	P	P	P	P	P	P	P	P			The Cloud Provider must agree to the CJIS Cloud Provider Security Addendum for any CIEM layer in which they have control or access.	Same as control

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.1	5.1.1.6	Agency User Agreements	consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. An NCJA (public) receiving access to FBI CJIS data shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board. 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. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. An NCJA (private) receiving access to FBI CJIS data shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (private) is a local bank. All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see													
5.1	5.1.1.7	Security and Management Control Outsourcing Standard	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. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact Council Security and Management Control Outsourcing Standard. Each Channeled that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing. 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, and shall be subject to the same extent of audit review as are local user agencies.													

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.1	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. The CJA 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. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this policy.	PC	PC	PC	PC	PC	PC	PC	PC			The Cloud Provider must agree to utilize an incident reporting and response process consistent with the CJIS policy. The process must be provided with independent verification that the process is followed. Service monitoring of the Cloud Provider must adhere to the Service Level Agreements (SLA) specified in the Provider contract, and the SLA's will be reviewed under other sections of this policy for completeness and suitability	Same as control
5.1	5.1.2.1	Managing Changes to Service Providers	Any changes to services provided by a service provider shall be managed by the CJA. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change	PC	PC	PC	PC	PC	PC	PC	PC		All changes to services at CIEM layers under Agency control must comply with the standard policy requirements	Changes to CIEM layers on Cloud Provider control are not required to be reported unless the changes impact provider services to the supported agency.	
5.1	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.												
5.2	5.2	Policy Area 2: Security Awareness Training	Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI. The CSO/SIB may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.	PC	PC	PC	PC	PC	PC	PC	PC	PC		Provider documentation and testing must cover all items listed and provide contractual or binding guarantee's that the provider will fulfill all requirements specified by the provider documentation	Same as control
5.2	5.2.1	Awareness Topics	A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.												

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.2	5.2.1.1	All Personnel	At a minimum, the following topics shall be addressed as baseline security awareness training for all authorized personnel with access to CJI: 1. Rules that describe responsibilities and expected behavior with regard to CJI usage. 2. Implications of noncompliance. 3. Incident response (Points of contact; Individual actions). 4. Media protection. 5. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity. 6. Protect information subject to confidentiality concerns – hardcopy through destruction. 7. Proper handling and marking of CJI. 8. Threats, vulnerabilities, and risks associated with handling of CJI. 9. Dissemination and destruction.	PC	PC	PC	PC	PC	PC	PC	PC	C		Applicable to provider personnel involved with controlled or accessible layers only	Same as control

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.2	5.2.1.2	Personnel with Physical and Logical Access	In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI: 1. Rules that describe responsibilities and expected behavior with regard to information system usage. 2. Password usage and management—including creation, frequency of changes, and protection. 3. Protection from viruses, worms, Trojan horses, and other malicious code. 4. Unknown e-mail/attachments. 5. Web usage—allowed versus prohibited; monitoring of user activity. 6. Spam. 7. Social engineering. 8. Physical Security—increases in risks to systems and data. 9. Media Protection. 10. Handheld device security issues—address both physical and wireless security issues. 11. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance. 12. Laptop security—address both physical and information security issues. 13. Personally owned equipment and software—state whether allowed or not (e.g., copyrights). 14. Access control issues—address least privilege and separation of duties. 15. Individual accountability—explain what this means in the agency.	PC	PC	PC	PC	PC	PC	PC	PC	C		Applicable to provider personnel involved with controlled or accessible layers only	Same as control
5.2	5.2.1.3	Personnel with Information Technology Roles	In addition to 5.2.1.1 and 5.2.1.2 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.): 1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions. 2. Data backup and storage—centralized or decentralized approach. 3. Timely application of system patches—part of configuration management. 4. Access control measures. 5. Network infrastructure protection measures.	PC	PC	PC	PC	PC	PC	PC	PC	C		Applicable to provider personnel involved with controlled or accessible layers only	Same as control

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.2	5.2.2	Security Training Records	Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB/Compact Officer. Maintenance of training records can be delegated to the local level.	PC	PC	PC	PC	PC	PC	PC	PC	C		Provider testing should show maintenance of records for provider personnel	Same as control
5.3	5.3	Policy Area 3: Incident Response	There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile. Agencies shall: (i) establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities. There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile. Agencies shall: (i) establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities. ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of an	PC	PC	PC	PC	PC	PC	PC	PC	C	ISO's from the agency must maintain individual POC's with the Cloud Provider for Incident Response and are responsible to ensure all incidents at the agency or cloud provider layers are reported per the primary control requirement.	Provider document must show the existence and appropriate testing of an incident response process consistent with CJIS requirements for each layer where the provider has control or access	Same as control
5.3	5.3.1	Reporting Information Security Events	The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.	C	C	C	C	C	C	C	C	C	Reporting requirements from agencies will include cloud provider controlled layers		

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.3	5.3.1.1	Reporting Structure and Responsibilities													
5.3	5.3.1.1.1	FBI CJIS Division Responsibilities	The FBI CJIS Division shall: 1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC). 2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material. 3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed. 4. Disseminate prompt advisories of system threats and operating system vulnerabilities to all CSOs and ISOs through the use of the iso@leo.gov e-mail account, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips. 5. Track all reported incidents and/or trends. 6. Monitor the resolution of all incidents.												
5.3	5.3.1.1.2	CSA ISO Responsibilities	The CSA ISO shall: 1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response. 2. Identify individuals who are responsible for reporting incidents within their area of responsibility. 3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident. 4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected. 5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area. 6. Act as a single POC for their jurisdictional area for requesting incident response assistance.	PC	PC	PC	PC	PC	PC	PC	PC	C	Additionally, the CSA ISO shall manage the incident handling and reporting interface with the cloud provider, ensuring incidents involving provider controlled layers are reported using the same guidelines as agency controlled systems/layers.	The cloud provider must agree to report incidents occurring within provider controlled or accessed layers to the CSA ISO within binding contracts or SLA's	Same as control

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.3	5.3.2	Management of Information Security Incidents	A consistent and effective approach shall be applied to the management of information security incidents. Responsibilities and procedures shall be in place to handle information security events and weaknesses effectively once they have been reported.												
5.3	5.3.2.1	Incident Handling	The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly.	PC	PC	PC	PC	PC	PC	PC	PC	C	Agency incident handling capabilities will cover all agency controlled layers and include POC's and procedures for interfacing with the cloud provider for provider controlled layers.		
	5.3.2.1.1			P							P			Successful breaches of the provider boundary or internal network access controls must be reported at a minimum	
	5.3.2.1.2				P									Any physical access breach must be reported	Loss of control or inappropriate release of credentials having access to these layers must be reported.
	5.3.2.1.3					P	P	P	P	P				Any successful or attempted compromise of security containerization or segregation of shared resources by a Peer Cloud Consumer must be reported.	
5.3	5.3.2.2	Collection of Evidence	Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	PC	PC	PC	PC	PC	PC	PC	PC	C	The agency must maintain procedures and appropriate jurisdictions (e.g. potential physical locations) for the collection of evidence from the cloud provider in case of a security incident involving legal action	The cloud provider service agreements must allow the collection of evidence from provider controlled resources when the incident involves legal action. Digital evidence (e.g. logs) must be accessible in a non-proprietary format.	Provider access records must be accessible and provided if an incident involves legal action.

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.3	5.3.3	Incident Response Training	The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.	C	C	C	C	C	C	C	C	C	Agency training will include any special training required to manage incidents occurring within cloud provider controlled layers.		
5.3	5.3.4	Incident Monitoring	The agency shall track and document information system security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.	C	C	C	C	C	C	C	C	C	The agency incident monitoring will include tracking/monitoring of incidents reported by cloud providers		
5.4	5.4	Policy Area 4: Auditing and Accountability	Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components. Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.													

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.4	5.4.1	Auditable Events and Content (Information Systems)	The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems. The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.												
5.4	5.4.1.1	Events	The following events shall be logged: 1. Successful and unsuccessful system log-on attempts. 2. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource. 3. Successful and unsuccessful attempts to change account passwords. 4. Successful and unsuccessful actions by privileged accounts. 5. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.	PC	PC	PC	PC	PC	PC	PC	PC	C	Events must be recorded for every agency controlled layer within an agency controlled layer. Events recorded by the cloud provider on a cloud provider layer cannot constitute compliance with this requirement unless the event management/auditing system is accessible for agency or CJIS review of the audited events.	Provider audit records must cover the required events, as applicable to the layer technology, for all provider controlled layers. Audit records from a different provider controlled layer may be used to show compliance for any provider controlled layer as long as the events are adequately covered for that layer.	Audit records of provider access must be maintained for any layer to which the provider has access and provider access cannot be detected or audited by the supported agency.
	5.4.1.1.1			P							P			Audit records must address network devices, appliances and management software which controls the network and boundary.	
	5.4.1.1.2				P									Audit records must address physical access to the computing facilities for authorized personnel in addition to the visitor requirements identified in 5.9.1.7	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
	5.4.1.1.3					P	P	P	P	P				Audit records must show coverage of all applicable technologies within these layers.	
5.4	5.4.1.1.1	Content	The following content shall be included with every audited event: 1. Date and time of the event. 2. The component of the information system (e.g., software component, hardware component) where the event occurred. 3. Type of event. 4. User/subject identity. 5. Outcome (success or failure) of the event.	P	P	P	P	P	P	P	P			Content must be sufficient to fully identify the user/subject identity and originating node/layer. Full identification of the originating entity may require additional record content for some technologies.	
5.4	5.4.2	Response to Audit Processing Failures	The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.	P	P	P	P	P	P	P	P			Audit processing failures or loss of audit records for any provider controlled layer must be reported with the period of audit record failure of loss identified, regardless of cause.	
5.4	5.4.3	Audit Monitoring, Analysis, and Reporting	The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.	PC	PC	PC	PC	PC	PC	PC	PC	C	The agency is responsible for monitoring and analysis of audit records pertaining to any agency controlled layer, as well as any provider controlled layer for which the provider has granted access to audit records or logs. Provider access records for layers controlled by the agency must be verified with the provider to ensure access events generated by provider systems or personnel are valid.		The provider must agree to validate whether provider access events within agency controlled layers are valid access events

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.4	5.4.4	Time Stamps	The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.	PC	PC	PC	PC	PC	PC	PC	PC	C	Cloud infrastructure layers controlled by the agency must synchronize audit timestamp time sources with the same time sources utilized by the provider controlled portions of the infrastructure. Agency systems outside of the cloud infrastructure should use a root time source consistent with the time source used by the provider whenever practical. When a common time source with the cloud provider is not possible the agency must periodically compare timestamps generated from agency internal systems to cloud audit records to determine the typical variance. Timestamp comparison and correlation must also be included within the incident response processes when a common time source cannot be utilized between the agency and the cloud provider.	Providers must show the utilization of a common time source for audit information at all layers within the provider controlled infrastructure. If a common time source is not utilized, audit correlation capability must be demonstrated between non-common time source audit records.	
5.4	5.4.5	Protection of Audit Information	The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.	C	C	C	C	C	C	C	C	C	Audit records accessible to the agency from provider controlled layers must be periodically saved onto agency controlled layers for the appropriate retention period		
5.4	5.4.6	Audit Record Retention	The agency shall retain audit records for at least 365 days. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.	PC	PC	PC	PC	PC	PC	PC	PC	C			

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
	5.4.6.1					PC	PC	PC	PC	PC		C	Agency is responsible for retention on all agency controlled layers, and must ensure audit record retention occurs for all layers, regardless of control, on which unencrypted CJIS data exists. If provider policy does not include retention of audit records for the required period, the agency must obtain and retain the records prior to the provider deleting the records.	Provider must provide to the supported agency in non-proprietary digital format any audit records for the associated layers which will not be retained by the provider for the specified period.	Same as control
5.4	5.4.7	Logging NCIC and III Transactions	A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.												
5.5	5.5	Policy Area 5: Access Control	Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.												

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.5	5.5.1	Account Management	The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies. Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on: 1. Valid need-to-know/need-to-share that is determined by assigned official duties. 2. Satisfaction of all personnel security criteria. The agency responsible for account creation shall be notified when: 1. A user's information system usage or need-to-know or need-to-share changes. 2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.	PC	PC	PC	PC	PC	PC	PC	PC	C	The agency shall also validate access roles and accounts (if applicable to the technology) associated with any provider access granted to agency controlled levels. If provider access is not managed by the agency, the agency must maintain a list of access privileges held by the provider.		The provider must validate and document the security roles with access to any agency controlled layer, regardless of whether the access is managed or detectable by the supported agency on layers the agency controls.
5.5	5.5.2	Access Enforcement	The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers). Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.	PC	PC	PC	PC	PC	PC	PC	PC	C	Applied as applicable to the technologies within each layer. Access enforcement for one layer may be accomplished by another layer, either agency or provider controlled, if the access enforcement is technically sufficient to meet the control requirement. If access enforcement is applied from a provider controlled layer, the provider must otherwise meet the criteria as a 'Trusted' provider for the layer providing the access enforcement.	Access enforcement for all provider controlled layers must be documented for each technology present on that layer.	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.5	5.5.2.1	Least Privilege	The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know. Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.	PC	PC	PC	PC	PC	PC	PC	PC	C	If the provider cannot meet the log retention requirement for this control, the provider can still be compliant for the associated layer(s) if the agency obtains and maintains the logs in an accessible format for the required period	See agency addendum. Provider may still be considered compliant if all control requirements except the retention requirement are met AND the logs are provided to the supported agency in a non-proprietary and accessible digital format for retention beyond the provider retention period.	
5.5	5.5.2.2	System Access Control	Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to: 1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions. 2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.	PC	PC	PC	PC	PC	PC	PC	PC	C			
5.5	5.5.2.3	Access Control Criteria	Agencies shall control access to CJI based on one or more of the following: 1. Job assignment or function (i.e., the role) of the user seeking access. 2. Physical location. 3. Logical location. 4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside). 5. Time-of-day and day-of-week/month restrictions.	PC	PC	PC	PC	PC	PC	PC	PC	C			

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.5	5.5.2.4	Access Control Mechanisms	When setting up access controls, agencies shall use one or more of the following mechanisms: cryptography used is Federal Information Processing Standards (FIPS) 140-2 (as amended) compliant (see section 5.10.1.2 for encryption requirements). 4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency. 1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted. 2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices. 3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption	PC	PC	PC	PC	PC	PC	PC	PC	C	Access control mechanisms shall be applied to each controlled layer as appropriate to the technologies within each layer. Access control mechanisms may be inherited from provider controlled layers if the provider otherwise meets the criteria as 'Trusted' for the layer providing the access control mechanism.	Access control mechanisms must be explicitly identified and consistent with the primary control requirement for each provider controlled layer and technology within the layer in order for the provider to meet the 'Trusted' status requirement for this control.	
5.5	5.5.3	Unsuccessful Login Attempts	Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.	PC	PC	PC	PC	PC	PC	PC	PC	C			

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.5	5.5.4	System Use Notification	The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information: 1. The user is accessing a restricted information system. 2. System usage may be monitored, recorded, and subject to audit. 3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties. 4. Use of the system indicates consent to monitoring and recording. The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system. Privacy and security policies shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available and when				PC	PC	PC	PC	PC	C	Control must be met for all agency controlled layers which present a system or application logon to the user. Since cloud resources can be accessed from multiple locations, a system use notification on the user workstation/computer owned by the agency does not constitute compliance for this control. The cloud service/application logon or authentication interface must provide this capability.	The provider may be considered compliant with this control if equivalent agreements are in place with all internal provider employees with access or control privileges to the cloud infrastructure AND the initial authentication portal into the cloud infrastructure from external connections (e.g. internet) has an equivalent legal disclaimer covering items 2, 3, and 4 in the primary control requirements.	
5.5	5.5.5	Session Lock	The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of officer safety, devices that are: (1) part of a police vehicle; or (2) used to perform dispatch functions and located within a physically secure location, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.	P	P	P	PC	P	P	PC	PC	C	When technically feasible, administrative connections to identified agency controlled layers will terminate or lock after the period of inactivity identified in the primary control requirement. However, non-privileged access to the cloud infrastructure is not subject to this control as long as the agency controlled terminals used to access the cloud resources are compliant.	The provider may be considered compliant with this control if the provider internal workstations/computers used to administer or control the cloud infrastructure have equivalent controls placed upon them	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.5	5.5.6	Remote Access	The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet). The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access in the security plan for the information system.	PC	PC	PC	PC	PC	PC	PC	PC	C	Agency access to privileged functions within agency controlled layers is allowed for cloud based infrastructure. However, privileged function access must be tightly controlled and limited to only those users with a documented need.	The cloud provider shall document the remote access protections used to access the cloud infrastructure for both privileged and non-privileged access. If the documentation and testing for remote access methods and monitoring is deemed insufficiently secure, the provider will be considered 'Non-Trusted' for the all layers and mandatory encryption requirements for CJIS data at all infrastructure levels will be applied.	
5.5	5.5.6.1	Personally Owned Information Systems	A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).												
5.5	5.5.6.2	Publicly Accessible Computers	Utilizing publicly accessible computers to access, process, store or transmit CJI is prohibited. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.												

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.5	5.5.7	Wireless Access Restrictions	The agency shall: (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections–without requiring network or peripheral cabling. Examples of wireless technologies include, but are not limited to: 802.11x, cellular networks, Bluetooth, satellite and microwave. Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology, may require some additional security controls as described below.	P										This control will not normally apply, however, if the provider utilizes internal wireless access to the network infrastructure supporting the cloud infrastructure the network layer will automatically be considered a 'Non-Trusted Peer Cloud Consumer' shared resource and mandatory encryption requirements will apply to this layer unless the provider can show compliance with all of the 5.5.7, 5.5.7.1, 5.5.7.2, and/or 5.5.7.4	
5.5	5.5.7.1	All 802.11x Wireless Protocols	Agencies shall: 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. 2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices 3. Place APs in secured areas to prevent unauthorized physical access and user manipulation. 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. 5. Enable user authentication and encryption mechanisms for the management interface of the AP. 6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with section 5.6.2.1. 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. 8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services. 9. Enable all security features of the wireless product, including the cryptographic authentication,												

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.5	5.5.7.2	Legacy 802.11 Protocols	Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and are to be used only if additional security controls are employed. Agencies shall follow the guidelines below regarding wireless implementation and cases where the WEP and WPA security features are used to provide wireless security in conjunction with the CJIS required minimum encryption specifications. 1. Deploy media access control (MAC) access control lists (ACL); however, MAC ACLs do not represent a strong defense mechanism by themselves because they are transmitted in the clear from WLAN clients to APs so they can be captured easily. 2. Enable WEP/WPA. 3. Ensure the default shared keys are replaced by more secure unique keys. 4. Enable utilization of key-mapping keys rather than default keys so that sessions are unique when using WEP.												
5.5	5.5.7.3	Cellular	Cellular telephones, smart phones (i.e. Blackberry, iPhones, etc.), personal digital assistants (PDA), and “aircards” are examples of cellular handheld devices or devices that employ cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks. Cellular devices are at risk due to a multitude of threats and consequently pose a risk to the enterprise. Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include: 1. Loss, theft, or disposal. 2. Unauthorized access. 3. Malware. 4. Spam. 5. Electronic eavesdropping. 6. Electronic tracking (threat to security of data and safety of law enforcement officer). 7. Cloning (not as prevalent with later generation cellular technologies). 8. Server-resident data.												

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.5	5.5.7.3.1	Cellular Risk Mitigations	Organizations shall, at a minimum, ensure that cellular devices: 1. Apply available critical patches and upgrades to the operating system. 2. Are configured for local device authentication. 3. Use advanced authentication. 4. Encrypt all CJI resident on the device. 5. Erase cached information when session is terminated. 6. Employ personal firewalls. 7. Employ antivirus software.												
5.5	5.5.7.3.2	Voice Transmissions Over Cellular Devices	Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements when an officer determines there is an immediate need for the CJI to further an investigation or situations affecting the safety of an officer or the general public.												

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.5	5.5.7.4	Bluetooth	Bluetooth is an open standard for short-range radio frequency (RF) communication and is used primarily to establish wireless personal area networks (WPAN), commonly referred to as ad hoc networks or piconets. A piconet is composed of two or more Bluetooth devices in close physical proximity that operate on the same channel using the same frequency hopping sequence and can scale to include up to seven active slave devices and up to 255 inactive slave devices. Bluetooth voice and data transfer technology has been integrated into many types of business and consumer devices, including cellular phones, personal digital assistants (PDA), laptops, automobiles, printers, and headsets. Bluetooth does not provide end-to-end, audit, or non-repudiation security services. If such services are needed, they shall be provided through additional, higher-layer means in addition to the Bluetooth specification and 802.11 standards. The cryptographic algorithms employed by the Bluetooth standard are not FIPS approved. When communications require FIPS-approved cryptographic protection, this can be achieved by employing application-level FIPS-approved encryption over the native Bluetooth encryption. Agencies shall: 1. Provide users with a list of precautionary measures they should take to better protect handheld Bluetooth devices from theft. The organization and its employees should be responsible for its wireless technology components because theft of those components could lead to														
5.6	5.6	Policy Area 6: Identification and Authentication	The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.	PC	PC	PC	PC	PC	PC	PC	PC	C			

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.6	5.6.1	Identification Policy and Procedures	Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.	PC	PC	PC	PC	PC	PC	PC	PC	C			
5.6	5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges	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. Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. 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. Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.												

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.6	5.6.2	Authentication Policy and Procedures	Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI. Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.	PC	PC	PC	PC	PC	PC	PC	PC	C	Applicable to agency controlled layers which authenticate individual users. Authentication can be inherited for any layer from another agency or Trusted Cloud Provider layer. At least one layer in the agency controlled infrastructure must be identified as the primary provider authentication, however, authentication mechanisms can exist at any layer. Where they exist, they must remain compliant to the CJIS policy.	To qualify as a 'Trusted' provider for any layer which the provider retains control, the provider must show that individual users are authenticated on both operations cloud infrastructure components as well as the infrastructure management systems that control the cloud infrastructure. At least one layer in the provider controlled infrastructure must be identified as the primary provider authentication, however, authentication mechanisms can exist at any layer. Where they exist, they must remain compliant to the CJIS policy.	
5.6	5.6.2.1	Standard Authentication (Password)	Agencies shall follow the secure password attributes, below, to authenticate an individual's unique ID. Passwords shall: 1. Be a minimum length of eight (8) characters on all systems. 2. Not be a dictionary word or proper name. 3. Not be the same as the Userid. 4. Expire within a maximum of 90 calendar days. 5. Not be identical to the previous ten (10) passwords. 6. Not be transmitted in the clear outside the secure location. 7. Not be displayed when entered.	PC	PC	PC	PC	PC	PC	PC	PC	C	Applicable to all layers with authentication mechanisms	Applicable to all layers with authentication mechanisms	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.6	5.6.2.2	Advanced Authentication	Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based public key infrastructure (PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, or “Risk-based Authentication” that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.	PC	PC	PC	PC	PC	PC	PC	PC	C	Applicable to all layers with authentication mechanisms	Applicable to all layers with authentication mechanisms	
5.6	5.6.2.2.1	Advanced Authentication Policy and Rationale	The requirement to use or not use AA is dependent upon the physical, personnel and technical security controls associated with the user location. For example, AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10). Conversely, if the technical security controls have not been met AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions. INTERIM COMPLIANCE: 1. For interim compliance, users accessing CJI from devices associated with, and located within, a police vehicle are exempt from the AA requirement until September 30th 2013 if the information system being used has not been procured or upgraded anytime after September 30th, 2005. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with Section 5.9.1.3. 2. Internet Protocol Security (IPSec) does not meet the 2011 requirements for advanced authentication; however, agencies that have funded/implemented IPSec in order to meet the AA requirements of CJIS Security Policy v.4.5 may continue to utilize IPSec for AA until 2013. Examples: 	PC	PC	PC	PC	PC	PC	PC	PC	C	AA mechanisms shall be used to access cloud based services or application layers that allow access to unencrypted CJIS data. If AA mechanisms are not in place for cloud based resources, mandatory encryption of CJIS data within the cloud infrastructure must occur. Userid and password alone are not sufficient to provide authoritative authentication to cloud based resources accessible from the internet.		

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.6	5.6.2.2.2	Advanced Authentication Decision Tree	The following AA Decision Tree, coupled with figures 8 and 9 below, assist decision makers in determining whether or not AA is required. 1. Can request's originating location be determined physically? If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 2. a. The IP address is attributed to a physical structure; or b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure. If neither (a) or (b) above are true then the answer is "no". Skip to question number 4. 2. Does request originate from within a physically secure location (that is not a police vehicle) as described in section 5.9.1? If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 3. a. The IP address is attributed to a physically secure location; or b. If a mnemonic is used it is attributed to a specific device assigned to a specific physically secure location. If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required. 3. Are all required technical controls implemented at this location or at the controlling agency? If either (a) or (b) below are true the answer to the above question is "yes". Decision tree completed. AA requirement waived. a. Appropriate technical controls listed in sections	PC	PC	PC	PC	PC	PC	PC	PC	C	AA is mandatory for any cloud resource containing unencrypted CJIS data. However, if the cloud infrastructure is a dedicated, private resource only accessible via an encrypted Virtual Private Network (VPN) which uses AA (not directly accessible via the internet), then the service or application layer use of AA will be governed by this control.	Provider administrative access must meet the AA requirements for provider controlled layers which have access to unencrypted CJIS data. If the provider does not use AA mechanisms the provider will be considered 'Non-Trusted' for layers not utilizing AA.	Same as control
5.6	5.6.3	Identifier and Authenticator Management	The agency shall establish identifier and authenticator management processes	PC	PC	PC	PC	PC	PC	PC	PC	C	Applies to layers where technically applicable only.	Applies to layers where technically applicable only.	
5.6	5.6.3.1	Identifier Management	In order to manage user identifiers, agencies shall: 1. Uniquely identify each user. 2. Verify the identity of each user. 3. Receive authorization to issue a user identifier from an appropriate agency official. 4. Issue the user identifier to the intended party. 5. Disable the user identifier after a specified period of inactivity. 6. Archive user identifiers.	PC	PC	PC	PC	PC	PC	PC	PC	C	Applies to layers where technically applicable only.	Applies to layers where technically applicable only.	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.6	5.6.3.2	Authenticator Management	In order to manage information system authenticators, agencies shall: 1. Define initial authenticator content. 2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators. 3. Change default authenticators upon information system installation. 4. Change/refresh authenticators periodically. Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.	PC	PC	PC	PC	PC	PC	PC	PC	C	Applies to layers where technically applicable only.	Applies to layers where technically applicable only.	
5.6	5.6.4	Assertions	Identity providers can be leveraged to identify individuals and assert the individual's identity to a service or to a trusted broker who will in-turn assert the identity to a service. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be: 1. Digitally signed by a trusted entity (e.g., the identity provider). 2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion. Assertions generated by a verifier shall expire after 12 hours and shall not be accepted thereafter by the relying party.	PC	PC	PC	PC	PC	PC	PC	PC	C	Applies to layers where technically applicable only.	Applies to layers where technically applicable only.	
5.7	5.7	Policy Area 7: Configuration Management													

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.7	5.7.1	Access Restrictions for Changes	Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Section 5.5, Access Control, describes agency requirements for control of privileges and restrictions	PC	PC	PC	PC	PC	PC	PC	PC	C	Applies to each layer individually.	Applies to each layer individually.	
5.7	5.7.1.1	Least Functionality	The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.	PC	PC	PC	PC	PC	PC	PC	PC	C	Applies to each layer individually.	Applies to each layer individually.	
5.7	5.7.1.2	Network Diagram	The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams. The network topological drawing shall include the following: 1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point. 2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient. 3. “For Official Use Only” (FOUO) markings. 4. The agency name and date (day, month, and year) drawing was created or updated.	PC	PC	PC	PC	PC	PC	PC	PC	C	Applies to each agency controlled layer, however a single artifact depicting all layers is acceptable.	Applies to each provider controlled layer, however a single artifact depicting all layers is acceptable. FOUO markings are not required if the information is public.	
5.7	5.7.2	Security of Configuration Documentation	The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in section 5.5 Access Control.	PC	PC	PC	PC	PC	PC	PC	PC	C	Applicable to all agency controlled layers	Applicable to all provider controlled layers. Failure to provide complete documentation for any layer will automatically result in the provider being considered 'Non-Trusted' for that layer and mandatory CJIS data encryption requirements will apply.	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.8	5.8	Policy Area 8: Media Protection	Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.	P	P							C		For purposes of section 5.8, media will be considered any electronic copies of Cloud Consumer data anywhere held by the provider. This may include backup data, shadow copies, replication data, database transaction logs or any other electronic format which may contain recoverable information. The section 5.8 Media Protection controls will be applied to data files being 'moved' within the cloud infrastructure as well as any physical transport of devices or components that may contain recoverable information.	
5.8	5.8.1	Media Storage and Access	The agency shall securely store electronic and physical media within physically secure locations or controlled areas. The agency shall restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per section 5.10.1.2.	P	P							C		For purposes of section 5.8, media will be considered any electronic copies of Cloud Consumer data anywhere held by the provider. This may include backup data, shadow copies, replication data, database transaction logs or any other electronic format which may contain recoverable information. The section 5.8 Media Protection controls will be applied to data files being 'moved' within the cloud infrastructure as well as any physical transport of devices or components that may contain recoverable information.	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.8	5.8.2	Media Transport	The agency shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.	P	P							C		For purposes of section 5.8, media will be considered any electronic copies of Cloud Consumer data anywhere held by the provider. This may include backup data, shadow copies, replication data, database transaction logs or any other electronic format which may contain recoverable information. The section 5.8 Media Protection controls will be applied to data files being 'moved' within the cloud infrastructure as well as any physical transport of devices or components that may contain recoverable information.	
5.8	5.8.2.1	Electronic Media in Transit	“Electronic media” means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. Controls shall be in place to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in section 5.10.1.2 of this policy, is the optimal control during transport; however, if encryption of the data isn’t possible then each agency shall institute other controls to ensure the security of the data.	P	P							C		For purposes of section 5.8, media will be considered any electronic copies of Cloud Consumer data anywhere held by the provider. This may include backup data, shadow copies, replication data, database transaction logs or any other electronic format which may contain recoverable information. The section 5.8 Media Protection controls will be applied to data files being 'moved' within the cloud infrastructure as well as any physical transport of devices or components that may contain recoverable information.	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.8	5.8.2.2	Physical Media in Transit	The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.	P	P							C		For purposes of section 5.8, media will be considered any electronic copies of Cloud Consumer data anywhere held by the provider. This may include backup data, shadow copies, replication data, database transaction logs or any other electronic format which may contain recoverable information. The section 5.8 Media Protection controls will be applied to data files being 'moved' within the cloud infrastructure as well as any physical transport of devices or components that may contain recoverable information.	
5.8	5.8.3	Electronic Media Sanitization and Disposal	The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.	P	P							C		For purposes of section 5.8, media will be considered any electronic copies of Cloud Consumer data anywhere held by the provider. This may include backup data, shadow copies, replication data, database transaction logs or any other electronic format which may contain recoverable information. The section 5.8 Media Protection controls will be applied to data files being 'moved' within the cloud infrastructure as well as any physical transport of devices or components that may contain recoverable information.	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.8	5.8.4	Disposal of Physical Media	Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.	P	P							C		For purposes of section 5.8, media will be considered any electronic copies of Cloud Consumer data anywhere held by the provider. This may include backup data, shadow copies, replication data, database transaction logs or any other electronic format which may contain recoverable information. The section 5.8 Media Protection controls will be applied to data files being 'moved' within the cloud infrastructure as well as any physical transport of devices or components that may contain recoverable information.	
5.9	5.9	Policy Area 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.	P	P							C		All provider data centers and locations which house cloud infrastructure physical components and network components within the cloud infrastructure security boundary must comply will section 5.9 controls marked as applicable.	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
	5.9.0.1			P										Provider physical locations with special network access to the data centers must meet the section 5.9 controls marked as applicable to the provider. Special network access is defined as direct network access the bypasses the primary boundary defenses of the cloud infrastructure to provide administrative access to cloud infrastructure components. If physical protection is not met at locations with special network access the network layer will be considered 'Non-Trusted' and mandatory CJIS data encryption requirements will apply.	
5.9	5.9.1	Physically Secure Location	A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof. Sections 5.9.1.1 – 5.9.1.9 describe the physical controls required in order to be considered a physically secure location, while section 5.12 describes the minimum personnel security controls required for unescorted access to a physically secure location. For interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle shall be considered a physically secure location until September 30th 2013. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with section 5.9.1.3.	P	P							C			

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.9	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. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.	P	P							C			
5.9	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 shall issue credentials to authorized personnel.	P	P							C			
5.9	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 shall verify individual access authorizations before granting access.	P	P							C			
5.9	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.	P								C			
5.9	5.9.1.5	Access Control for Display Medium	The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.									C			
5.9	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.	P	P							C			
5.9	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). The agency shall escort visitors at all times and monitor visitor activity.	P	P							C			
5.9	5.9.1.8	Access Records	those areas officially designated as publicly accessible) that includes: 1. Name and agency of the visitor. 2. Signature of the visitor. 3. Form of identification. 4. Date of access. 5. Time of entry and departure. 6. Purpose of visit. 7. Name and agency of person visited. The visitor access records shall be maintained for a minimum of one year. Designated officials within the agency shall review the visitor access records frequently for accuracy and completeness.	P	P							C		Visitor agencies are not required on the provider visitor access records. However, sufficient information must be maintained to positively identify visitors to the facility.	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.9	5.9.1.9	Delivery and Removal	The agency shall authorize and control information system-related items entering and exiting the physically secure location.	P	P							C			
5.9	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. 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. 2. Lock the area, room, or storage container when unattended. 3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view. 4. Follow the encryption requirements found in section 5.10.1.2 for electronic storage (i.e. data “at rest”) of CJI.									C			
5.1	5.10	Policy Area 10: System and Communications Protection and Information Integrity	Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency’s virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the policy for protecting systems and communications infrastructures.	PC	PC	PC	PC	PC	PC	PC	PC	C	Section applies to technically appropriate components	Section applies to all technically appropriate components	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.1	5.10.1	Information Flow Enforcement	Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see section 5.5) are: 1. Prevent CJI from being transmitted unencrypted across the public network. 2. Block outside traffic that claims to be from within the agency. 3. Do not pass any web requests to the public network that are not from the internal web proxy. Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.	PC							P		Item 1 is agency responsibility	Items 2 and 3 are provider responsibility.	
5.1	5.10.1.1	Boundary Protection	The agency shall: 1. Control access to networks processing CJI. 2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. 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. 4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use. 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 shall “fail closed” vs. “fail open”). 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.								PC		All items must be addressed, but can be shared between the agency and the cloud provider based on the technical architecture and levels of control.	All items must be addressed, but can be shared between the agency and the cloud provider based on the technical architecture and levels of control.	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.1	5.10.1.2	Encryption	1. Encryption shall be a minimum of 128 bit. 2. When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption). EXCEPTIONS: See sections 5.5.7.3.2 and 5.10.2. 3. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption). 4. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards. Note 1: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete. Note 2: While FIPS 197 (Advanced Encryption Standard) certification is desirable, a FIPS 197 certification alone is insufficient as the certification is for the algorithm only vs. the FIPS 140-2 standard which certifies the packaging of an implementation. 5. For agencies using public key infrastructure 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. Registration to receive a public key certificate shall: 	PC	PC	PC	PC	PC	PC	PC	PC	C	Applies to all encryption unless a higher requirement has been levied. Refer to the mandatory encryption requirements table to determine CIEM layers where CJIS data must be encrypted.	Applies to all encryption unless a higher requirement has been levied. Refer to the mandatory encryption requirements table to determine CIEM layers where CJIS data must be encrypted.	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.1	5.10.1.3	Intrusion Detection Tools and Techniques	The agency shall implement network-based and/or host-based intrusion detection tools. The CSA/SIB shall, in addition: 1. Monitor inbound and outbound communications for unusual or unauthorized activities. 2. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort. 3. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.	PC			PC				PC		Intrusion Detection tools compliant with this control must exist at Layer 1, 3, 8, or a combination of the layers. If the agency maintains control of one or more of these layers, intrusion detection tools must be deployed by the agency on at least one layer. This will typically be the OS (layer 4) if applicable to the agency. If intrusion detection tools do not exist within in either a agency controlled or 'Trusted' provider controlled layer, this control requirement will be considered unmet and mandatory CJIS data encryption will be employed for the entire cloud infrastructure.	Intrusion Detection tools compliant with this control must exist at Layer 1, 3, 8, or a combination of the layers. If the provider maintains control of one or more of these layers, intrusion detection tools must be deployed by the provider on at least one layer. As long as intrusion detection tools are employed on at least one provider controlled layer and can show coverage of these three layers, the provider will be considered compliant for all layers they control.	
5.1	5.10.1.4	Voice Over Internet Protocol	Appropriate agency officials must explicitly authorize the use of Voice over Internet Protocol (VoIP). Agencies using the VoIP protocol shall: 1. Establish usage restrictions and implementation guidance for VoIP technologies. 2. Document, monitor and control the use of VoIP within the agency.												
5.1	5.10.2	Facsimile Transmission of CJI	CJI transmitted via facsimile is exempt from encryption requirements.												
5.1	5.10.3	Partitioning and Virtualization	As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.			PC							Applicable if agency has control of the virtualization layer.		

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.1	5.10.3.1	Partitioning	The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality. 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). Separation may be accomplished through the use of one or more of the following: 1. Different computers. 2. Different central processing units. 3. Different instances of the operating system. 4. Different network addresses. 5. Other methods approved by the FBI CJIS ISO.					PC	PC	PC					
5.1	5.10.3.2	Virtualization	Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this policy, the following additional controls shall be implemented in a virtual environment: 1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc. 2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment. 3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines that process CJI internally. 4. Device drivers that are "critical" shall be contained within a separate guest. The following are additional technical security control best practices and should be implemented wherever feasible: 1. Encrypt network traffic between the virtual machine and host. 2. Implement IDS and IPS monitoring within the virtual machine environment. 3. Virtually firewall each virtual machine from each other (or physically firewall each virtual machine from each other with an application layer firewall) and ensure that only allowed protocols will			PC								

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.1	5.10.4	System and Information Integrity Policy and Procedures													
5.1	5.10.4.1	Patch Management	components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws. The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as: 1. Testing of appropriate patches before installation. 2. Rollback capabilities when installing patches, updates, etc. 3. Automatic updates without individual user intervention. 4. Centralized patch management. Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.	PC	PC	PC	PC	PC	PC	PC	PC	C			
5.1	5.10.4.2	Malicious Code Protection	The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available). The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.				PC	PC	PC	PC	PC	C	Malicious code protection must exist for all identified layers, but multiple layers may use the same malicious code protection component when technically feasible.	Malicious code protection must exist for all identified layers, but multiple layers may use the same malicious code protection component when technically feasible.	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.1	5.10.4.3	Spam and Spyware Protection	The agency shall implement spam and spyware protection. The agency shall: 1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers). 2. Employ spyware protection at workstations, servers and/or mobile computing devices on the network. 3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this policy document.				PC				PC				
5.1	5.10.4.4	Personal Firewall	A personal firewall shall be employed on all devices that are mobile by design (i.e. laptops, handhelds, personal digital assistants, etc.). For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a computer, permitting or denying communications based on policy. At a minimum, the personal firewall shall perform the following activities: 1. Manage program access to the Internet. 2. Block unsolicited requests to connect to the PC. 3. Filter incoming traffic by IP address or protocol. 4. Filter incoming traffic by destination ports. 5. Maintain an IP traffic log.				C				PC		A firewall must exist at some layer of the model. If a 'Trusted' provider layer with firewall component does not exist, the primary control requirements will be applied to the system OS layer. If a firewall does not exist within an agency controlled or 'Trusted' provider controlled layer of cloud infrastructure the entire infrastructure will be considered 'Non-Trusted' and mandatory encryption requirements will be applied to the entire infrastructure.		
5.1	5.10.4.5	Security Alerts and Advisories	The agency shall: 1. Receive information system security alerts/advisories on a regular basis. 2. Issue alerts/advisories to appropriate personnel. 3. Document the types of actions to be taken in response to security alerts/advisories. 4. Take appropriate actions in response. 5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.												

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.1	5.10.4.6	Information Input Restrictions	The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only. Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.												
5.1	5.11	Policy Area 11: Formal Audits	Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.												
5.1	5.11.1	Audits by the FBI CJIS Division		PC	PC	PC	PC	PC	PC	PC	PC	C	Prior to contracting for cloud services, agencies are advised to determine the provider controlled layers for which the provider is willing or capable of providing security documentation and/or independent testing results. It is highly recommended that the documentation and independent test results be considered as a high value criteria when selecting a cloud provider. If insufficient provider documentation or independent testing is available, mandatory CJIS encryption requirements may significantly reduce the utility of the cloud service or application as well as potentially causing significant cost increases required to provide adequate security if the provider is not doing so with documentation and testing.	At the discretion of the FBI CJIS Division, audits of cloud providers may be conducted by physical or technical audits as would be conducted at any CSA OR via inspection of cloud provider documentation and testing conducted by an independent third party testing organization. The CJIS Division will analyze the provider documentation and any existing test results to determine whether the documentation and testing provides sufficient coverage and detail based on the provider architecture. Additionally, the CJIS Division will determine if any independent testing conducted on the provider infrastructure is sufficient to show provider compliance with CJIS policy. Any layers for which sufficient documentation or testing does not exist are automatically considered 'Non-Trusted' provider layers and mandatory CJIS	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.1	5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.	PC	PC	PC	PC	PC	PC	PC	PC	C	Applies to all controlled layers		
5.1	5.11.1.2	Triennial Security Audits by the FBI CJIS Division	The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.	PC	PC	PC	PC	PC	PC	PC	PC	C		All cloud provider contracts or service agreements must explicitly identify areas, technologies, or CIEM layers which the provider will allow external audits or provide for independent testing.	
5.1	5.11.2	Audits by the CSA	Each CSA shall: 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. 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. 3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.												
5.1	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. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.												

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.1	5.12	Policy Area 12: Personnel Security	Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.												
5.1	5.12.1	Personnel Security Policy and Procedures													
5.1	5.12.1.1	Minimum Screening Requirements for Individuals Requiring Access to CJI:	1. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI. When appropriate, the screening shall be consistent with: (i) 5 CFR 731.106; (ii) Office of Personnel Management policy, regulations, and guidance; and (iii) agency policy, regulations, and guidance. (See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.) Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check. 2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency. 3. If a felony conviction of any kind exists, the hiring authority in the Interface Agency shall deny access to CJI. However, the hiring authority 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. 4. If a record of any other 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.	PC	PC	PC	PC	PC	PC	PC	PC	C		For a cloud provider to be considered a 'Trusted' provider for any CIEM layer, the provider must be compliant with the Personnel security requirements for ALL personnel with access or administrative control of that layer.	

Appendix A. Cloud Control Catalog

Section	Control	Control Name	Control Requirement	L1	L2	L3	L4	L5	L6	L7	L8	L9	Agency Addendum	Provider Control Addendum	Provider Access Addendum
5.1	5.12.1.2	Personnel Screening for Contractors and Vendors	In addition to meeting the requirements in paragraph 5.12.1.1, contractors and vendors shall meet the following requirements: 1. Prior to granting access to CJI, the CGA on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record check. 2. If a record of any kind is found, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the Contractor-appointed Security Officer. 3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) shall review the matter. 4. A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified. 5. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants. 6. The CGA shall maintain a list of personnel who have been authorized access to CJI and shall, upon request, provide a current copy of the access list to											For a cloud provider to be considered a 'Trusted' provider for any CIEM layer, the provider must be compliant with the Personnel security requirements for ALL personnel with access or administrative control of that layer.	
5.1	5.12.2	Personnel Termination	The agency, upon termination of individual employment, shall immediately terminate access to CJI.	PC	PC	PC	PC	PC	PC	PC	PC	C		Access termination must be to infrastructure systems where unencrypted CJIS data may reside.	
5.1	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.	PC	PC	PC	PC	PC	PC	PC	PC	C		Access termination must be to infrastructure systems where unencrypted CJIS data may reside.	
5.1	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.	PC	PC	PC	PC	PC	PC	PC	PC	C		Access termination must be to infrastructure systems where unencrypted CJIS data may reside.	