TECHNICAL REPORT

Recommendations for Implementation of Cloud Computing Solutions

Federal Bureau of Investigation
Criminal Justice Information Services Division
1000 Custer Hollow Road
Clarksburg, WV, 26306

August 10, 2012

Recommendations for Implementation of Cloud Computing Solutions

Table of Contents

Executive Summary iii

1.0 Introduction 1

2.0 Description of the Issues 1

2.1 Transmission of Data 2

2.2 Storage of Data 3

2.3 Application Access and Service Layering 4

2.4 Emergency Access and Disaster Recovery 5

2.5 Retention and Backup 6

2.6 Legal 6

2.7 Access Authorizations, Authentication Methods, and Identity Management 7

2.8 Service Provider Viability and Structure 8

2.9 Audit and Monitoring Capabilities and Authorization 8

2.10 Cryptographic Key and Certificate Management 8

3.0 Analysis of the Issues 9

3.1 Transmission of Data 9

3.2 Storage 10

3.3 Application Access/Service 11

3.4 Emergency Access/Disaster Recovery 11

3.5 Retention/Backup Copies 11

3.6 Legal 12

3.7 Identity Management / Access Authorization / Authentication Methods 12

3.8 Provider viability and structure 12

3.9 Audit/Monitoring capability/authorization 12

3.10 Cryptographic key/Certificate Management 12

4.0 Technical and Operational Standards for Cloud Computing 14

4.1 Cloud Computing Trust Model Categorization 15

4.2 Trusted and Non-Trusted entities 19

4.3 Layer Control and Access 20

4.4 Evaluation and Impact of Shared Resources 20

4.5 Evaluation Criteria for Cloud Infrastructure Layers 21

5.0 Cloud Deployment Evaluation Process 24

6.0 CJIS Security Policy Recommended Changes 32

Appendix A: Cloud Control Catalog 56

Appendix B: Common Cloud Provider Infrastructure Examples 57

Appendix C: Definitions 63

Appendix D: References 64

Recommendations for Implementation of Cloud Computing Solutions

Executive Summary

This Technical Report provides recommendations for specific policies and procedures to be followed by Criminal Justice Information System (CJIS) community members implementing cloud computing solutions. These recommendations are based on the analysis and findings of a study conducted by the FBI Information Security Office and presented to the CJIS Advisory Policy Board on June 6, 2012 [The Security Policy as it relates to Cloud Computing].

Technical and Operational issues impacting the implementation of Cloud Computing Solutions were examined in the following areas:

- Transmission of Data
- Storage of Data
- Application Access and Service Layering
- Emergency Access and Disaster Recovery
- Retention and Backup
- Legal
- Access Authorization, Authentication methods, and Identity Management
- Service Provider Viability and Structure
- Audit and Monitoring Capabilities and Authorization
- Cryptographic Key and Certificate Management

Based on this analysis, a procedure was developed to enable Agencies and Organizations to evaluate their prospective Cloud Computing Solutions to ensure compliance with the CJIS Security Policy.

These recommendations are intended to provide a basis for crafting of specific policy language to be coordinated with, and approved by the CJIS Advisory Policy Board. Once approved, these provisions will be integrated into the CJIS Security Policy to provide a standard and systematic approach to implementing cloud computing solutions. The Technical and Operational Standards, and their associated evaluation criteria, serve as the framework for checklists and guidelines. These allow CJIS community members to confirm that their cloud computing initiatives are compliant with the security policy.

Recommendations for Implementation of Cloud Computing Solutions

1.0 Introduction

This Technical Report provides recommendations for specific policies and procedures to be followed by Criminal Justice Information System (CJIS) community members implementing cloud computing solutions. These recommendations are based on the analysis and findings of a study conducted by the FBI Information Security Office and presented to the CJIS Advisory Policy Board on June 6, 2012 [The Security Policy as it relates to Cloud Computing].

Cloud Computing has evolved to a mature state and offers distinct cost saving opportunities by consolidating and restructuring information technology services. The Federal government has developed policies and directives that mandate migration to cloud computing solutions as a means of reducing information technology infrastructure service costs. Departments and Agencies must ensure their information security and privacy requirements are met, given the risks posed by cloud computing solutions. Many state and local governments are seeking cloud solutions. These jurisdictions also recognize that certain categories of information must be protected, including Law Enforcement Sensitive and Personally Identifiable Information. Members of the Criminal Justice Information System (CJIS) community have agreed to comply with the standards developed and promulgated in the CJIS Security Policy. The current version of the policy, Version 5.0 dated 02/09/2011, does not specifically address the vagaries introduced by cloud computing solutions. No language in the current version specifically precludes using a cloud computing solution. The desired end state is for CJIS community members to be able to adopt cloud solutions, provided that prudent security measures are implemented.

The recommendations contained herein are intended to provide a basis for crafting of specific policy language to be coordinated with, and approved by the CJIS Advisory Policy Board. Once approved, these provisions will be integrated into the CJIS Security Policy to provide a standard and systematic approach to implementing cloud computing solutions. The Technical and Operational Standards, and their associated evaluation criteria, serve as the framework for checklists and guidelines. These allow CJIS community members to confirm that their cloud computing initiatives are compliant with the security policy.

2.0 Description of the Issues

There are a number of technical and operational issues that must be considered when evaluating potential cloud computing solutions. These include:

- Transmission of Data
- Storage of Data
- Application Access and Service Layering
- Emergency Access and Disaster Recovery
- Retention and Backup
- Legal
- Access Authorization, Authentication methods, and Identity Management
- Service Provider Viability and Structure
- Audit and Monitoring Capabilities and Authorization
- Cryptographic Key and Certificate Management

Each of these issues has impact across the entire spectrum of cloud computing services – Cloud Email, Cloud Storage, and Cloud Applications.

2.1 Transmission of Data

2.1.1 General: Cloud services inherently transmit customer data across uncontrolled internet connections that are susceptible to monitoring and interception. While most cloud based services utilize some form of encryption either via web-based communications (e.g. SSL or TLS over HTTPS) or through a proprietary client to server application, the effectiveness of the data transmission encryption may depend on a number of variables and the actual cryptographic algorithms and protocols may not meet the Federal Information Processing Standards (FIPS) encryption requirements. Cloud services utilizing proprietary transmission software may require FIPS 140-2 (or successor) validation in order to meet US Government standards, as individual evaluation of proprietary software interfaces for cryptographic implementation would likely not be feasible outside of the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP). Cloud services utilizing web based (e.g. HTTPS) encryption may require specific web browser usage and configuration to ensure only appropriate and approved cryptographic algorithms are employed.

2.1.2 HTTPS encryption: Actual cryptographic algorithms employed in any HTTPS (e.g. SSL, TLS) protected session using a web browser are determined during the initial session set up as a negotiation between the client web browser and the web server. Many, but not all, web browsers and web servers have a 'FIPS' mode of operation that can be configured and has been functionally validated through the NIST CMVP. To ensure proper encryption, appropriate web browser and web server configurations must be in place. Since Cloud services remove control of the web server component from the organization, only web browser settings are available to the organization to enforce appropriate encryption mechanisms. Browser-only configuration to enforce FIPS compliant cryptography often has unintended side-effects that may impact the function of other web site access or applications. This introduces a risk that users or administrators will intentionally or unintentionally bypass the encryption enforcement through the use of alternate browsers or improper web browser configuration. Strong encryption enforcement would typically be configured on the web server component within an organization by the server administrator during initial setup and would have limited to no impact on any other organizational system other than potentially restricting the web browser versions that are compatible. While a Cloud service provider may set appropriate server configurations as part of the service, this is an item that needs to be addressed with any potential provider.
HTTPS connections involve two separate cryptographic algorithms. The first is a key exchange algorithm that creates a session specific to be used by the transmission encryption algorithm for security the session traffic. Use of both algorithm types is governed by statutory and regulatory restrictions for Federal government use and both must be FIPS 140-2 (or successor) approved algorithm types and be implemented by a FIPS 140-2 validated product.

2.1.3 Cloud Email: Email transmission from within an organizational email system to recipients outside the organizational email system experience equivalent risks if the organizations email system is within the organizational protected enclave or a cloud email provider. Both internal

and cloud based email exits organizational control once sent to an external recipient and must be protected by recipient to recipient cryptography if the message contains non-public government information.
Cloud based email may have a higher risk pertaining to email sent within the organizational email system than a private email system. Risks associated with data storage (see Storage section) may also apply to internal email, as well as email at rest on the cloud provider systems. Email is an asynchronous service and is particularly susceptible to interception and tampering. While human users have a general expectation for rapid email delivery, short delays are common, and even delays of several hours will often go unnoticed between email sending and delivery. Use of a cloud service may increase the risk of malicious email tampering (change, deletion, or addition of email content) for email sent to recipients within an organization by organizational outsiders, but may reduce the risk from tampering by organizational insiders. The tampering risk for email sent external to the organization will be slightly elevated from the risks associated by using a private email system due the added complexity of the system and the potential for key system compromise within the cloud infrastructure by other cloud customers that could grant access to the cloud email infrastructure.

2.1.4 Cloud Storage: Transmission related risk for Cloud Applications is primarily related to in transit encryption mechanism as discussed in the general transmission section and the HTTPS encryptions section.

2.1.5 Cloud Applications: Transmission related risk for Cloud Applications is primarily related to in transit encryption mechanism as discussed in the general transmission section and the HTTPS encryptions section.

2.2 Storage of Data

2.2.1 General: Cloud services typically reside within a shared infrastructure with multiple customers' data residing on the same physical and logical storage media. This increases the risk of data spillage across logical (customer) boundaries either by intentional manipulation of the shared infrastructure by a malicious actor, or unintentional spillage due to administrator error in system configuration or data manipulation operations.
Cloud service providers may encrypt data at the logical or physical storage level to limit exposure of customer's data. Storage encryption issues are similar in nature to those described in the Transmission section.
Data that is logically or physically stored by the cloud service in an unencrypted format is susceptible to modification, deletion, and unauthorized disclosure. Stored data that is encrypted is still susceptible to unauthorized deletion.
The physical storage facilities may be in multiple mirrored locations with third or fourth party staff potentially having physical access. This may be partially mitigated due to a low likelihood that extended staff would have knowledge or appropriate logical access to specific customer's data.
Organizational data may be physically or logically moved periodically to ensure efficient operation of the cloud service as a whole based on overall utilization. This may impact the need for periodic reviews or the level of service monitoring required to ensure any data storage controls or limitations are enforced.

Physical and logical storage mechanisms for cloud service must be understood in order to evaluate their potential for compliance with existing government policy. This may be an issue with some providers as their storage mechanisms are considered highly proprietary and may include elements considered trade secrets.

2.2.2 Physical Storage locality: Due to the nature of cloud services, the specific physical location of data may be indeterminate from the customer perspective. For U.S government data, assurances and auditing that data is not stored, either in primary, backup, or a residual form, outside of the legal jurisdiction of the U.S. government. U.S. government data physically stored outside the jurisdiction of the United States may be subject to access or handling laws of the country in which it is physically stored. This could result access being granted to the data by a non-U.S. government or court.
A legal opinion may be required to determine the impact of physical data storage for local law enforcement that resides in a different legal jurisdiction. Specific laws or requirements in both the jurisdiction of the using law enforcement entity as well as in the jurisdiction where the physical storage resides could potentially complicate or cause unintended consequences regarding E-Discovery actions or access to computer forensic data (e.g. logs) during incident handling of any data breach or loss.

2.2.3 Applicability to different Cloud services: Data storage issues and risks apply to all cloud services. Individual services may store residual or ancillary data in different forms (e.g transaction logs, error logs, usage data, and temporary files) that may or may not contain elements of sensitive data. Each proposed or evaluated service would require a technology specific evaluation to determine applicable physical or logical storage that must be addressed.

2.3 Application Access and Service layering

2.3.1 General: Cloud services will typically consist of a number of technical 'layers' from the physical device, usually through a virtualization layer, and potentially multiple application layers (e.g. web interface layer, application processing layer, database layer, etc).
Sensitive government data may reside within each of these layers in some form that may be accessible to system administrators with responsibility for that particular layer. System administrators or logging sub-systems at each layer may have limited visibility into what access is granted or is occurring with different layers.
System administrators and maintainers may fall under different organizational sub-units of the cloud service provider or administrative and maintenance functions may be outsource to a third-party for particular functions.
System administrators and maintainers may be physically located in foreign countries and subject to governance/subpoena/legal action by that country. If sensitive U.S. Government data is accessible to those administrators, regardless of actual storage location, a local court could feasibly require them to access and provide the data to the local government. While this might not be supportable under international law, any complaints would likely have to be entered after the fact.
Multiple customers of the service provider may use shared resources within some layers of service provider infrastructure and this may be obscured intentionally or unintentionally by the service provider (e.g. a customer may request a dedicated web instance or storage location for

sensitive data, but the data may be accessible from a shared database resource) due to the complexity of the cloud services infrastructure.
Any resource layer shared by multiple customers may be susceptible to manipulation by a customer in order to gain access to all data stored on that layer data stored on layers above or below the comprised resource layer.
Data being actively processed within a resource layer (e.g. manipulated or changed and not simply transmitted) cannot be encrypted for protection within that resource layer. This potentially allows any user or administrator with access to that resource layer to gain access to the data, regardless of any encryption that may be applied at different resource layers.

2.3.2 Cloud Email: Access can be restricted to the email payload (body text and/or attachments) through the use of end-to-end encryption. However, email headers (addressing data), subject lines, and some email metadata could still be exposed at some application layers as this information is necessary for email processing. However, this would limit the cloud services ability to perform some recovery or protective (e.g. virus scan) services.
Unencrypted email would likely be accessible from multiple application, virtualization, and storage resource layers as plain text as email data is not stored or handled in a binary format in many email systems.
Email attachments may be encrypted separately from the email body text, and may be protected exclusive of the rest of the email message. Human factor considerations for the end-users may be an issue to ensure sensitive data about or from the attachment is not inadvertently placed in the email body with the assumption it is protected.

2.3.3 Cloud Storage: Cloud storage solutions may allow end-to-end encryption using user held cryptographic keys. This may preclude any portion of the stored files, with the exception of document titles and possibly document metadata to be fully secure at any resource layer. However, this would preclude the use of some services such as virus detection and potentially complicate disaster recovery.
Some cloud storage options may allow for end-to-end data encryption, but maintain backup copies of the encryption key to perform some system operations and data recovery at client request. In that case, the key escrow or storage mechanisms may require evaluation if that function is selected for use.

2.3.4 Cloud Applications: Any cloud application that performs data processing off the end-user client computer will have unencrypted data present on one or more of the applications resource layers.

2.4 Emergency Access and Disaster Recovery

2.4.1 General: Cloud service provider facilities may be affected by natural or man-made disasters that occur at a significant physical distance from the organizational customer base. However, service loss to local customers may still occur in the case of a local disaster that affects the local Internet Service Provider (ISP) that services the local customer's primary facility. Conversely, local disaster recovery may be enhanced through cloud services from an alternate facility using an alternate ISP. Continuity of Operations Plans or Disaster Recovery plans designed for local data services will likely need to be re-designed for cloud services.

Disaster recovery priorities for a cloud service provider may not be consistent with the customer availability requirements of law enforcement during large scale natural or man-made disasters. Non-local data storage that results in loss of access to local law enforcement data during large scale man-made disasters could critically impede the investigation or apprehension of threat actors responsible for the disaster. This may include targeted denial of service attacks against cloud service providers if it became public knowledge that law enforcement actions were dependent on the cloud provider.

2.4.2 Applicability to Cloud services: This section applies equally to any cloud based service. Applicability is dependent on the sensitivity and time criticality of the data to the law enforcement mission and the particular technological implementations of the service.

2.5 Retention and Backup

2.5.1 General: Government data, and especially law enforcement data, may be subject to specific retention requirements. Any cloud service provider agreement must be assessed to compliance to any retention requirements associated with the data that will be resident within the cloud service.
Backup systems may require decryption of certain data stores or data streams to function properly. These systems may or may not re-encrypt the data for storage within the backup system or within another storage location. If a different cryptographic system is used, it may also need to be evaluated for FIPS compliance separately from the primary cloud service
Backup data may be stored in a different physical location from the primary data store and be subject to the same physical storage locality issues as identified in the Storage section of this document.
Transaction logs, access logs, error logs, and other data sources with ancillary or residual data that may contain sensitive information may or may not be backed up. Additionally, this data may be backed up and stored using a different mechanism from the primary data. Retention of some ancillary data sources may be required in order to meet standards for forensic or investigative analysis of any data breach or compromise of law enforcement information.

2.5.2 Applicability to Cloud services: This section applies equally to any cloud based service. Applicability is dependent on the sensitivity and time criticality of the data to the law enforcement mission and the particular technological implementations of the service.

2.6 Legal

2.6.1 General: A legal opinion may be required on the applicability of the issues in this section based on particular technical implementations of cloud services.
Potential ‘Chain of custody’ issues may arise for data handled using cloud services if satisfactory access and tracking logs are not maintained at a high level of integrity assurance. Due to the high level of complexity in cloud services, and a generally low level of understanding of the technologies by the general populace, a sufficiently skilled attorney could potentially introduce confusion over proper handling at a jury trial. This is only likely to apply to certain data types at certain stages in their lifecycle but may be a concern in some cases.

Loss or compromise of certain data types governed by privacy regulations may trigger required government actions to contain the data loss or notify the affected public. Some required actions could be inconsistent with some cloud service provider general agreements.
Some E-discovery actions could require excessive expense when utilizing a cloud provider or their service interface may be incompatible with bulk search methods.
Data breach investigations or computer forensic actions to determine the source of sensitive information spillage may not be fully supported by the logging levels and operational data retained by the cloud service.

2.7 Access Authorizations, Authentication Methods, and Identity Management

2.7.1 General: Cloud services are typically based on the concept of a high level of accessibly to the service and stored information from any physical location. The identity management, access authorization, and authentication mechanisms used by the cloud service must enforce appropriate protections and utilize government approved cryptographic mechanisms.
The identity management and access authorization functions of a cloud service may either be managed directly by the cloud provider or delegated to one or more individuals from the customer organization who are given special access rights. If management is retained by the service provider, a robust mechanism for remotely validating the identity of individuals presenting themselves as from the customer organization must be in place to prevent successful social engineering attacks. This same structure must be in place for the authorized customer account managers if delegated to the customer.
Authentication mechanisms must be separately evaluated from standard service functions to ensure compliance with FIPS standards in the handling and transmission of user credentials, as well as the storage of user data within the account database.
Information within the account database of the service provider beyond the user credentials may constitute sensitive information as user data may provide all the information necessary to execute a spear-phishing attack on key individuals. Some cloud services may publish user data in formats or within the web service to enhance user search features, but may use mechanisms that are accessible by non-organizational users.
Cloud services may provide a limited ability to audit the roles and permissions assigned to all accounts within the customer's portion of the cloud service. Cloud service providers will typically not provide customers with information regarding administrative roles held by the service provider or third party service providers responsible for some elements of the cloud service.
Audit record retention, content, and availability may be limited with cloud services
Cloud service providers may not be able to enforce particular password rules or lifespan.
The combination of username and password alone is generally insufficient protection of sensitive information that is accessible from anywhere on the World Wide Web. Additional protections in the form of Internet Protocol address restrictions or multi-factor authentication mechanisms may not be available from many cloud service providers.

2.8 Service Provider Viability and Structure

2.8.1 General: General cloud provider agreements do not require the cloud provider to notify the cloud service users of provider internal changes. This could include changes to the internal

security services, or physical locations of data storage that would adversely affect the security posture for a government or law enforcement customer.
Commercial cloud service providers may re-organize or sell/buy business units to/from other companies. This may cause modification to existing cloud services or changes in the nationality of service administrators.
Upon discontinuation of cloud services (either by customer request, provider dissolution, or provider request) it may be impossible to verify that all ancillary or residual data has been properly sanitized from the provider infrastructure, even if the primary data is properly removed from the service.
Refresh or replacement of provider hardware or media may result in unintentional release of residual data in an recoverable format. The service provider would typically not notify customers of internal hardware or media changes that might result in decommissioning or disposal of devices that may contain customer data.

2.9 Audit and Monitoring Capabilities and Authorization

2.9.1 General: Most cloud service providers are not configured to support audits of their information handling and service configurations by customers or customer representatives. In most cases it may be impractical or impossible to validate provider assertions as to their internal storage, transmission, and management systems.

2.10 Cryptographic Key and Certificate Management

2.10.1 General: Cloud services secured by service provided cryptographic mechanisms will have cryptographic key generation and/or digital certificate management, distribution, revocation, and escrow capability. These functions may or may not meet the FIPS standards for creation, handling, and storage of cryptographic keys protecting sensitive government information.
Cloud service providers may use third party providers for some cryptographic key or public key infrastructure management. These third party providers may or may not be based in the United States or subject to U.S. government oversight, but may be subject to oversight from foreign governments.

3.0 Analysis of the Issues

3.1 Transmission of Data

3.1.1 General: Proper encryption of sensitive information in transit across uncontrolled network space (e.g. the internet) is critical to ensure confidentiality of data as well as to prevent inappropriate modification of data while in transit.
Federal government information must be protected by FIPS validated cryptography per executive branch directives and statutory requirements.
Cloud service components that handle sensitive Federal data must either natively encrypt the data in transit with a FIPS validated cryptographic suite, or the cloud service customer should pre-encrypt data prior to placing the data within the cloud service using approved cryptography in order to comply with regulatory and statutory requirements.

3.1.2 HTTPS encryption: Due to configuration requirements on both client and server components of an HTTPS web-based connection, HTTPS allowable cryptographic suites must be analyzed for any prospective cloud provider.
The most appropriate solution is to restrict acceptable cryptographic suites from the cloud service servers through cloud provider configurations. Appropriate provider agreements or Service Level Agreements (SLA) should explicitly identify that the cloud provider will restrict allowable cryptographic suites from the server components for the organizations service connection points. The SLA should also specify mutually agreeable methods to verify proper technical functions
If the cloud service will not inherently restrict allowable cryptographic suites, it may be possible to construct an acceptable alternative solution by configuring all user terminals authorized to access the cloud service to only utilize approved cryptographic suites. This may be impractical or impossible if connection is permitted to the cloud resource from a large base of client systems. This scheme would heavily rely on user training and proper user behavior to restrict access to only approved client systems which may be infeasible in many organizations. However, if the cloud provider has the technical capability to restrict client connections to a specific set of clients (e.g. via IP address or domain name restrictions) it may be possible to employ an acceptable solution, but validation of proper function may be difficult.

3.1.3 Cloud Email: The transmission of cloud based email from the client to the cloud service may be appropriately protected by an acceptable HTTPS encryption method. However, this would not properly protect transmission of an email with sensitive content within the cloud server (mailbox to mailbox) infrastructure, nor would it protect the sensitive information if sent to an external organization or entity. Analysis of internal transmission issues is documented in the ‘Storage’ section, as the internal transmission issues are the equivalent to the storage issues with respect to email services.

3.1.4 Cloud Storage: Transmission related risk for Cloud Applications is primarily related to in transit encryption mechanism as discussed in the general transmission section and the HTTPS encryptions section.

3.1.5 Cloud Applications: Transmission related risk for Cloud Applications is primarily related to in transit encryption mechanism as discussed in the general transmission section and the HTTPS encryptions section.

3.2 Storage

3.2.1 General: Due to the nature of cloud storage, end-to-end encryption from the organizationally controlled client using organizationally generated and controlled cryptographic keys would provide the best solution for protection of stored data.
Cloud storage that incorporates FIPS validated cryptographic suites may be acceptable for some data types, but significant SLA clauses must exist for management of cloud provider personnel and procedures involved with the creation, management, storage, and retrieval of cryptographic keys maintained by the provider to access data within the cloud storage.

3.2.2 Physical Storage locality: Due to potential jurisdictional issues or legally allowable access to data being granted by foreign countries, offshore storage locations of primary, ancillary, and residual law enforcement sensitive data would be unacceptable. Any cloud provider SLA must address this concern. Provider compliance with this requirement may be very difficult to verify for ancillary or residual data depending on the provider structure and technical mechanisms.

3.2.3 Cloud Email: This analysis section applies to cloud email concerns for transmission within the cloud infrastructure as well. Due to the nature of cloud email there are two primary concerns. First is the protection of any sensitive data within attachments, and second is the protection of any sensitive data within the email body text. Since cloud email transfers between email accounts on the cloud servers within a non-government controlled network space, encryption of any sensitive data within the email body or attachment prior to the email leaving the organizational client system is critical.
An acceptable solution for attachments can be achieved with any number of cryptographic products and appropriate user training/policy to ensure encryption prior to attaching any sensitive data to the email. In some cases, it may be possible to technically enforce attachment encryption, depending on the availability and organizational use of specific email client software to connect to the cloud service. However, solutions of this nature may be costly to maintain the client software required to operate them, and rely heavily on proper user behavior as it may be difficult to prevent user bypass of the protection mechanisms by technical means.
The most appropriate solution is client-to-client encryption of both email body text and payload data. This would require installation and maintenance of a client-based cryptographic system and cryptographic key creation and maintenance by the using organization. Technical mechanisms must be in place to ensure only approved client software from approved client computers is permitted to connect to the cloud service for initial generation of emails that contain sensitive data. This also requires the cloud service provider to support client access software that is capable of enforcing end-to-end encryption, and may require disabling the web interface to the cloud email service to prevent users bypassing the client software security features for convenience. In this scenario there is still a low level potential for information exposure through the email subject line which is often not encrypted by most end point solutions.

3.2.4 Cloud Storage: An end-to-end data encryption system would alleviate any cloud storage concerns if the cloud service interface can be configured to only accept files for storage from a client encrypted source.
Cloud storage systems where the service provider generates or holds keys in escrow for data recovery would not be acceptable without strict personnel and access permissions controls being applied to all provider personnel with access to the key store.

3.2.5 Cloud Applications: Cloud applications the process or manipulate data using processors within the cloud infrastructure cannot be fully encrypted using user provided keys. The cryptographic keys to access the stored application data would necessarily exist within the cloud infrastructure and would likely preclude true end-to-end encryption from organizationally controlled clients. This may include file or email views provided by the cloud service.

3.3 Application access/Service

3.3.1 General: Due to the highly complex and potentially fluid nature of cloud infrastructures, any infrastructure shared between multiple customers would likely require client end-to-end encryption methods to ensure there is no exposure of sensitive data to disclosure or modification. If the cloud provider can guarantee separate infrastructure, either physically, or through cryptographic separation at all service and application layers, the solution might be acceptable for processing of sensitive data. However, for physical segregation, the SLA must address the personnel security and access concerns to the same degree as would be applied to any contract provider given access to sensitive data. For cryptographic segregation, personnel security and access concerns could be limited to the provider staff with access to the cryptographic key material.
Ancillary and residual data must be protected in an equivalent manner. This may be difficult to accomplish depending on the provider infrastructure.

3.4 Emergency Access/Disaster Recovery

3.4.1 General: Emergency access to data and Disaster Recovery plans for the provider should be explicitly defined in the SLA. The SLA must include clear definition of priorities for restoration of provider services and the support priorities given the government cloud services in specific disaster scenarios to include large scale man-made disaster scenarios.

3.5 Retention/backup copies

3.5.1 General: Provider documentation and SLA's must specifically address the data content and types of ancillary or residual data that may exist and detail the provider handling procedures for all data types.
SLA's must specifically identify data retention periods for primary, ancillary, and residual data sources
Backup, ancillary, and residual data must conform to the same physical and cryptographic storage requirements as primary data.

3.6 Legal

3.6.1 General: SLA's should specifically identify procedures and responsibility distribution between cloud provider and the government organization for activities related to privacy data or sensitive data breaches, to include investigation and the clean-up of sensitive data involved in a spillage.
Cloud services utilized for data that may be subject to e-discovery proceedings should have clearly defined SLA clauses covering retention periods of data, timeline to conduct actions, acceptable data formats, and pre-defined expenses for e-discovery actions.
SLA's must define the level of access and methods for access to provider log data and services needed to conduct computer forensic investigation into any loss or breach of sensitive data.

3.7 Identity Management / Access authorization / Authentication Methods

3.7.1 General: SLA's and contractual agreements should explicitly specify roles and responsibilities between the service provider and government customer regarding Identity Management and Access Authorization.
Cloud provider personnel with the technical capability and access to modify the service account database or access lists should undergo personnel screening commensurate with the most sensitive data that exists in an unencrypted format within that service.

3.8 Provider viability and structure

3.8.1 General: SLA's should clearly identify service provider policy regarding the issues from this section. Contractual agreements should explicitly specify timelines and allowable service changes in the event of ownership transfer of the provider.
Discontinuation of cloud services will remain a risk. It is likely infeasible to fully guarantee access to and validation of ancillary and residual data destruction if the cloud service provider discontinues services. The SLA's and contractual agreements should specific the intended actions, and only financially sound providers should be considered.
SLAs or contractual agreements should specify service provider responsibilities on the sanitization of data from media and retired devices.

3.9 Audit/Monitoring capability/authorization

3.9.1 General: SLAs must specify the specific audit authority provided to the government or government representatives with regards to access during an audit of the provider security controls. Audit access should cover the aspects of the implementation required to ensure client end-to-end security of sensitive data, and may include systems processing ancillary or residual data sources to ensure provider SLAs are being met.

3.10 Cryptographic key/Certificate Management

3.10.1 General:

Recommendations for Implementation of Cloud Computing Solutions

The most effective risk reduction mechanism regarding cryptographic keys or digital certificate management is to generate, distribute, maintain, and revoke all keys and certificates using organizationally controlled key management systems.
The use of a third party (either governmental or non-governmental) public key infrastructure provider may be acceptable in some circumstances for creation and management of public key certificates, but not for shared or private key creation and management.
Use of cloud service provided cryptographic services would require the service provider personnel with access to the keys to undergo personnel security checks commensurate with the sensitivity of the data protected by the provider cryptographic keys.

4.0 Technical and Operational Standards for Cloud Computing

Cloud Computing operations require the same security controls applied to any other system processing, displaying, transporting, or storing Criminal Justice Data. Due to the variance in technical and operational structures in existence between various Cloud Providers, it can be difficult to determine the extent of control exercised by the Cloud Provider and Cloud Consumer at the different layers of the cloud infrastructure. In order to evaluate the security requirements for any particular cloud service implementation, the specific trust model for the cloud implementation must be determined. Figure 4.1 shows the Cloud Infrastructure Evaluation Model (CIEM) used to evaluating cloud infrastructures for CJIS data with 9 technical layers. Not all of the layers shown will exist within every Cloud Provider infrastructure, but for each layer, the scope of control and presence must be determined for the primary Cloud Provider, supplementary service providers, and Peer Cloud Consumers. Cloud Providers and Peer Consumers may further be classified as trusted or non-trusted entities. The trust model categorization for a particular cloud implementation will define the specific security controls that must be applied to the cloud implementation in order for the implementation to meet CJIS standards. Control or access to the 9 layers shown in the figure may rest with either the Cloud Provider, the CJIS Cloud Consumer, or may be shared between the two. Additionally, access to certain layers may be shared among multiple Cloud Consumers (e.g. Network Layer traffic). Shared access layers of the model must be identified in order to determine the specific security requirements for that layer to meet CJIS standards.

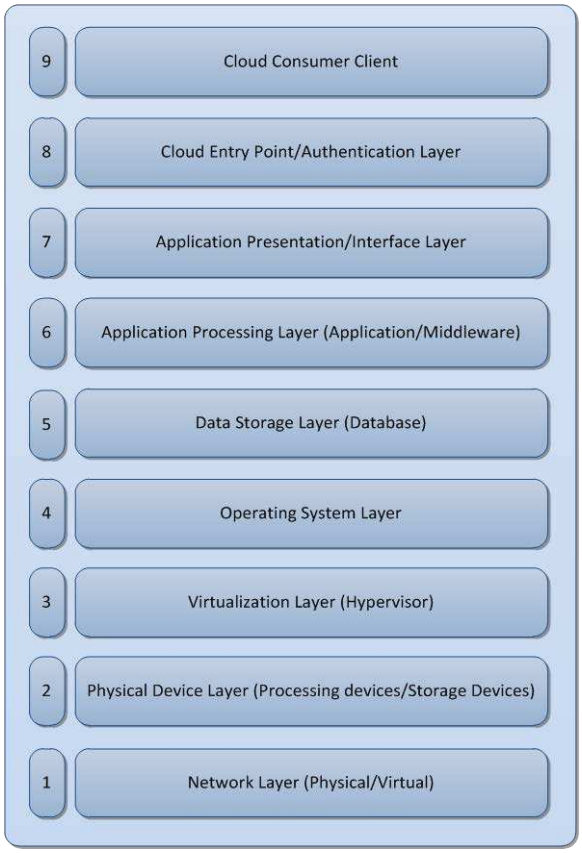

Figure 4.1 CJIS Cloud Infrastructure Evaluation Model

Recommendations for Implementation of Cloud Computing Solutions

4.1 Cloud Computing Trust Model Categorization

4.1.1 Network Layer

The network layer of the model consists of the devices and infrastructure, either physical, virtual or both that form the network data transport layer of the infrastructure. This includes all switches, routers, bridges, network load balancers, or other devices that operate primarily at layer 3or below of the Open System Interconnection (OSI) model. The primary function of this layer is the transport and management of communications traffic between physical or logical network nodes. The network layer may be presented to the Cloud Consumer as either a physical infrastructure or a software virtualized network. If presented as a physical infrastructure, the network may be considered either a shared or private resource depending on the provider implementation and trust level. If a virtual network is implemented within layer 3 of the model (virtualization layer) vice within dedicated network devices, the Cloud Provider trust level will be determined by the layer 3 trust level while the shared resource determination will be based on the layer 1 criteria in this section.

This layer includes the physical and logical protections applied to the Cloud Provider network infrastructure, to include any network segment within the Cloud Provider infrastructure over which Cloud Consumer traffic may pass that is not within the direct control of the Cloud Provider. (NOTE: The Consumer to Provider interface, if 'Internet' based, is not necessarily considered part of the Cloud Provider infrastructure. An example of a non-Provider controlled network segment that is within the Provider infrastructure would be an internet or dedicated third party connection between two Cloud Provider physical facilities.)

NOTE: Control of this layer is typically reserved by the Cloud Provider exclusively, but Access to this layer may be granted to Cloud Consumers in some models.

4.1.2 Physical Device Layer

The Physical Device Layer consists of all physical computing devices whose primary function is to support application processing or data storage. This CIEM layer includes standard, general purpose computing platforms as well as any dedicated appliance or specialized device used to either perform processing or storage of data. This layer specifically includes specialized storage systems (e.g. large disk array appliances) and any other physical devices not explicitly included within CIEM layers.

This CIEM layer also includes the physical protections provided by the Cloud Provider over all physical devices, excluding devices whose physical protection is explicitly covered by the Network (layer 1) layer of the CIEM.

NOTE: This layer will typically be a Shared Resource layer in most provider infrastructure models; however, some providers may offer premiums solutions to permit dedicated hardware at this layer.

NOTE: Control and access of this layer is typically reserved by the Cloud Provider exclusively, but both control and access to dedicated physical devices may be allowed as a premium service by some providers to Cloud Consumers

4.1.3 Virtualization Layer

The Virtualization Layer of CIEM consists of the virtualization software or other software component used to abstract the Operating System layer from the Physical Device layer resources. Most Cloud Provider implementations will utilize some form of commercial or custom virtualization software suite consisting of a 'Hypervisor' that manages access and separation functions between the Physical Device and Operating System layers as well as a management software component that executes on dedicated systems to control overall infrastructure resources and may control the Physical Device to Operating System mappings.

NOTE: Control and access of this layer is typically reserved by the Cloud Provider exclusively, but both control and access to dedicated physical devices may be allowed as a premium service by some providers.

NOTE: This layer will typically be a Shared Resource layer in most infrastructure models; however, some providers may offer premiums solutions to a dedicated virtualization layer. This will only occur when dedicated hardware has been reserved by the Cloud Consumer as a premium service.

4.1.4 Operating System Layer

The Operating System (OS) layer of the CIEM consists of the basic Operating System instance upon which services and applications are executed. The OS layer may consist of a single OS or a cluster/grouping of multiple OS's which provide application or service platforms. Some providers retain full control of the OS layer, while others offer full control to the Cloud Consumer. Numerous options for shared control/access of the OS layer exist with different providers.

This layer includes the storage mechanism and controls associated with the OS file system and persistent file storage that is presented by the Virtualization layer to the OS instance as being part of the physical machine upon which the OS is executing.

4.1.5 Data Storage Layer

The Data Storage Layer of the CIEM consists of the provider infrastructure components, systems, and services that provide structured or unstructured data storage exclusive of the file storage that is presented by the Virtualization layer to the OS instance as being part of the physical machine upon which the OS is executing. This may include persistent storage or file systems presented to the OS layer as a 'Network Drive' or other external storage resource. However this layer is primarily concerned with structured data storage within a Database Management System (DBMS) or similar bulk data storage application/service.

Cloud Providers may offer access to a general 'database' as a service or a dedicated DBMS instance installed within a dedicated OS. Generally, access to a 'database' will refer to a specific database structure that resides within a shared DBMS. In the case of a dedicated DBMS, large storage files associated with the DBMS may be stored on shared file system space. The options available from a number of Cloud Providers may make determination of whether the database capability is a Shared or Dedicated Resource difficult.

NOTE: In some cases a Cloud Provider may offer Dedicated Resources at a higher level of the CIEM, and a lower level of the CIEM, but still provide the database as a Shared Resource. Provider claims of a Dedicated Resource in this layer should be carefully examined.

NOTE: This layer may not be relevant to particular cloud based applications or services and may be discarded for the analysis of Cloud Provider infrastructure where it is not utilized for CJIS data.

4.1.6 Application Processing Layer

The Application Processing Layer of the CIEM consists of the application or service components responsible for the processing, manipulation, or handling of data. The application components may either be a Cloud Provider custom application/service, or a commercially available application (to include desktop applications) delivered as a cloud based service. Multiple applications/services may exist within the Application Processing layer, and each application should be individually evaluated regarding trust level, scope of control, and as a Shared or Dedicated Resource.

Executable code that processes, manipulates, or transforms data and executes directly on the OS layer will be considered at the Application Processing Layer. Executable code or 'scripting language' code that executes within the 'web' interface component (e.g. web server) will be classified as Application Presentation Layer for purposes of the CJIS CIEM. For example, a binary executable installed directly on the OS would be Application Processing layer, while a .NET binary executing within a stand-alone web server component would be considered Application Presentation layer. However, a dedicated application that contains an embedded web server component for presentation would be evaluated at the Application Processing layer.

NOTE: The Application Processing Layer may not exist in some cloud scenarios. For instance, a web site at the Application Presentation layer may directly access a DBMS at the Data Storage layer and simply provide and input/output interface to the Data Storage Layer, precluding the need for application processing of the data.

4.1.7 Application Presentation Layer

The Application Presentation Layer consists of the cloud infrastructure components that format or encapsulate data or applications in a fashion suitable for distribution as a cloud service or application. Typically this will consist of the 'web' or 'internet-enabled' components of a cloud service or application. This layer consists of any executable binary, script, or other code that executes inside the context of a web server instance (e.g. IIS, Apache, etc) as well as the web server itself, whether installed on the same or a different OS from any supported Application Processing Layer or Data Storage Layer component. This layer will typically include any system component designed for direct Hypertext Transfer Protocol (HTTP) access from outside the Cloud Provider infrastructure, to include both embedded and stand-alone web server components. However, it should also include components intended for direct access from outside the Cloud Provider infrastructure.

Executable code that processes, manipulates, or transforms data and executes directly on the OS layer will be considered at the Application Processing Layer. Executable code or 'scripting language' code that executes within the 'web' interface component (e.g. web server) will be classified as Application Presentation Layer for purposes of the CJIS CIEM. For example, a

binary executable installed directly on the OS would be Application Processing layer, while a .NET binary executing within the web server component would be considered Application Presentation layer. However, a dedicated application that contains an embedded web server component for presentation would be evaluated at the Application Processing layer as well as at the Application Presentation layer.

The Application Presentation Layer may include the authentication and access control mechanism for the Application Presentation Layer itself and/or one or more underlying layers (e.g. Application Processing Layer, Data Storage Layer). Alternatively, it may only act to pass user credentials to an underlying layer.

NOTE: The Application Presentation Layer will exist in some form in any Cloud Service that is accessible from the Internet. However, some cloud scenarios may only allow access to the services or applications through a dedicated Virtual Private Network (VPN) connection. In these cases the Application Presentation Layer of the CIEM may not exist (e.g. Cloud Entry Point layer directly connects to Application layer, Data Storage Layer, or OS layer.)

4.1.8 Cloud Entry Point Layer

The Cloud Entry Point layer consists of Cloud Provider infrastructure devices or services intended to either protect lower layer components from unauthorized external access or explicitly allow authorized access. This layer consists of Gateways, Intrusion Prevention/Detection Devices, Proxies, Firewalls, VPN's, or other similar devices intended to separate the Cloud Provider infrastructure from the internet or other external networks. Components within this layer may or may not require or allow explicit authentication prior to allowing external network access into the Cloud Provider infrastructure.

NOTE: This layer does NOT include Firewalls, Intrusion Prevention/Detection Device/software, Proxies, VPN's, or similar protective devices installed directly at the OS or Application Processing layers of a Cloud Consumer controlled component. It includes only dedicated boundary devices/software between provider infrastructure and external networks/internet.

NOTE: Cloud Providers will typically retain both control and access to this layer. Some providers may allow Cloud Consumer control of some elements of this layer pertaining to the Consumer's components only through a dedicated management console. Rarely will this constitute full delegation of control of this layer to the Cloud Consumer.

4.1.9 Cloud Consumer Client Layer

The Cloud Consumer Client Layer consists of the software components installed on Cloud Consumer computing resources within physical control of the Cloud Consumer (e.g. desktop computer, laptop, etc) that are used to access the cloud based applications, services, or data. In most cases this layer will consist of the web browser installed on the client computers, but may include one or more browser plug-ins from either the Cloud Provider or a third-party provider (e.g. Java, Flash, Silverlight, etc). However, in some cases specialized Cloud Provider agents or software may be installed on Client Computers that autonomously interface with aspects of the Cloud Provider infrastructure or utilize protocols other than HTTP/HTTPS to communicate with Cloud Provider services.

NOTE: This layer is included to capture special requirements that may exist regarding patching or maintenance of client based software components. Both control and access will typically reside solely with the Cloud Consumer for the components installed on the client computers; however any specialized Cloud Provider software should be evaluated to determine if the software provides either control or access from Cloud Provider components to the client.

4.2 Trusted and Non-Trusted entities

Both Cloud providers and Peer Cloud Consumers may be classified as either trusted or non-trusted entities. Trusted entities are providers or peer consumers that have undergone evaluation against a common set of security controls (e.g. NIST SP 800-53 or equivalent) and provides documentation, artifacts, or federal government agency approval of security control application to their systems, personnel, and processes. For example, a Cloud Provider that can provide documentation and testing to support compliance with controls equivalent to those set forth in CJIS policy, including personnel security on individuals with technical control or access to the cloud infrastructure, would be considered a 'trusted' provider. Security controls provided by a trusted provider will be evaluated in the same fashion as any other contracted service provider and compliance to the evaluated controls may be inherited by the CJIS Cloud Consumer. Conversely, a Cloud Provider that cannot, or will not provide documentation or acceptable testing of security controls applied to the cloud infrastructure under their control will be considered a non-trusted provider. Security functions provided by non-trusted providers will not be considered as part of the CJIS evaluation process, which will result in additional controls being necessary within the portions of the cloud infrastructure controlled or accessed by the non-trusted providers.

Trusted Cloud Providers with specific controls in place to enforce separation between Cloud Consumers within the Cloud infrastructure will be evaluated regarding the effectiveness of the separation and those controls may or may not be considered acceptable based on their conformance to existing CJIS policy requirements. However, for non-trusted Cloud Providers, separation controls will not be considered and peer level Cloud Consumers will be considered to have potential access to the CJIS Cloud Consumer resources at every shared resource level, and additional controls must be applied to the shared resource CIEM layers by the CJIS Cloud Consumer.

Cloud Providers may be considered either Trusted or Non-Trusted for each level of the cloud infrastructure evaluation model, based on the control and testing documentation provided that is applicable to each layer of the model. Third Party or supplementary Cloud Providers contracted by the primary Cloud Provider to provide portions of the infrastructure are considered part of the primary Cloud Provider for determination of trust. If any component of the Cloud Provider (s) is considered Non-Trusted for a layer, the Cloud Provider will be considered Non-Trusted for the layer. However, if the primary Cloud Provider can show that any supplementary or third-party infrastructure providers have neither sole control nor access of the portion of the infrastructure they provide, the Cloud Provider status may still be considered 'Trusted' after careful evaluation of the specific scenario. For example, a Cloud Provider that relies on multiple third-party Internet Service Providers for connectivity between the Cloud Provider data centers, but appropriately encrypts the data transiting the connections and retains control over which links data traverses may still be considered a trusted provider since the third party providers have neither access (due to cryptographic separation) nor sole control (affecting data availability) to the CIEM layer.

Some peer level Cloud Consumers may be evaluated and considered Trusted Peer Cloud Consumers, under the same criteria used to determine trusted or non-trusted Cloud Providers. If a trusted or non-trusted Cloud Provider can demonstrate that certain CIEM levels are shared only between a set of Trusted Cloud Consumers (e.g. Semi-Private Cloud) control requirements may be reduced in some cases for those layers. For some CIEM layers, controls applied to the layer are based on the trust level of the layer itself and one or more layers below.

4.3 Layer Control and Access
Cloud Providers may have Full Control, Access, or No Access to any particular layer of the cloud infrastructure. A determination of the level of control and access the Cloud Provider possesses must be made for each layer in the CIEM. The level of control or access the Cloud Provider has for any layer will affect the security controls or encryption requirements for that layer, but may also affect the control or encryption requirements for other layers of the CIEM.

4.3.1 CIEM Layer Full Control: The Cloud Provider exercises administrative or management control over the layer. This includes control/management of the account or credential database, security roles, backup/restoration, or any resource management within the CIEM layer. While in some scenarios it may be possible to exert management control without having access to the data, for purposes of the CJIS policy and security control assignment, any entity that maintains management control of a CIEM layer will be considered to have access to that layer as well.

4.3.2 CIEM Layer Access: The Cloud Provider possessed the credentials (username/password, encryption key, token, etc) or other technical means (e.g. logs, backup data, etc) to read unencrypted data at the CIEM layer, they are considered to have Access to the layer. This specifically includes scenarios where the Cloud Provider retains the capability to gain access to a layer using a non-destructive method (gain access without deletion of Consumer data) or escrowed encryption keys even if that capability is not generally exercised.

4.3.3 CIEM Layer No-Access: The Cloud Provider is considered to have No-Access to a CIEM layer if there is no physical, logical, or technical means available to read or record Cloud Consumer data that exists within a CIEM layer. (NOTE: This is typically only possible for CIEM layer 4-9 and it may be difficult to validate provider claims of 'No-Access' at any layer) It is possible for a Cloud Provider to still exert some management control over resources at a CIEM layer, but still be considered to have 'No-Access' to the layer for purposes of data confidentiality. This is generally accomplished via cryptographic separation where the provider does not retain the keys, but still controls allocation of resources at the layer.

4.4 Evaluation and Impact of Shared Resources
In some cloud computing technical architectures, the Cloud Provider may offer different levels of service access to layers within the CIEM based on customer needs and pricing. This can introduce additional risk in Non-Trusted Peer Consumer environments, depending on the potential level of access granted to Non-Trusted Peer Consumers. If a Non-Trusted Peer Consumer may have access to a lower technical level of the cloud infrastructure than the CJIS Cloud Consumer there is an increased risk of the Non-Trusted Peer Consumer violating the Cloud Provider separation policies in such a way as to gain un-detected access to CJIS Cloud Consumer resources. Without access to the same level of the cloud infrastructure as potential

peer consumers, detection of unauthorized access at lower levels in the cloud infrastructure model may be impossible for the CJIS Cloud Consumer.

Potential security issues resulting from Non-Trusted Peer Consumer access are most likely to occur within layers 4-7 of the CIEM, and particularly within layers 5-6. Within CIEM layers 5-6, separation between peer cloud consumers may only be enforced by the security applied to a single application or middleware product. For example, a shared Database Management System (DBMS) may provide data storage at layer 5 of the CIEM. Each peer consumer may have a unique database within the DBMS, but separation between the database instances is only enforced by the rules applied to the DBMS. In this case, mis-configuration of DBMS rules, mis-configuration or CJIS Cloud Consumer database security, or malicious exploitation of the DBMS could all allow a Peer Cloud Consumer inappropriate access to the CJIS Cloud Consumer database.

To properly identify risks in this area, all layers of the cloud infrastructure model of the Cloud Provider that contain Shared Resources must be identified. Further, Shared Resource layers to which peer consumers may be granted some level of access must be identified. All CIEM layers will be considered either a Shared Resource layer or a Dedicated Resource layer.

4.5 Evaluation Criteria for Cloud Infrastructure Layers

Table 4.1 provides specific evaluation criteria for each layer in the cloud infrastructure evaluation model. These criteria serve as a guide to evaluating the trust level of the Cloud Provider and the determination of shared or dedicated resource status.

Layer	Trusted Provider	Dedicated Resource
Network Layer	**1.** Any network traffic within the Cloud Provider infrastructure managed or accessed by a third party provider is encrypted and protected at a level commensurate with the CJIS policy.	1. The Cloud Provider is Trusted for this layer. 2. Shared Devices (physical or virtual) have undergone Common Criteria or US Government testing to validate the separation mechanisms/software 3. Provider documentation and testing identifies and validates specific configurations used to enforce separation of Peer Consumer network traffic at this resource layer.
Physical Device Layer		1. The Cloud Provider is Trusted for this layer. 2. Dedicated hardware (both computing platform and storage) is guaranteed to

		the CJIS Cloud Consumer for exclusive access.
Virtualization Layer	1. The virtualization Hypervisor has undergone Common Criteria or US Government testing to validate the security functions and virtualization container separation functions.	1. The Cloud Provider is Trusted for this layer. 2. The Physical Device Layer (layer 2) is NOT a Shared Resource 3. The Virtualization layer instance is dedicated to the CJIS Cloud Consumer.
Operating System Layer	1. The Cloud Provider it Trusted for the Virtualization Layer	1. The Cloud Provider is Trusted for this layer. 2. The OS instance is dedicated to the CJIS Cloud Consumer 3. The file system presented to the OS instance by the Virtualization layer as being part of the physical machine upon which the OS executes is either: 4. A dedicated resource, 5. Encrypted using FIPS 140-2 (or successor) approved cryptographic algorithm (128-bit or longer key length) with the decryption keys only accessible to the Virtualization Layer and OS Layer, or 6. File system segregation is enforce by a Common Criteria or equivalent US Government certified product with validated/tested configuration settings applied to guarantee resource separation.
Data Storage Layer	1. The Cloud Provider is Trusted at the OS layer.	1. The Cloud Provider is Trusted for this layer. 2. The DBMS (or similar

		storage middleware/application) instance is dedicated to the sole use of the CJIS Cloud Consumer
Application Processing Layer	1. The Cloud Provider is Trusted at the OS layer. 2. The Cloud Provider is Trusted at the Data Storage layer (if a data storage layer exists for the application).	1. The Cloud Provider is Trusted for this layer. 2. No Peer Cloud Consumers have direct access to resources on this layer 3. The application instance is dedicated to the CJIS Cloud Consumer
Application Presentation Layer		1. The Cloud Provider is Trusted for this layer. 2. No Peer Cloud Consumers have direct access to resources on this layer 3. The application instance is dedicated to the CJIS Cloud Consumer
Cloud Entry Point Layer		1. The Cloud Provider is Trusted for this layer. 2. No Peer Cloud Consumers have direct access to resources on this layer 3. The application instance is dedicated to the CJIS Cloud Consumer
Cloud Consumer Client Layer	1. Any specialized Cloud Provider software installed on client computers has been evaluated and tested to ensure proper function and security in accordance with the standard CJIS policy requirements.	1. This layer will always be a Dedicated Resource layer.

Table 4.1 Evaluation Criteria

5.0 Cloud Deployment Evaluation Process

CJIS Agencies and Organizations desiring to implement cloud computing solutions must ensure that those solutions are fully compliant with the CJIS Security Policy. Agencies and organizations will perform an analysis of their proposed solutions and provide the results to CJIS for adjudication. Upon successful adjudication permission will be granted for implementation. This procedure is enabled by the Cloud Provider Evaluation Process.

5.1 CJIS Cloud Provider Evaluation Process.

This process is intended for use by prospective CJIS Cloud Consumers, as well as by CJIS review of proposed Cloud deployment involving CJIS data. There are four main steps in the process, with 3-4 tasks within each step, as depicted in Figure 5.1.

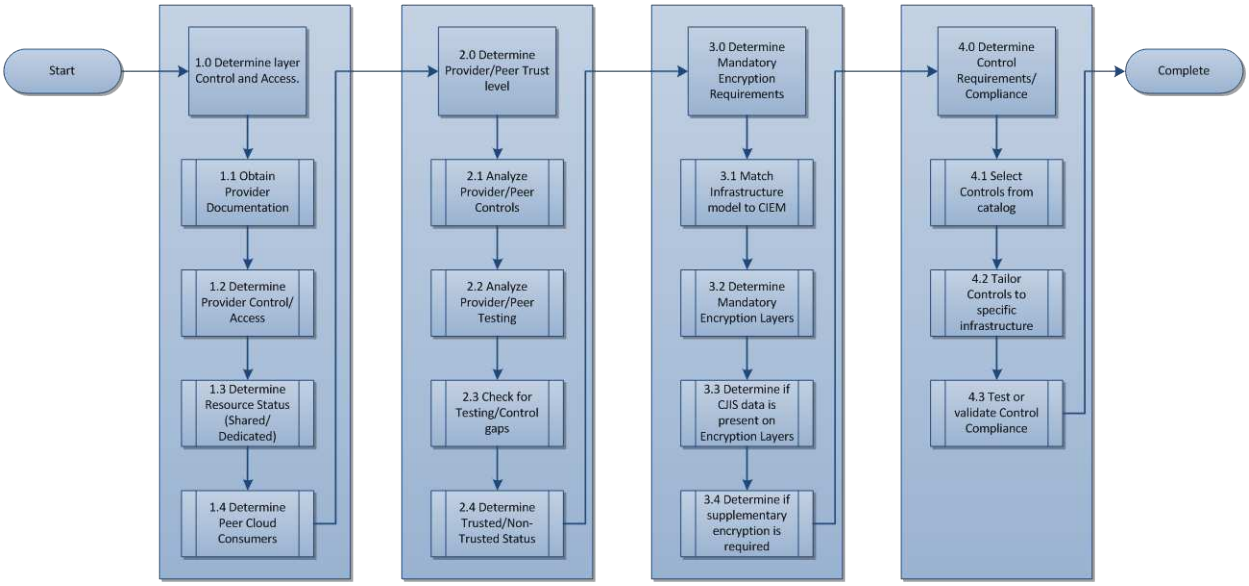

Figure 5.1 Cloud Deployment Evaluation Process

The following sections describe the process used to evaluate any proposed Cloud Infrastructure for suitability to house CJIS data and to determine the specific control requirements that must be applied to the infrastructure in order to be acceptable for CJIS data storage, processing, transmission, or display.

5.1.1 Determine layer Control and Access.

The purpose of this step is to determine which entities (e.g. Cloud Provider, Third-Party Provider, CJIS Cloud Consumer, Peer Cloud Consumer) have Control, Access, or share resources on each of the 9 layers of the CIEM. This step is broken down into four tasks described in the following sections.

5.1.1.1 Obtain Provider Documentation

Obtain Cloud Provider documentation. Documentation may be available from the Provider website in the form of white-papers, technical documents, diagrams or Service Level Agreements (SLA). Documentation may also be available from the Provider via special request. The Cloud Provider may be able to provide information security documentation sufficient to complete the infrastructure evaluation, however, in most cases specific questions or an active dialog will need to occur between the prospective CJIS Cloud Consumer or the CJIS infrastructure evaluator and the Cloud Provider to address the information required to complete some of the following tasks and steps.

5.1.1.2 Determine Provider Control/Access

Based on the Cloud Provider documentation and/or discussions with the Cloud Provider, determine if the Cloud Provider infrastructure employs components at all layers of the CIEM. For each layer employed within the CIEM, determine the level of control and access the Provider maintains per section 4.2.

5.1.1.3 Determine Resource Status (Shared/Dedicated)

Based on the Cloud Provider documentation and/or discussions with the Cloud Provider, determine if each layer employed within the Cloud Provider infrastructure meets the criteria of a 'Dedicated' resource per section 4.5. If the layer does not meet the criteria for a Dedicated Resource layer, then the layer will be considered a 'Shared' Resource layer.

5.1.1.4 Determine Peer Cloud Consumers

For each 'Shared' Resource layer identified in the preceding task, determine what, if any, rules are applied by the Cloud Provider to segregate resources between Peer Cloud Consumers. If the Cloud Provider indicates Peer Cloud Consumers are restricted to particular customer types, (e.g. Government customers) obtain a list of current customers and the rules applied to identify future customers that may share resources at each CIEM layer.

NOTE: This task is intended to identify address 'Semi-Private' cloud implementations where the Cloud Provider specifically designs and markets the cloud service to a restricted customer based, such as federal, state, or local government entities. Normally, commercially available cloud infrastructures will not offer pricing options for 'shared' or 'dedicated' resources, but will not allow restrictions on which other peer consumers may share resources in the 'shared' models

5.1.2 Determine Provider/Peer Trust Level

The four tasks within this process step characterize the trust level that can applied to the Cloud for each CIEM layer where the Provider has 'Control' or 'Access'. For any layer that has been identified as a Shared Resource layer, the trust level of any current or possible Peer Cloud Consumers must also be identified. If the Cloud Provider has either control or access to a layer and uses a sub-provider or third party provider with either control or access for some or all of the technical functions within a layer, the layer trust level will be the lowest level of trust for the entire layer. For example, if the primary Cloud Provider functions satisfy the criteria for 'Trusted Provider' for a given layer, but a supplementary Cloud Provider also provides services but does not meet the 'Trusted Provider' criteria, then the entire layer is considered to be a 'Non-Trusted Provider' layer, unless the primary Cloud Provider and definitively prove the third party provider cannot exercise either control of access over the CJIS data.

For a CIEM layer identified as a Shared Resource layer to be considered a 'Trusted Peer Cloud Consumer' layer, all of the following criteria must be met:

- Current Peer Cloud Consumer listing with contact information for associated approving authorities or authorizing officials is provided
- Rules for assigning new Peer Cloud Consumers to the shared resource is provided
- Only federal, state, or local government entities may be assigned to the shared resource
- Peer Cloud Consumers have authorizations to operate based on a formal approval process (NIST Risk Management Framework, CJIS authorization process, or equivalent) with final written approval from a federal, state, or local government approving authority.
- The Cloud Provider process for adding new Peer Consumers to the shared resource includes notification to existing Peer Consumers for the resource that a new Peer Consumer is being added.

5.1.2.1 Analyze Provider/Peer Controls

Identify all security controls applied by the Cloud Provider (or third party providers) associated with each layer of the CIEM for which control or access resides with the provider. Compare the controls against the criteria identified in section 4.4, to include the controls listed in Appendix A (Cloud Control Catalog) as required for a trusted provider at each layer of the SIEM.

Identify Cloud Provider specific controls that substantiate provider claims of 'No Access' to all CIEM layers identified as 'No Provider Access' layers. Testable controls must exist within one or more layers of the CIEM assigned to Cloud Provider control to substantiate 'No-Access' at higher layers of the CIEM. For example, to substantiate provider 'No-Access' to layer 4, testable controls should be present at layers 2 and 3 to prove 'No-Access' at layer 4. Controls validating 'No-Access' claims must be testable and satisfactorily complete testing, otherwise a minimum rating of 'Non-Trusted Provider Access' must be assigned to the layer.

Identify existing and mandatory controls applied to each Peer Consumer and compare against Appendix A requirements for each layer identified as a shared resource layer

5.1.2.2 Analyze Provider/Peer Testing

Obtain test results from the Cloud Provider or contract/conduct independent testing of the Providers control compliance claims. If the Provider has contracted with an independent third party evaluation agency, CJIS will conduct a review of the test results, and may require auditing by a CJIS representative of existing test results or retesting of the results by a CJIS representative. All controls identified as mandatory in the preceding task must have complete test results available that are applicable to each CIEM layer under review. Missing or incomplete test results or the inability of CJIS to fully review the test agency will result in the provider being considered 'Non-Trusted' for the associated CIEM layer.

Peer Cloud Consumer requirements and test procedures associated with each layer will be analyzed to determine if the Trusted Peer Consumer requirements identified in Appendix A are being met by all Peer Consumers sharing resources with the CJIS Cloud Consumer.

5.1.2.3 Check for Testing/Control gaps

Test results from task 2 of this step are compared against both control claims (task 1) and control requirements identified in Appendix A to qualify Providers or Peers at each layer of the CIEM

for 'Trusted' status. Control testing will be matched against the particular technical implementation of each layer individually to ensure all requirements have been successfully met and properly tested. Many controls are duplicated for each layer; however, they may apply to different devices or software components at different layers in the CIEM. This may include a detailed analysis of the Cloud Provider internal architecture in order to determine if requirements have been met. Validated control compliance at one CIEM layer does not necessarily prove compliance at a different layer. For example, a provider might meet the physical security requirements for the primary data center (CIEM layer 2), but could fail to have met or tested the physical security requirements for some or all network components (CIEM layer 1) that exist outside the primary data center. Alternatively, compliance with logical access controls at layer 2 or 3 (or other combinations) may reside with a different organizational unit with the Cloud Provider than compliance with layers 4, 5, or 6 and would need additional test results to validate.

5.1.2.4 Determine Trusted/Non-Trusted Status

Based on the preceding task results, each CIEM layer to which the Cloud Provider (or sub-Providers) has either control or access privileges should be identified as either a 'Trusted Provider' or 'Non-Trusted Provider'. Any discrepancy or incomplete information will automatically result in a 'Non-Trusted' provider status for the associated CIEM layer.

For each Shared Resource CIEM layer, the presence of Trusted and Non-Trusted Peer Cloud Consumers must be identified. The layer will be categorized as a 'Trusted Peer Cloud Consumer layer only if all Trusted Peer criteria are met for all current and future Peer Consumers. In all other cases, the layer will be considered a Shared Non-Trusted Peer Consumer layer.

5.1.3 Determine Mandatory Encryption Requirements

The purpose of this step and four tasks within it are to determine for each CIEM layer if full encryption of CJIS data is mandatory for that layer. For layers designed as mandatory encryption layers, the CJIS information (possible all Cloud Consumer data) contained within that layer must be encrypted to the standard identified in section 5.10.1.2 of CJIS Security Policy. Encryption/Decryption keys may only be stored and accessible within a CIEM layer that does not have a mandatory encryption requirement.

5.1.3.1 Match Infrastructure model to CIEM.

Match the particular infrastructure model being employed by the CJIS Cloud Consumer to the CIEM and the Cloud Infrastructure Questionnaire (Table 5.1). Mark any layer rows as Not Applicable (N/A) if that layer is not being utilized by the CJIS Cloud Consumer. The layer may still exist within the Cloud Provider infrastructure, but will only be considered if employed by the CJIS Cloud Consumer service or application.

Evaluation Layer	Trusted	Non-Trusted	Shared	Dedicated
Layer 1				
Layer 2				

Layer 3				
Layer 4				
Layer 5				
Layer 6				
Layer 7				
Layer 8				
Layer 9				

Table 5.1 Questionnaire

5.1.3.2 Determine Mandatory encryption layers.

Compare a completed Cloud Infrastructure Questionnaire (Table 5.1) with the Mandatory Encryption Table (Table 5.2) to determine which layers of the infrastructure model must have all CJIS data encrypted.

Certain Cloud Provider infrastructure scenarios will drive a mandatory data encryption requirement for one or more CIEM layers based on the trust level and levels of control/access of the provider at various levels and the presence of Non-Trusted Peer Cloud Consumers at various levels. Table- 5.2 defines the common scenarios that result in mandatory encryption requirements at various CIEM layers. The table reflects the status results that require Mandatory Layer Encryption for each Evaluation Layer.

As an example, consider Layer 4. If L2 status is N, then Layer 4 encryption is required. If L4 is N, then Layer 4 encryption is required. If L2 and L3 are T, but L4 is TS, then encryption of Layer 4 is required. No encryption of Layer 4 is required for any other cases.

Evaluation Layer	L1 Status	L2 Status	L3 Status	L4 Status	L5 Status	L6 Status	L7 Status	L8 Status	L9 Status	Mandatory Layer Encryption
Layer 1	N									Y
	TS									Y
Layer 2		N								Y
Layer 3			N							Y

Layer 4		N								Y
				N						Y
		T	T	TS						Y
Layer 5		N								Y
			N							Y
				N						Y
				TS						Y
					N					Y
		T	T	TD	TS					Y
Layer 6		N								Y
			N							Y
				N						Y
				TS						Y
					N					Y
					TS					Y
						N				Y
		T	T	TS	TS	TS				Y
Layer 7		N								Y
			N							Y
				N						Y
				TS						Y
					N					Y
					TS					Y
						N				Y
						TS				Y
		T	T	TD	TD	TD	TS			Y
Layer 8										Y
Layer 9									N	Y

Key	
N	Control or Access held by a Non-Trusted Cloud Provider, Any value for 'Shared' or 'Dedicated' resource layer

TD	Control or Access held by a Trusted Cloud Provider, 'Dedicated' resource layer or resource layer with ONLY Trusted Peer Cloud Consumers sharing resources at that layer.
TS	Control or Access held by a Trusted Cloud Provider, 'Shared' resource layer with the potential for a Non-Trusted Peer Cloud Consumer to be sharing resources at that layer.

Table 5.2 Mandatory Encryption Table

All CIEM layers with a mandatory encryption requirement will treat CJIS data as if it is being transmitted/stored outside of a physically secured location per section 5.10.1.2 of CJIS Security Policy. However, if bulk CJIS data is stored within a mandatory encryption layer, a minimum of AES 128-bit encryption should be used to encrypt the data.

All connections between CIEM Layer 9 (Client layer) and any Cloud Provider infrastructure layer have a mandatory encryption requirement using the same controls identified in section 5 of the CJIS Security Policy.

5.1.3.3 Determine if CJIS data is present on encryption layers.

For all CIEM layers identified for mandatory encryption, identify if CJIS data exists that is accessible within those layers. CJIS data may not exist within all layers of a particular model (e.g. layer 5 data storage layer may not be utilized for CJIS data, but could be used for other CJIS Cloud Consumer data). The mandatory encryption requirement may be waived for layers that do not store, process, transmit, or otherwise access CJIS data or encryption/decryption keys for CJIS data.

5.1.3.4 Determine if supplementary encryption is required.

Based on the overall infrastructure design employed by the CJIS Cloud Consumer and Cloud Provider, determine if supplementary encryption requirements are necessary to protect either CJIS data, or encryption/decryption keys associated with CJIS data. Cases not fully covered by the CIEM or Table 5.2 may require supplementary encryption to ensure data protection is adequate.

5.1.4 Determine Control Requirements/Compliance

The purpose of this step is to determine if all controls required for the Cloud Infrastructure being employed by the CJIS Cloud Consumer and all associated Cloud Providers for CJIS data are fully compliant with CJIS policy.

5.1.4.1 Select Controls from catalog.

Select controls from the table in Appendix A for each layer of the CIEM based on which entities have control of the layer, access to the layer, or are present on a Shared Resource layer. Control requirements will vary for each layer based on the applicable technologies and whether the

Cloud Provider and any Peer Cloud Consumers meet the criteria for 'Trusted' providers or peer consumers.

Each control identified as applicable from Appendix A, will have responsibility assigned to either the Cloud Provider or the CJIS Cloud Consumer. If a Cloud Provider does not sufficiently comply with a control requirement, the CJIS Cloud Consumer must either apply equivalent supplementary controls in order to meet compliance requirements or make design modifications to the cloud based infrastructure, service, or application in such a way that compliance can be achieved (e.g. supplementary encryption of data)

5.1.4.2 Tailor controls to specific infrastructure.

Due to the continuing advancement of technology and the wide range of choices available in the design of a cloud-based infrastructure, service, or application, it may be necessary to tailor the controls identified in the CJIS Security Policy and Appendix A of this addendum to more closely match the employment scenario and specific technologies. Tailoring of the control requirements can only be accomplished by communication between the CJIS Cloud Consumer and the CJIS compliance reviewers to ensure all parties understand and agree to specific control requirement tailoring. Any control tailoring will be documented as part of the overall security plan for the cloud infrastructure hosting the CJIS data.

5.1.4.3 Test or validate control compliance.

Conduct or contract testing for all controls assigned to the CJIS Cloud Consumer. Verify that previously analyzed Cloud Provider testing (section 5.1.2.2) shows compliance in all Provider assigned controls. Supplementary testing may be required for some controls if not adequately covered by existing, trusted test results.

6.0 CJIS Security Policy Recommended Changes

The CJIS Security Policy does not explicitly preclude Agencies and Organizations from implementing Cloud Computing Solutions. However, in light of the requirements for vetting cloud provider services, there are changes that will provide clarity and ensure that the Policy is comprehensive. Table 6.1 provides rational for development of language that can be inserted into each referenced section.

CJIS Security Policy Paragraph	Section Title	Agency / Organization Consideration	Cloud Service Provider Consideration
5.1.1.3	Criminal Justice Agency User Agreements		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
5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum		The Cloud Provider must agree to the CJIS Cloud Provider Security Addendum for any CIEM layer in which they have control or access.
5.1.2	Monitoring, Review, and Delivery of Services		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
5.1.2.1	Managing Changes to Service Providers	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.
5.2	Security Awareness Training		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
5.2.1.1	All Personnel		Applicable to provider personnel involved with controlled or accessible layers only
5.2.1.2	Personnel with Physical and Logical Access		Applicable to provider personnel involved with controlled or accessible layers only
5.2.1.3	Personnel with Information Technology Roles		Applicable to provider personnel involved with controlled or accessible layers only

5.2.2	Security Training Records		Provider testing should show maintenance of records for provider personnel
5.3	Policy Area 3: Incident Response	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 documents 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
5.3.1	Reporting Information Security Events	Reporting requirements from agencies will include cloud provider controlled layers	
5.3.1.1.2	CSA ISO Responsibilities	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
5.3.2.1	Incident Handling	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			Successful breaches of the provider boundary or internal network access controls must be reported at a minimum
5.3.2.1.2			Any physical access breach must be reported

5.3.2.1.3			Any successful or attempted compromise of security containerization or segregation of shared resources by a Peer Cloud Consumer must be reported.
5.3.2.2	Collection of Evidence	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.
5.3.3	Incident Response Training	Agency training will include any special training required to manage incidents occurring within cloud provider controlled layers.	
5.3.4	Incident Monitoring	The agency incident monitoring will include tracking/monitoring of incidents reported by cloud providers	
5.4.1.1	Events	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.

5.4.1.1.1			Audit records must address network devices, applications and management software which control the network and boundary.
5.4.1.1.2			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
5.4.1.1.3			Audit records must show coverage of all applicable technologies within these layers.
5.4.1.1.1	Content		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.
5.4.2	Response to Audit Processing Failures		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.

5.4.3	Audit Monitoring, Analysis, and Reporting	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.	
5.4.4	Time Stamps	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	Protection of Audit Information	Audit records accessible to the agency from provider controlled layers must be periodically saved onto agency controlled layers for the appropriate retention period	
5.4.6.1		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.
5.5.1	Account Management	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.	

5.5.2	Access Enforcement	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.
5.5.2.1	Least Privilege	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.
5.5.2.4	Access Control Mechanisms	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.

5.5.4	System Use Notification	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	Session Lock	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

5.5.6	Remote Access	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.
5.5.7	Wireless Access Restrictions		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

5.6.2	Authentication Policy and Procedures	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.
5.6.2.1	Standard Authentication (Password)	Applicable to all layers with authentication mechanisms	Applicable to all layers with authentication mechanisms
5.6.2.2	Advanced Authentication	Applicable to all layers with authentication mechanisms	Applicable to all layers with authentication mechanisms

5.6.2.2.1	Advanced Authentication Policy and Rationale	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.	
5.6.2.2.2	Advanced Authentication Decision Tree	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.
5.6.3	Identifier and Authenticator Management	Applies to layers where technically applicable only.	Applies to layers where technically applicable only.
5.6.3.1	Identifier Management	Applies to layers where technically applicable only.	Applies to layers where technically applicable only.
5.6.3.2	Authenticator Management	Applies to layers where technically applicable only.	Applies to layers where technically applicable only.
5.6.4	Assertions	Applies to layers where technically applicable only.	Applies to layers where technically applicable only.
5.7.1	Access Restrictions for Changes	Applies to each layer individually.	Applies to each layer individually.

5.7.1.1	Least Functionality	Applies to each layer individually.	Applies to each layer individually.
5.7.1.2	Network Diagram	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.
5.7.2	Security of Configuration Documentation	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.
5.8	Media Protection		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.
5.8.1	Media Storage and Access		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.

5.8.2	Media Transport		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.
5.8.2.1	Electronic Media in Transit		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.
5.8.2.2	Physical Media in Transit		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.

5.8.3	Electronic Media Sanitization and Disposal		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.
5.8.4	Disposal of Physical Media		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	Policy Area 9: Physical Protection		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.

5.9.0.1			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.
5.9.1.8	Access Records		Visitor agencies are not required on the provider visitor access records. However, sufficient information must be maintained to positively identify visitors to the facility.
5.10	System and Communications Protection and Information Integrity	Section applies to technically appropriate components	Section applies to all technically appropriate components
5.10.1	Information Flow Enforcement	Item 1 is agency responsibility	Items 2 and 3 are provider responsibility.

5.10.1.1	Boundary Protection	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.
5.10.1.2	Encryption	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.
5.10.1.3	Intrusion Detection Tools and Techniques	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 an 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.
5.10.3	Partitioning and Virtualization	Applicable if agency has control of the virtualization layer.	

5.10.4.2	Malicious Code Protection	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.
5.10.4.4	Personal Firewall	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.	

5.11.1	Audits by the FBI CJIS Division	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 encryption requirements will be enforced for those layers.
5.11.1.1	Triennial Compliance Audits	Applies to all controlled	

	by the FBI CJIS Division	layers	
5.11.1.2	Triennial Security Audits by the FBI CJIS Division		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.
5.12.1.1	Minimum Screening Requirements for Individuals Requiring Access to CJI:		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.
5.12.1.2	Personnel Screening for Contractors and Vendors		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.
5.12.2	Personnel Termination		Access termination must be to infrastructure systems where unencrypted CJIS data may reside.
5.12.3	Personnel Transfer		Access termination must be to infrastructure systems where unencrypted CJIS data may reside.

5.12.4	Personnel Sanctions		Access termination must be to infrastructure systems where unencrypted CJIS data may reside.

Table 6.1 CJIS Security Policy Recommended Changes

Appendix A

Cloud Control Catalog [Attached]

Appendix B: Common Cloud Provider Infrastructure Examples.
The following sections provide examples of three common Cloud Provider infrastructure models and show how they would be evaluated under the CIEM.

NOTE: The following sections represent potential evaluations from different categories of provider services. Actual provider infrastructure and services may not necessarily evaluate to the same levels of trust, control, and access as described in the examples.

4.6.1 Software-as-a-Service (SaaS) Example
In the Software-as-a-Service (SaaS) example, we will examine a typical Cloud Provider model for delivery of an on-demand application.

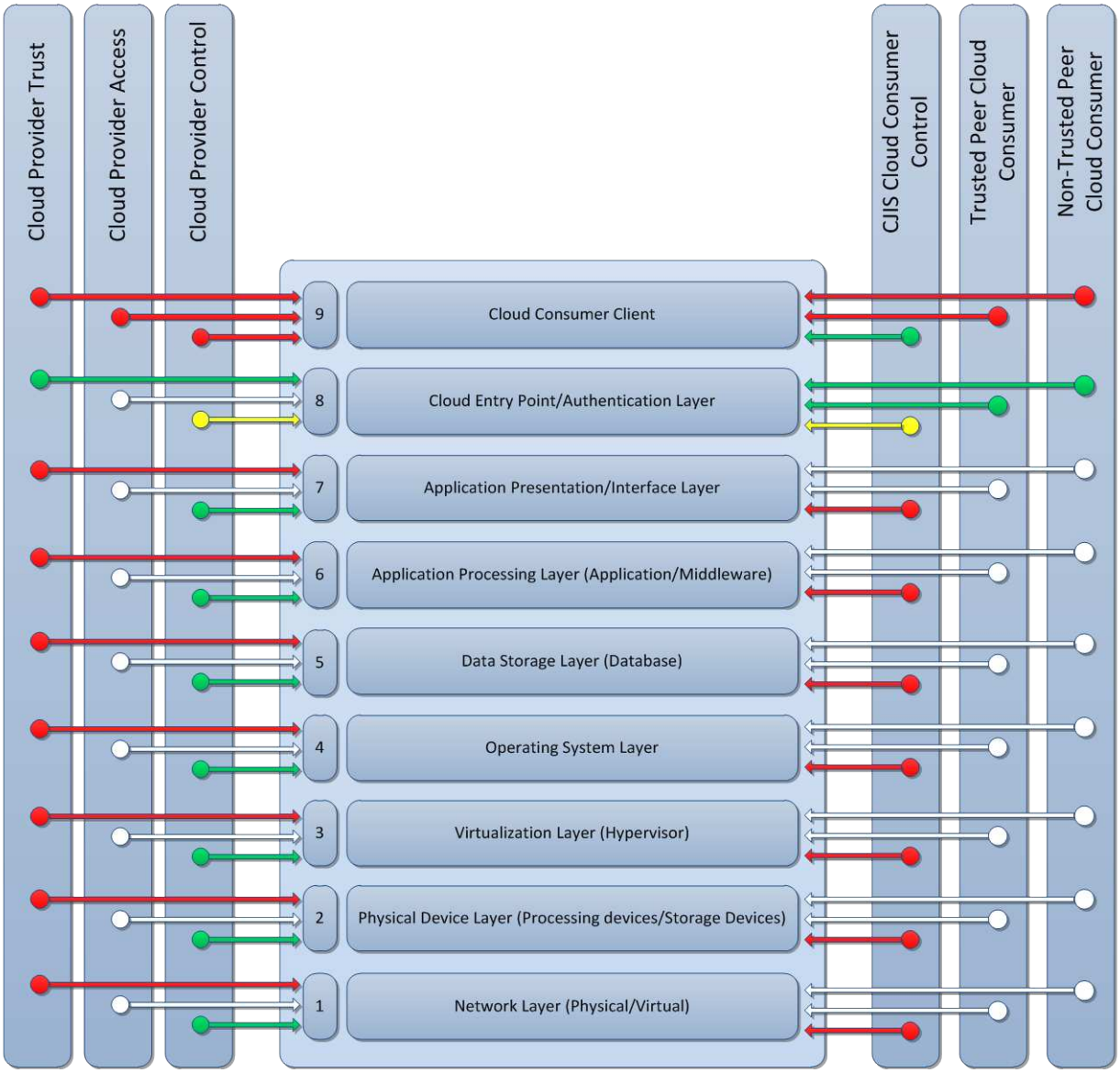

Figure B-1 SaaS example.

In this example we see a case where a Cloud Provider is providing a commercial on-demand cloud based application. This would be similar to an internet based email application or productivity product. In this scenario the Cloud Provider controls all layers 1-7 of the CIEM model completely, and shares user account management control of the Cloud Entry Point with the CJIS Cloud consumer, which also serves as the only authentication mechanism in the model. Unfortunately the Cloud Provider does not provide any security documentation or testing for layers 1-7 (this would be typical of this business model) and is considered 'Non-Trusted for those layers. Since encryption is always required through the Cloud entry point (boundary layer) and the provider is Non-Trusted for layers 1-7, the entire Cloud infrastructure has a mandatory CJIS data encryption requirement. Because of this we do not need to determine the presence of Peer Cloud Consumers (denoted by the white arrows) since a mandatory encryption requirement already exists. For this model to be utilized for CJIS data, the data would need to be encrypted per the CJIS Security Policy standards prior to being uploaded to the Cloud service or application. The CJIS data must be kept in an encrypted state at all times on the cloud infrastructure and the decryption keys must be maintained under CJIS Cloud Consumer control and not loaded to the cloud infrastructure at any time. This model could have some utility for storing individual CJIS data in encrypted single file formats in order to allow distributed access to the data by users with the proper decryption keys on their local computers. However, this model is not useful if any processing or manipulation of the data is required. Figure B-2 shows the resulting mandatory encryption requirements.

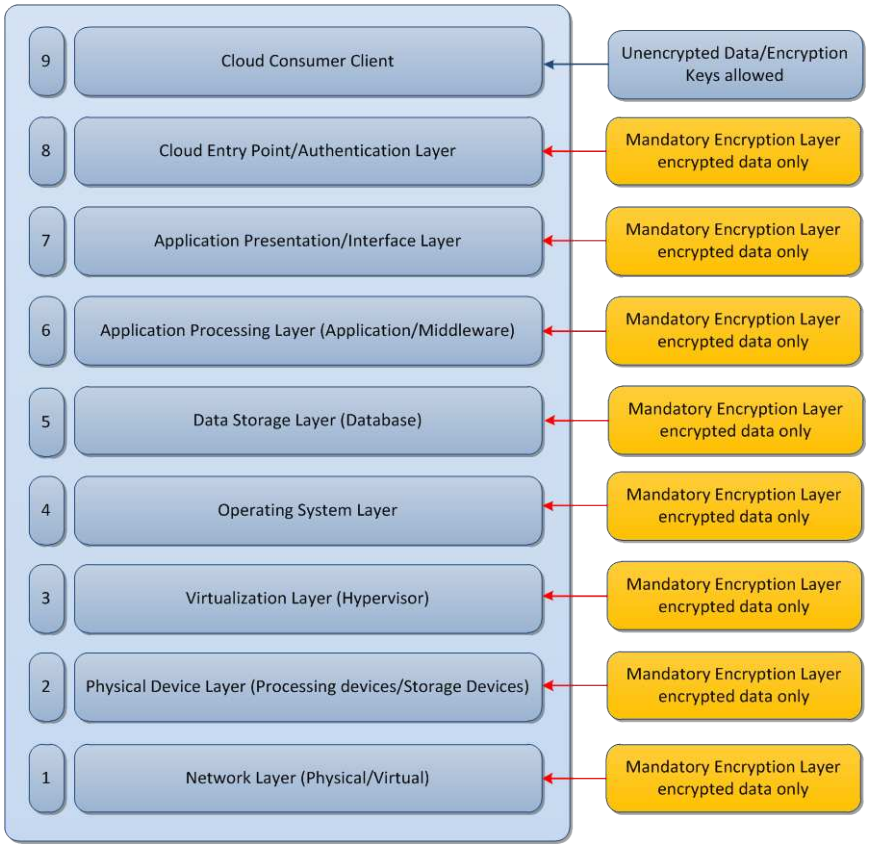

Figure B-2 SaaS encryption requirements

4.6.2 Platform-as-a-Service (PaaS) Example

In the Platform-as-a-Service example, we will examine a typical Cloud Provider model for delivery of an on-demand application platform where the Cloud Consumer controls several layers of the model.

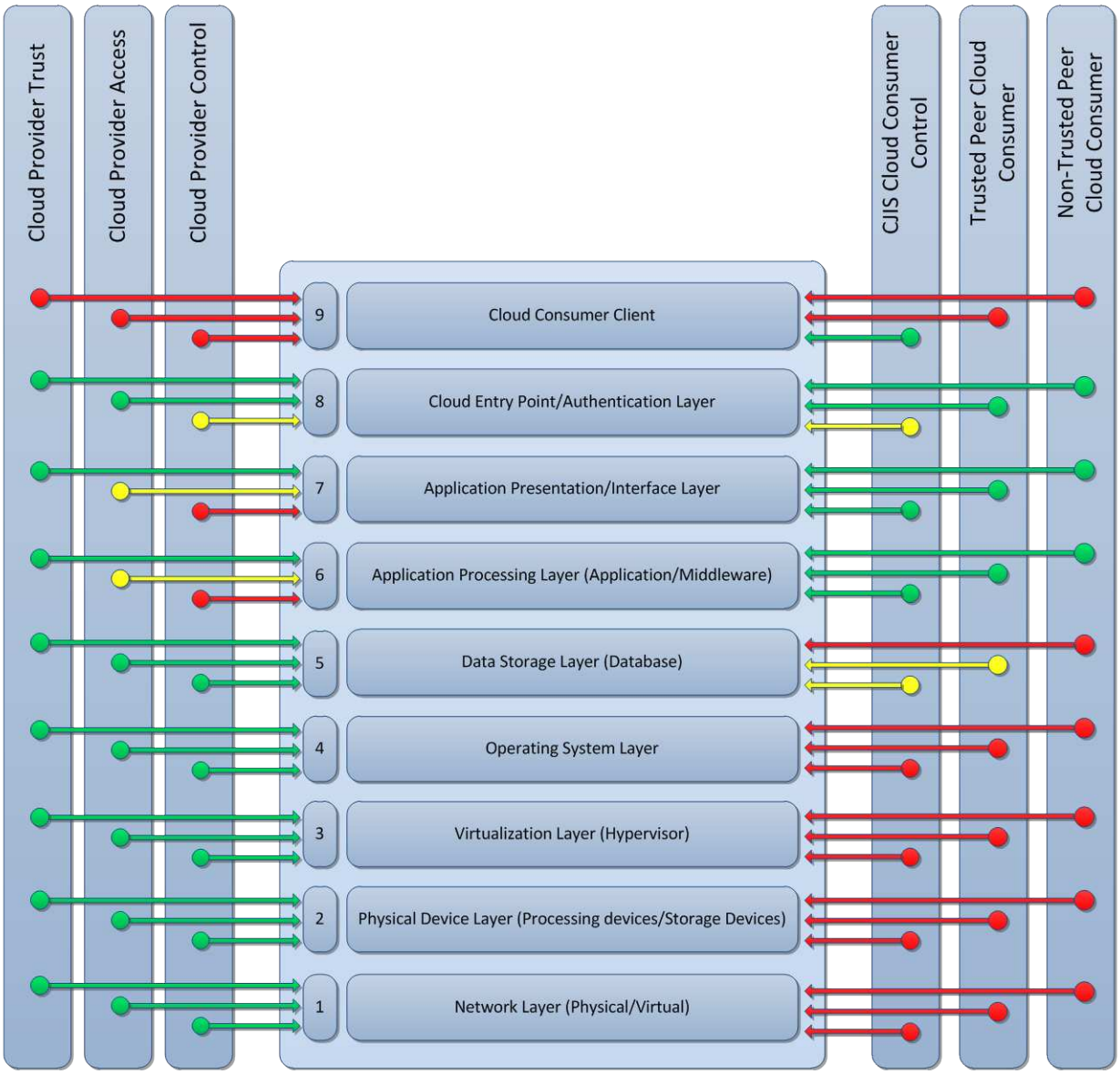

Figure B-3 PaaS example.

In this example, we see a case where a Cloud Provider is providing an application platform service with provider control of the infrastructure, Operating System (OS) and a database server. The provider shares access with the consumer to the application processing and presentation layer and shares control at layer 8, but the provider delivers documentation and testing results from a trusted independent testing organization to satisfy the Trusted Cloud Provider criteria for layers 1-8 of the CIEM and is compliant with all mandatory controls for Appendix A for those layers. A number of both Trusted and Non-Trusted Peer Cloud Consumers are present within the

cloud infrastructure at layers 6-8. Figure B shows the resulting mandatory encryption model. Since layer 5 is a shared resource only with a Trusted Peer Consumer, encryption is not required at that layer, but is required on layers 6-8 due to the presence within the infrastructure of a Non-Trusted Peer Cloud Consumer.

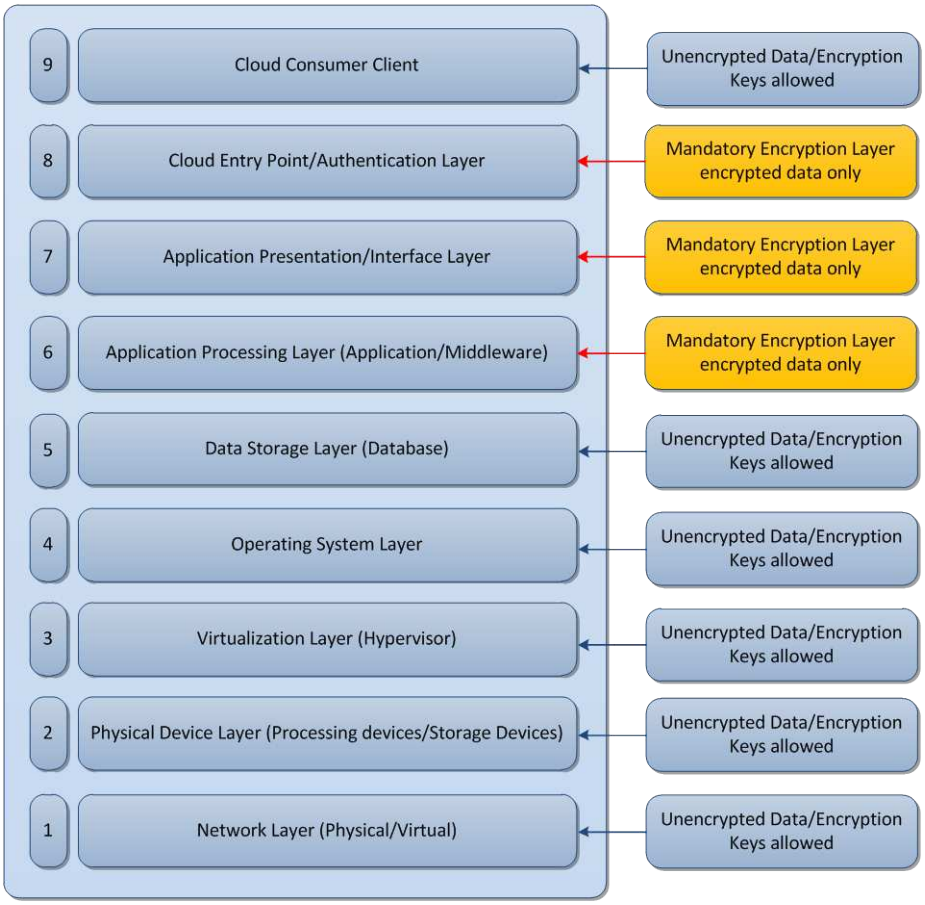

Figure B-4 PaaS encryption requirements

4.6.3 Infrastructure-as-a-Service (IaaS) Example

In the Infrastructure-as-a-Service example, we will examine a typical Cloud Provider model for delivery of an on-demand general purpose computing platform.

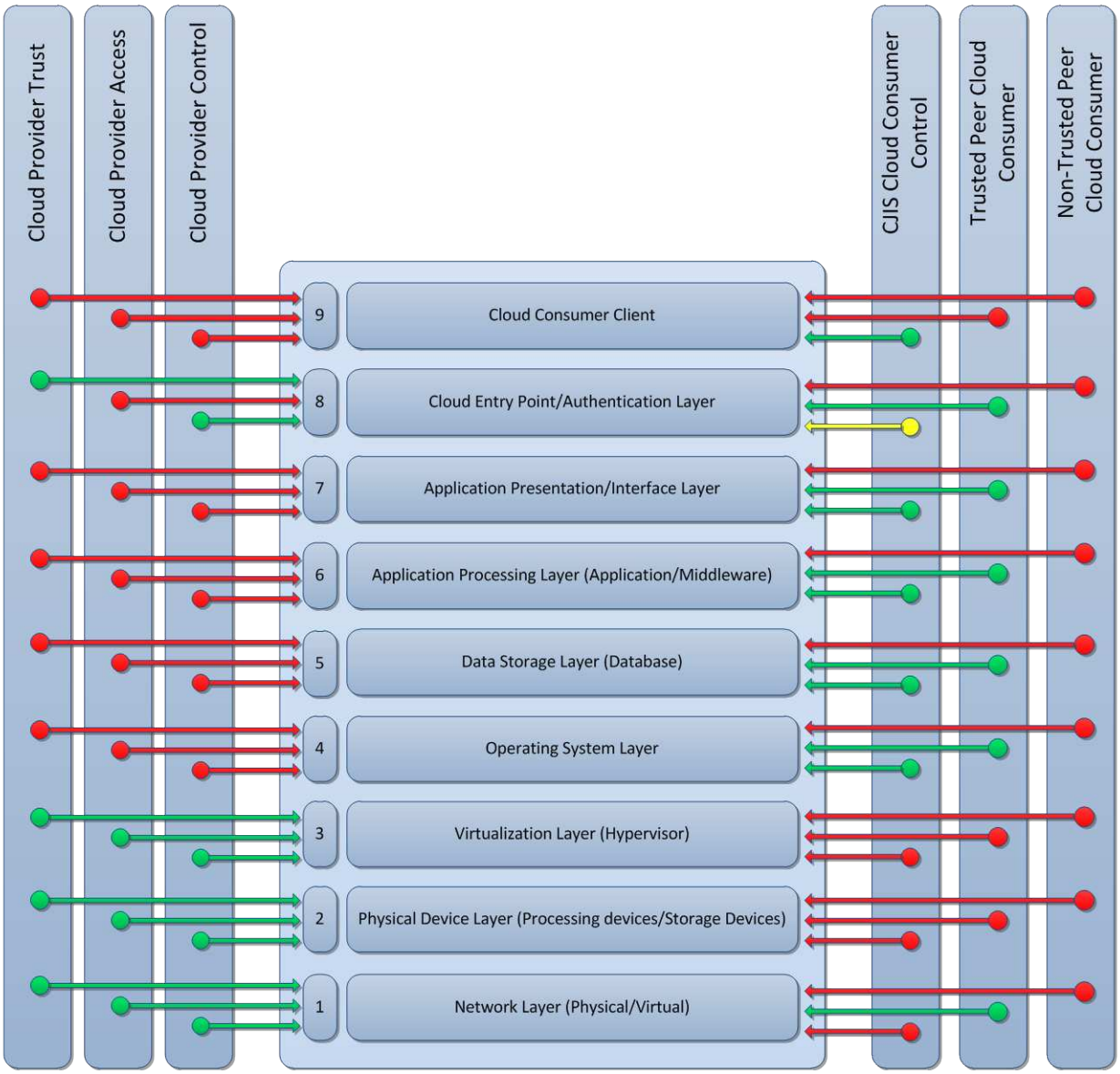

Figure B-5 IaaS encryption requirements

In this example we see a cloud architecture based on providing on-demand general purpose computing resources. The customer can choose and install their operating system and any applications or software installed. In this case the Cloud Provider controls only layers 1-3 and portions of layer 8 of the CIEM. Since the Provider meets the criteria for a Trusted Provider on layers 1-3 and 8, mandatory, and only Trusted Peer Cloud Consumers are determined to be in the environment, mandatory encryption is only required between the Consumer client and through the Cloud Provider boundary (layer 8). For this example, assume the actual application authentication occurs at layer 7 (typical for this model) and the Cloud Provider control of layer 8

does not expose any application access credentials to the provider. Figure B-6 shows the resulting encryption requirements for this model, assuming all mandatory controls from Appendix A are being met by both the provider and consumer.

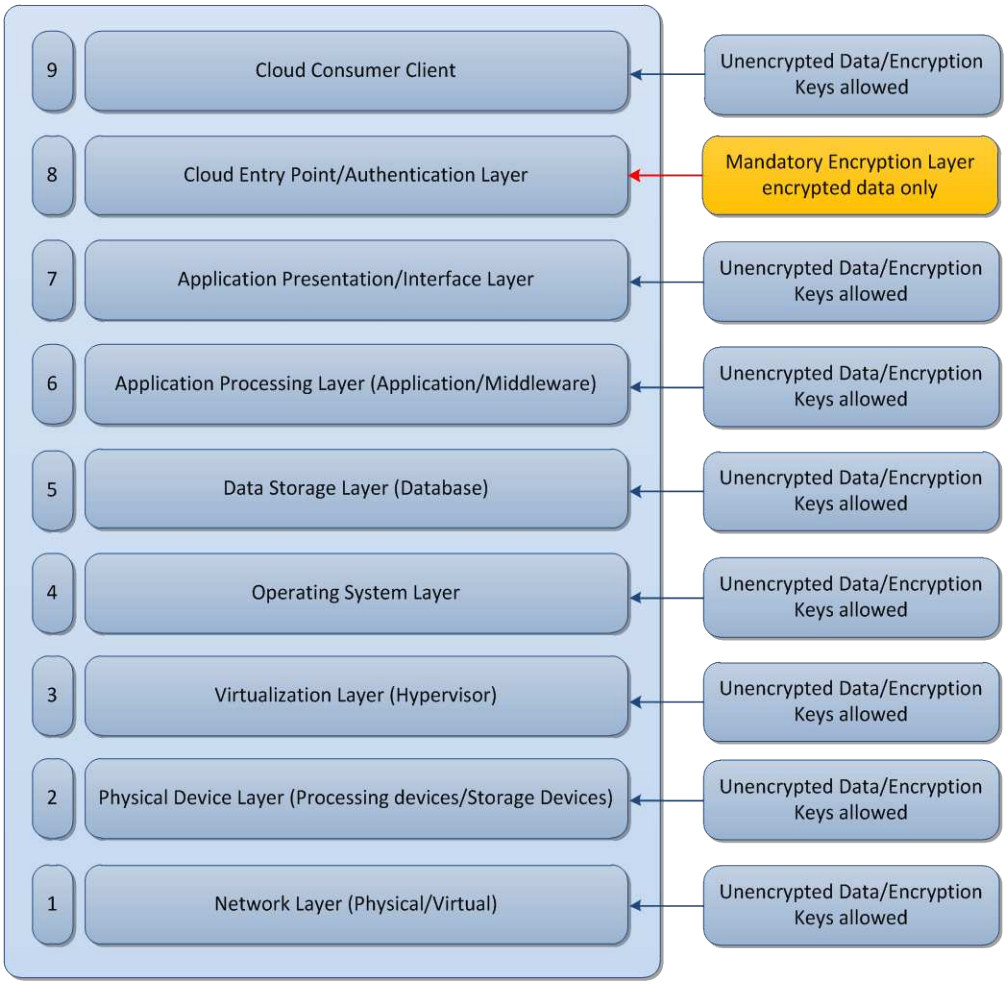

Figure B-6 IaaS encryption requirements

Appendix C: Definitions and Acronyms

Definitions:

Cloud Provider: A provider of Cloud services or applications. May be a single provider, or a combination of a primary provider from whom the services are contracted and one or more third-party providers that support the cloud infrastructure.

Trusted Cloud Provider: A Cloud Provider that has provided documentation and testing to show compliance with CJIS criteria for one or more layers in the CIEM. Provider trust is determined for each layer of the CIEM allowing a provider to be 'Trusted' at one layer and 'Non-Trusted' at another.

Non-Trusted Cloud Provider: A Cloud Provider unable or unwilling to provide sufficient documentation, testing, or auditing to satisfy CJIS controls for one or more layers of the CIEM. Provider trust is determined for each layer of the CIEM allowing a provider to be 'Trusted' at one layer and 'Non-Trusted' at another.

Peer Cloud Consumer: A customer of a Cloud Provider that has some level of access or control to the same layer of the Cloud Provider infrastructure on which CJIS data may be accessible.

Trusted Peer Cloud Consumer: A Peer Cloud Consumer that has provided documentation and testing to show compliance with CJIS criteria for one or more layers in the CIEM. Trusted Peer Cloud Consumers are typically government agencies, but may be commercial entities that have undergone US Government System Authorization consistent with the CJIS policy. Peer Consumer trust is determined for each layer of the CIEM allowing a provider to be 'Trusted' at one layer and 'Non-Trusted' at another based on the specific controls for which they are compliant.

Non-Trusted Peer Cloud Consumer: A Peer Cloud Consumer unable or unwilling to provide sufficient documentation, testing, or auditing to satisfy CJIS controls for one or more layers of the CIEM. Peer Consumer trust is determined for each layer of the CIEM allowing a provider to be 'Trusted' at one layer and 'Non-Trusted' at another.

Acronyms:

CIEM	Cloud Infrastructure Evaluation Model
SLA	Service Level Agreement

Appendix D: References

A. Department of Justice / Federal Bureau of Investigation

1. Federal Bureau of Investigation - Criminal Justice Information Services (CJIS) Security Policy, Version 5.0, dated 02/09/2011
2. Federal Bureau of Investigation – FBI Statement on CJIS and Cloud Computing, dated February 2012
3. Department of Justice – DOJ Office of Community Oriented Policing Services Law Enforcement Tech Guide for Information Technology Security, dated 2006

B. Other Federal Agency Policies and Documents Investigated

1. Department of Homeland Security – DHS Sensitive Systems policy Directive 4300A, Version 8.0, dated March 14, 2011
2. Department of the Army – Army Regulation 380-5, Department of the Army Information Security Program, dated 29 September 2000
3. Department of the Navy – SECNAV MANUAL M-5510.36, Department of the Navy Information Security Program [Naval Criminal Investigative Service], dated June 2006
4. Department of Defense – DoD Manual 5200.01 Volume 3, DoD Information Security Program: Protection of Classified Information, dated February 24, 2012
5. U.S. Department of Commerce – DoC Office of the Chief Information Officer IT Privacy Policy, dated January 22, 2009
6. Department of Energy – DOE Order 471.6 Information Security, dated January 20, 2011
7. Department of Energy – DOE Manual 470.4 / with Change 1 Information Security Manual, dated June 20, 2011
8. Department of Veterans Affairs – VA Handbook 6500 Information Security Program, dated September 18, 2009

C. State and Local Policies Investigated

1. Commonwealth of Virginia – ITRM Policy SEC519-00, Virginia Information Technologies Agency (VITA) Information Security Policy, dated July 24, 2009

2. Commonwealth of Virginia – COV ITRM Guideline SEC507-00, Virginia Information Technologies Agency (VITA) Information Technology Data Protection Guide, dated April 18, 2007

3. State of Colorado – Office of Information Technology Data Strategy, dated January 26, 2010

4. State of Arizona – Government Information Technology Agency (GITA) Statewide Policy P100 Revision 2.0 Information technology, dated October 17, 2008

5. Yuma County, Arizona – Yuma County, Arizona Information Security Policy, dated April 13, 2006

6. City of Seattle, Washington – City of Seattle Information Systems Security Policy, dated January 1, 2007

D. Other Resources Investigated

1. The White House – Office of the Chief Information Officer of the United States Federal Cloud Computing Strategy, dated February 8, 2011

2. National Institute of Standards and Technology - NIST Special Publication800-146 Draft Cloud Computing synopsis and Recommendations, dated May 2011

3. National Institute of Standards and Technology - NIST Special Publication 800-60 Volumes 1 and 2 Guide for mapping types of Information and Information Systems to Security Categories, dated August 2008

4. National Institute of Standards and Technology - NIST Special Publication 800-53 Recommended Security Controls for Federal Information systems and Organizations, dated August 2009

5. National Institute of Standards and Technology - NIST Special Publication 800-32 Introduction to Public key Technology and the Federal PKI Infrastructure, dated 20 February 2001

6. National Institute of Standards and Technology - FIPS PUB 200 Minimum Security requirements for federal Information and Information Systems, dated March 2006

7. National Institute of Standards and Technology - FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems, dated February 2004