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

This document outlines the specific security policies and practices for Evidence.com and how they are compliant with the CJIS Security Policy, version 5.5. Also, responses are provided to questions posed in the CJIS Security Policy Appendix G.3 Cloud Computing.

In addition to the details explained in this document, TASER International contractually commits to the CJIS Security Policy with customers by incorporating the CJIS Security Addendum within the TASER Master Services Purchasing Agreement.

CJIS Security Policy, Version 5.5	TASER Policies, Practices, and Standards
5.1 - Policy Area 1: Information Exchange Agreements	
5.1.1 - Information Exchange	The TASER Master Services Purchasing Agreement (MSPA) outlines the data protection roles, responsibilities, and data ownership.
5.1.1.1 - Information Handling	TASER International maintains policies and practices for Evidence.com for securely handling information
5.1.1.2 to 5.1.4: State and Federal Agency User Agreements; Criminal Justice Agency User Agreements; Interagency and Management Control Agreements; Private Contractor User Agreements and CJIS Security Addendum; Agency User Agreements, Outsourcing Standards for Non-Channelers; Monitoring, Review, and Delivery of Services; Managing Changes to Service Providers; Secondary Dissemination; Secondary Dissemination of Non-CHRI CJI;	TASER acknowledges and abides by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is included by reference in the TASER MSPA which contractually commits TASER to the CJIS Security Policy requirements. CJIS Security Addendum Certification pages are maintained for each authorized TASER employee and are available to customers.

5.2 - Policy Area 2: Security Awareness Training	
5.2.1 to 5.2.1.3: Awareness Topics; All Personnel; Personnel with Physical and Logical Access; Personnel with Information Technology Roles;	TASER International maintains a comprehensive security awareness program. TASER leverages the product CJIS Online to deliver CJIS-specific training for personnel working on the Evidence.com services.
5.2.2 – Security Training Records	TASER International maintains records to ensure all required personnel complete security awareness training. Records of training can be provided to customers.
5.3 - Policy Area 3: Incident Response	
5.3.1 – Reporting Information Security Events	TASER International maintains comprehensive security incident response plans for Evidence.com include reporting to appropriate parties.
5.3.2 – Management of Information Security Incidents	TASER International maintains security incident response policies and practices for Evidence.com.
5.3.2.1 – Incident Handling	TASER International maintains security incident response procedures and capabilities for Evidence.com.
5.3.2.2 – Collection of Evidence	The TASER International security incident response practices for Evidence.com include requirements to collect and maintain appropriate evidence, when necessary.
5.3.3 – Incident Response Training	The TASER International security awareness training for Evidence.com includes security incident response roles and responsibilities, including reporting expectations.
5.3.4 – Incident Monitoring	TASER International documents and tracks security incidents for Evidence.com and maintains such documentation to meet this requirement.
5.4 - Policy Area 4: Auditing and Accountability	
5.4.1 to 5.4.1.1.1: Auditable Events and Content (Information Systems); Events; Content	Evidence.com systems are configured to log all required events, and more, to a central logging system. Additionally, within the Evidence.com application, logs are generated and secured that detail all access to evidence data. Robust evidence audit reports are available to customers.
5.4.2 – Response to Audit Processing Failures	The Evidence.com central logging system is configured to alert administrators of any log collection or processing failures.

5.4.3 – Audit Monitoring, Analysis, and Reporting	TASER International employs advanced detection and analysis capabilities of system events for Evidence.com. This includes automated detection and alerts for unusual activity or attacks.
5.4.4 – Time Stamps	The Evidence.com central logging system collects event generation time, and event received time.
5.4.5 – Protection of Audit Information	The Evidence.com central logging system is protected, and access to the logged information is limited to authorized administrators. Logs cannot be edited or changed.
5.4.6 – Audit Record Retention	Evidence.com central log data is maintained for at least 1 year.
5.4.7 – Logging NCIC and III Transactions	Not applicable to Evidence.com security practices.
5.5 - Policy Area 5: Access Control	
5.5.1 – Account Management	TASER International maintains account management policies and practices for Evidence.com, including quarterly account validation.
5.5.2 – Access Enforcement	TASER International maintains account management practices and access control policies for Evidence.com to ensure access is limited to authorized accounts.
5.5.2.1 – Least Privilege	TASER International access controls for Evidence.com are designed according to the principle of least privilege.
5.5.2.2 – 5.5.5: System Access Control; Access Control Criteria; Access Control Mechanisms; Unsuccessful Login Attempts; System User Notification; Session Lock	Evidence.com access control mechanisms are maintained in compliance with the specific CJIS security requirements.
5.5.6 – Remote Access	TASER International maintains policies and practices for Evidence.com that limit remote access to only required individuals, via managed VPN connections requiring 2-factor authentication.
5.5.6.1 – Personally Owned Information Systems	TASER International maintains requirements for the use of personally owned devices.
5.5.6.2 – Publically Accessible Computers	Evidence.com back-end system administration is prohibited from public access computers.
5.6 - Policy Area 6: Identification and Authentication	
5.6.1 – Identification Policy and Procedures	TASER International maintains policies and practices for Evidence.com for identifying and authenticating users before allowing access.

5.6.1.1 – 5.6.2: Use of Originating Identifiers in Transactions and Information Exchanges; Authentication Policy and Procedures	Not applicable to Evidence.com security practices.
5.6.2.1 – 5.6.2.1.2: Standard Authenticators; Password; Personal Identification Number (PIN)	Evidence.com authentication mechanisms are maintained in compliance with the specific CJIS security requirements.
5.6.2.2 – 5.6.2.2.2: Advanced Authentication; Advanced Authentication Policy and Rational; Advanced Authentication Decision Tree	Evidence.com requires at least 2-factor authentication for all system administration access. Additionally, advanced authentication is available for customer accounts.
5.6.3 – 5.6.3.2: Identifier and Authenticator Management; Identifier Management; Authenticator Management; Assertions	TASER International maintains policies and practices for Evidence.com for Identifier and Authenticator management.
5.6.4 - Assertions	TASER International utilizes a combination of internal and trusted external certification authorities for validating individual identities. Certificates are issued internally through an internal trusted authority. For external access, commercial CA's are used. Private keys and certificates are stored and distributed securely.
5.7 - Policy Area 7: Configuration Management	
5.7.1 – Access Restrictions for Changes	TASER International limits Evidence.com system changes to only authorized administrators.
5.7.1.1 – Least Functionality	Evidence.com system configurations are designed according to the principle of least functionality.
5.7.1.2 – Network Diagram	TASER International maintains a current system diagram for Evidence.com.
5.7.2 – Security of Configuration Documentation	Evidence.com system configuration documentation is classified as confidential, and protected accordingly.
5.8 - Policy Area 8: Media Protection	
5.8.1 – Media Storage and Access	TASER International ensures digital evidence in Evidence.com is stored in physically secure and controlled locations.
5.8.2 – 5.8.2.1: Media Transport; Electronic Media in Transit	TASER International maintains practices for securely handling Evidence.com data, when in transit.
5.8.2.2 – Physical Media in Transit	Information from Evidence.com is not put into physical form.
5.8.3 – Electronic Media Sanitization and Disposal	TASER International maintains practices for sanitizing and disposing of electronic media.

5.8.4 – Disposal of Physical Media	Evidence.com does not store or manage physical evidence or physical documents containing CJI.
5.9 - Policy Area 9: Physical Protection	
5.9.1.1 – Security Perimeter	Evidence.com defines and controls the physically secure perimeter.
5.9.1.2 – Physical Access Authorizations	TASER International ensures physical access is limited to authorized personnel.
5.9.1.3 – Physical Access Control	TASER International ensures physical access is limited to authorized personnel, including the use of Iris and RFID access control systems at TASER facilities.
5.9.1.4 – Access Control for Transmission Medium	TASER International protects access to transmission lines.
5.9.1.5 – Access Control for Display Medium	TASER International controls display medium to prevent unauthorized viewing of CJI.
5.9.1.6 – Monitor Physical Access	TASER International maintains policies and practices for monitoring physical access, and responding to suspicious events.
5.9.1.7 – Visitor Control	TASER International maintains policies and practices for controlling visitor access.
5.9.1.8 – Delivery and Removal	TASER International maintains policies and practices for controlling information system-related items.
5.9.2 – Controlled Area	TASER International maintains policies and practices for Evidence.com related to physical protection.
5.10 - Policy Area 10: System and Communication Protection and Information Integrity	
5.10.1 – Information Flow Enforcement	TASER International maintains a range of capabilities for controlling data flows in Evidence.com, including firewalls, proxies, and load balancers.
5.10.1.1 – Boundary Protection	TASER International maintains controls to protect and monitor boundaries of Evidence.com. These include firewalls, network segmentation, proxies, and intrusion detection systems.
5.10.1.2 – Encryption	Evidence data transmitted and stored in Evidence.com is encrypted with 128 bits or stronger. FIPS 140-2 approved encryption ciphers (or stronger) are used, including AES 256, and RSA 2048. TASER International maintains policies and practices for Evidence.com for encryption key and certificate management.

5.10.1.3 – Intrusion Detection Tools and Techniques	Evidence.com employs advanced detection and analysis capabilities of system events. This includes automated detection and alerts for unusual activity or attacks.
5.10.1.4 – Voice over Internet Protocol	Not applicable to Evidence.com security practices.
5.10.1.5 – Cloud Computing	The TASER International Information Security Program is designed to provide a high level of protection against current and emerging threats. This includes meeting or exceeding the CJIS security standards. The TASER MSPA outlines the data protection roles, responsibilities, data ownership, and allowable uses for data.
5.10.2 – Facsimile Transmission of CJI	Not applicable to Evidence.com security practices.
5.10.3 – Partitioning and Virtualization	Evidence.com is operated on industry-leading Infrastructure as a Service (IaaS) partners that provide secure partitioning and virtualization capabilities.
5.10.3.1 – Partitioning	Evidence.com uses many partitioning and segmentation methods for security purposes. These include network segmentation, OS separation, firewalls, and logical access separation.
5.10.3.2 – Virtualization	Evidence.com operates on secure virtualized environments that meet the additional virtualization controls defined within the CJIS Security Policy.
5.10.4.1 – Patch Management	TASER International maintains policies and practices for Evidence.com for patch management.
5.10.4.2 – Malicious Code Protection	TASER International maintains policies, practices and technologies for Evidence.com to protect against malicious software.
5.10.4.3 – Spam and Spyware Protection	TASER International maintains policies, practices and technologies for Evidence.com to protect against spam and phishing attacks.
5.10.4.4 – Security Alerts and Advisories	TASER International maintains policies and practices for disseminating appropriate security information to personnel, customers, and other stakeholders.
5.10.4.5 – Information Input Restrictions	Not applicable to Evidence.com security practices.
5.11 - Policy Area 11: Formal Audits	
5.11.1.1 to 5.11.3 – Triennial Compliance Audits by the FBI CJIS Division; Triennial Security Audits by the	TASER International adheres to the audit requirements of the FBI CJIS Security Policy.

FBI CJIS Division; Audits by the CSA; Special Security Inquiries and Audits	
5.12 - Policy Area 12: Personnel Security	
5.12.1 – Personnel Security Policy and Procedures	TASER International maintains policies and practices for ensuring all Evidence.com personnel are trustworthy and competent to handle sensitive data and systems.
5.12.1.1 – Minimum Screening Requirements for Individuals Requiring Access to CJI	TASER International maintains policies and practices for ensuring all Evidence.com personnel are trustworthy and competent to handle sensitive data and systems. Authorized TASER personnel are available for state of residence and national fingerprint-based record checks at either the state or local level.
5.12.1.2 – Personnel Screening for Contractors and Vendors	TASER International maintains policies and practices for ensuring all Evidence.com personnel are trustworthy and competent to handle sensitive data and systems. Authorized TASER personnel are available for state of residence and national fingerprint-based record checks at either the state or local level.
5.12.2-3 – Personnel Termination; Personnel Transfer	TASER International maintains policies and practices for access management related to termination or transfer of personnel.
5.12.4 – Personnel Sanctions	TASER International maintains a formal sanction process for personnel failing to comply with established security policies and practices.
5.13 - Policy Area 13: Mobile Devices	
5.13.1 – 5.13.10: All 802.11x Wireless Protocols; Cellular; Cellular Service Abroad; Voice Transmissions Over Cellular Devices; Bluetooth; Mobile Device Management (MDM); Wireless Device Risk Mitigation; Legacy 802.11 Protocols; System Integrity; Patching/Updates; Malicious Code Protection; Physical Protection; Personal Firewall; Incident Response; Auditing and Accountability; Access Control; Wireless Hotspot Capability; Identification and Authentication; Local Device Authentication; Device Certificates	The Evidence.com back-end system environment is not directly accessible via a wireless network or via cellular devices. Evidence.com data is not transferred via Bluetooth.

CJIS Security Policy Appendix G.3 Cloud Computing

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

Appendix 6.3 Questions	Evidence.com Policies, Practices, and Standards
Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)	TASER International maintains policies and practices for Evidence.com that limit remote access to only required individuals, via managed VPN connections requiring at least 2-factor authentication.
Will advanced authentication (AA) be required for access to CJI within a cloud environment? (5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale)	Evidence.com requires at least 2-factor authentication for all system administration access. 2-factor authentication is available for individual customer accounts.
Does/do any cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9 Physical Protection)	TASER International regularly reviews the specific security practices and audit results documented by AWS to ensure they meet the relevant portions of the CJIS Security Policy.
Are the encryption requirements being met? (5.10.1.2 Encryption) • Who will be providing the encryption as required in the CJIS Security Policy? (client or cloud service provider) • Is the data encrypted while at rest and in transit?	Evidence data transmitted and stored in Evidence.com is encrypted with 128 bits or stronger. FIPS 140-2 approved encryption ciphers (or stronger) are used, including AES 256, and RSA 2048. TASER International maintains policies and practices for Evidence.com for encryption key and certificate management.
What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response) • Will the cloud subscriber be notified of any incident? • If CJI is compromised, what are the notification and response procedures?	TASER International maintains comprehensive security incident response plans for Evidence.com including reporting to appropriate parties.
Is the cloud service provider a private contractor/vendor? • If so, they are subject to the same screening and agreement requirements as any other	TASER acknowledges and abides by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is included by reference in the TASER MSPA which contractually commits TASER to the CJIS Security

private contractors hired to handle CJI? (5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors)	Policy requirements. CJIS Security Addendum Certification pages are maintained for each authorized TASER employee and are available to customers. TASER International maintains policies and practices for ensuring all Evidence.com personnel are trustworthy and competent to handle sensitive data and systems. Authorized TASER personnel are available for state of residence and national fingerprint-based record checks at either the state or local level.
Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? (5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)	TASER International adheres to the audit requirements of the FBI CJIS Security Policy.
How will event and content logging be handled? (5.5 Policy Area 4, Auditing and Accountability) • Will the cloud service provider handle logging and provide that upon request?	Evidence.com systems are configured to log all required events from Policy Area 4, and more, to a central logging system.

[v20160818]