This document outlines the specific security features for EVIDENCE.com, as well as the general security policies and practices related to TASER International's management of EVIDENCE.com

TASER International recognizes the need for law enforcement agencies to adhere to their regulatory obligations when using EVIDENCE.com. Knowing this key requirement, EVIDENCE.com was designed and is operated to ensure that it aligns with the FBI's CJIS Security Policy. TASER International can provide additional documentation to demonstrate how EVIDENCE.com is aligned with the CJIS Security Policy. Contact your TASER sales representative for more details.

TASER International has partnered with Amazon Web Services (AWS) to provide a secure, extremely scalable and highly reliable infrastructure to operate EVIDENCE.com. This partnership includes a shared commitment to ensure the infrastructure operating EVIDENCE.com is aligned with the CJIS Security Policy. Additionally, AWS complies with many security assurance and certification programs and undergoes regular security audits. These include SOC 1/SSAE 16, SOC 2 & 3, CJIS, ISO 27001, FedRAMP, PCI, FISMA, and FIPS 140-2. TASER International regularly reviews the specific security practices and audit results documented by AWS to ensure the highest standards are met.

More details on AWS security and compliance practices and assurance programs can be found here http://aws.amazon.com/security and here http://aws.amazon.com/compliance.

EVIDENCE.com: Security Features

EVIDENCE.com provides many security features and capabilities to enable customers to securely manage digital evidence. EVIDENCE.com customers have varying risk profiles, and different security needs. Many of the following security features can be enabled or disabled by customers as needed, or can be changed to meet a specific level of risk. The default settings for these security features were chosen to provide a strong level of security, while still maintaining flexibility and convenience. Customers are encouraged to evaluate these features and align them with their own unique needs.

Access Control
EVIDENCE.com includes many features to provide robust access control. • Customizable password length & complexity requirements • Customizable lockout (failed login) limits • Customizable session timeout settings • Mandatory challenge questions when authenticating from new locations • Multiple multi-factor authentication options (one time code via SMS, Email, or Phone call-back) • Role-based permission management • Device-level permission management (for example, allow specific users to use the web-based interface, but not the mobile application) • Restrict access to defined IP ranges (limit access to approved office locations)

Encryption

EVIDENCE.com uses strong encryption to protect evidence data in transit and at rest.
• FIPS 140-2 approved encryption ciphers (or stronger)
• Robust SSL/TLS implementation for data in transit.
  ○ RSA 2048 bit key
  ○ TLS 1.2 with 256 bit connection
  ○ Perfect Forward Secrecy
• 256 bit AES encryption for evidence data in storage

Evidence Integrity
EVIDENCE.com includes features to ensure the integrity and authenticity of digital evidence. These features ensure the evidence meets chain-of-custody requirements and can be proven to be authentic and free from tampering. • Forensic fingerprint of each evidence file using industry standard SHA-1 hash function. Integrity is validated before and after upload to ensure no changes occurred during transmission. • Full tamper-proof evidence audit records. Logs the *when*, *who*, and *what* for each evidence file. These records cannot be edited or changed, even by account administrators. • Original evidence files are never altered; even when derivative works (video segments) are created. • Deletion protection, including deletion approval workflows, deletions notification emails, and a deletion remorse period to recover accidently deleted evidence files.

EVIDENCE.com: General Security Practices

Access Management
TASER International maintains account management policies and practices for EVIDENCE.com. These include access control standards, account management procedures, regular account and permission validation, the principle of least privilege, and remote access policies that include 2-factor authentication for all administrative activities.
Security Monitoring & Response
TASER International maintains security monitoring and incident response policies and practices for EVIDENCE.com. These include robust attack detection, incident response procedures, logging and monitoring standards, and reporting to appropriate parties.
Vulnerability Management
TASER International maintains vulnerability management policies and practices for EVIDENCE.com. These include regular vulnerability scans and penetration tests, awareness of newly disclosed vulnerabilities and security patches, and vulnerability remediation procedures.
Configuration Management
TASER International maintains configuration management policies and practices for EVIDENCE.com. These include system configuration standards, patch management procedures, malicious software protection, and secure architecture standards.

Data Protection

TASER International maintains policies and practices to protect data stored in EVIDENCE.com. These include a data classification standard, data handling and transfer practices, encryption standards, and key management procedures.

Personnel

TASER International maintains policies and practices to ensure trustworthy and competent people are working with EVIDENCE.com. These include criminal background checks, and regular security training that includes recognizing and defending against the latest threats.

Physical Protection

TASER International maintains policies and practices for physical protection of EVIDENCE.com. These include biometric access controls for TASER facilities, physical access management procedures, and identification badge standards.

The EVIDENCE.com data centers are managed by Amazon Web Services (AWS). TASER regularly validates audit results of AWS security practices to ensure the data center physical security practices are robust and effective. AWS provides many layers of physical security for their data centers. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or AWS. All physical access to data centers by AWS employees is logged and audited routinely. See the AWS Security Whitepaper for more details: http://aws.amazon.com/security/

Risk Management

TASER International maintains policies and practices for risk management of EVIDENCE.com. These include various types of risk assessments, practices to identify and address high-risk issues, regular assessments to test security control effectiveness, and security metrics for continuous monitoring.

Third-Party Security Management

TASER International maintains policies and practices for vendor security management related to EVIDENCE.com. These include vendor security evaluations and review of audit reports to ensure security and compliance expectations are being met.

Cyber Insurance

TASER International has a comprehensive cyber insurance policy which provides insurance coverage for a breach of EVIDENCE.com and covers professional services liability, privacy liability, privacy regulatory liability, regulatory fines and penalties, and security liability. TASER International is able to issue an insurance certificate to its customers naming them as additional insureds under our cyber insurance policy for added protection.

[Version 3.0 - Released January 7, 2015]