CJIS TECHNICAL AUDIT 5.9.4 TRACKING SHEET

Agency Name

Date of Non-Compliance

Date Corrective Action Plan (CAP) due

CJISSECPOL V.5.9.4 - Sanctionable Controls	Audit Compliancy Status In/Out	Explanation	Actions taken or plan (including the timeline) to bring these items into compliance	Date Compliance Achieved
INFORMATION EXCHANGE AGREEMENTS				
5.1.1.4 - INTERAGENCY & MCAs				
5.1.1.5 SECURITY ADDENDUMS				
AWARENESS AND TRAINING				
AT-1 POLICY AND PROCEDURES				
AT-2 LITERACY TRAINING AND AWARENESS				
AT-3 ROLE-BASED TRAINING				
AT-4 TRAINING RECORDS				
INCIDENT RESPONSE				
IR-1 POLICY AND PROCEDURES				
IR-2 INCIDENT RESPONSE TRAINING				
IR-4 INCIDENT HANDLING				
IR-5 INCIDENT MONITORING				
IR-6 INCIDENT REPORTING				
IR-7 INCIDENT RESPONSE ASSISTANCE				
IR-8 INCIDENT RESPONSE PLAN				
AUDITING AND ACCOUNTABILITY				
AU-2 EVENT LOGGING				
AU-3 CONTENT OF AUDIT RECORDS				
AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES				
AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING				
AU-8 TIME STAMPS				
AU-9 PROTECTION OF AUDIT INFORMATION				
AU-11 AUDIT RECORD RETENTION				
ACCESS CONTROL				
AC-2 ACCOUNT MANAGEMENT				
AC-2 (4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS				
AC-3 ACCESS ENFORCEMENT				
AC-4 INFORMATION FLOW ENFORCEMENT				
AC-5 SEPARATION OF DUTIES				
AC-6 LEAST PRIVILEGE				
AC-6 (1) AUTHORIZE ACCESS TO SECURITY FUNCTIONS				
AC-6 (2) NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS				
AC-6 (5) PRIVILEGED ACCOUNTS				
AC-6 (7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES				
AC-6 (9) LOG USE OF PRIVILEGED FUNCTIONS				
AC-6 (10) PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS				

CJIS TECHNICAL AUDIT 5.9.4 TRACKING SHEET

AC-7 UNSUCCESSFUL LOGON ATTEMPTS				
AC-8 SYSTEM USE NOTIFICATION				
AC-11 DEVICE LOCK				
AC-11 (1) PATTERN-HIDING DISPLAYS				
AC-17 REMOTE ACCESS				
AC-18 WIRELESS ACCESS				
AC-18 (1) WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION				
AC-19 ACCESS CONTROL FOR MOBILE DEVICES				
AC-19 (5) ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE OR CONTAINER-BASED ENCRYPTION				
AC-20 USE OF EXTERNAL SYSTEMS				
AC-20 (1) USE OF EXTERNAL SYSTEMS | LIMITS ON AUTHORIZED USE				
AC-20 (2) USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES — RESTRICTED USE				
AC-21 INFORMATION SHARING				
IDENTIFICATION AND AUTHENTICATION				
IA-0 USE OF ORIGINATING AGENCY IDENTIFIERS IN TRANSACTIONS AND INFORMATION EXCHANGES				
IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)				
IA-4 IDENTIFIER MANAGEMENT				
IA-5 AUTHENTICATOR MANAGEMENT				
IA-5(1) AUTHENTICATOR MANAGEMENT | AUTHENTICATOR TYPES				
IA-5(2) AUTHENTICATOR MANAGEMENT | PUBLIC KEY-BASED AUTHENTICATION				
IA-5(6) AUTHENTICATOR MANAGEMENT| PROTECTION OF AUTHENTICATORS				
CONFIGURATION MANAGEMENT				
5.7.1.2 Network Diagram				
MEDIA PROTECTION				
MP-1 POLICY AND PROCEDURES				
MP-2 MEDIA ACCESS				
MP-4 MEDIA STORAGE				
MP-5 MEDIA TRANSPORT				
MP-6 MEDIA SANITIZATION				
MP-7 MEDIA USE				
PHYSICAL PROTECTION				
PE-2 PHYSICAL ACCESS AUTHORIZATIONS				
PE-3 PHYSICAL ACCESS CONTROL				
PE-4 ACCESS CONTROL FOR TRANSMISSION				
PE-5 ACCESS CONTROL FOR OUTPUT DEVICES				
PE-6 MONITORING PHYSICAL ACCESS				
PE-6 (1) MONITORING PHYSICAL ACCESS | INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT				
PE-17 ALTERNATE WORK SITE				

CJIS TECHNICAL AUDIT 5.9.4 TRACKING SHEET

SYSTEMS AND COMMUNICATIONS PROTECTION				
SC-2 SEPARATION OF SYSTEM AND USER FUNCTIONALITY				
SC-7 BOUNDARY PROTECTION				
SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY				
SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT				
SC-13 CRYPTOGRAPHIC PROTECTION				
SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES				
SC-28 PROTECTION OF INFORMATION AT REST				
FORMAL AUDITS				
5.11.1.2 Triennial Security Audits by the FBI CJIS Division				
PERSONNEL SECURITY				
5.12 Personnel Security				
5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI				
5.12.2 Personnel Termination and 5.12.3 Personnel Transfer				
5.12.4 Personnel Sanctions				
MOBILE DEVICES				
5.13 Mobile Devices				
5.13.1.1 All 802.XX Wireless Protocols				
5.13.1.4 Mobile Hotspots				
5.13.2 Mobile Device Management (MDM)				
5.13.3 Wireless Device Risk Mitigations				
5.13.4.3 Personal Firewall				
5.13.5 Incident Response (Mobile Devices)				
5.13.7.2 Advanced Authentication				
5.13.7.2.1 Compensating Controls				
SYSTEM AND SERVICES ACQUISITION				
SA-22 UNSUPPORTED SYSTEM COMPONENTS				
SYSTEM AND INFORMATION INTEGRITY				
SI-1 POLICY AND PROCEDURES				
SI-2 FLAW REMEDIATION				
SI-2 (2) FLAW REMEDIATION | AUTOMATED FLAW				
SI-3 MALICIOUS CODE PROTECTION				
SI-4 SYSTEM MONITORING				
SI-4 (2) SYSTEM MONITORING | AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS				
SI-4 (4) SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC				
SI-4 (5) SYSTEM MONITORING | SYSTEM-GENERATED ALERTS				
SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES				
SI-8 SPAM PROTECTION & SI-8 (2) SPAM PROTECTION|AUTOMATIC UPDATES				
SI-11 ERROR HANDLING				
SI-12 INFORMATION MANAGEMENT AND RETENTION				