AGENDA
Kansas Criminal Justice Information System (KCJIS)
Polices and Procedure Subcommittee
Tuesday September 8, 2020 10:00 – 12:00

Join Microsoft Teams Meeting

+1 785-414-8630   United States, Topeka (Toll)
Conference ID: 230 218 498#

Facilitator: Don Cathey, Kansas Highway Patrol; KCJIS Information Security Officer
Don.cathey@ks.gov  785-368-6518

10:00 Join Microsoft TEAMS meeting
Rollcall of attendees /verify subcommittee quorum.

Meeting Objectives:
Review the current KCJIS Policies and Procedures manual for required updates

1. To ensure continued compliance with FBI CJIS Security Policy revisions (version 5.9)
2. Discuss proposed changes to KCJIS specific policies and procedures to include in KCJIS version 5.9 as follows:
   a. Add language to the INTRODUCTION section to include by reference NLet's policies.
   b. Add language to 4.3 Personally Identifiable Information (PII) to clarify when PII obtained via the KCJIS may be used in the interest of public safety.
   c. Modify policy 5.3.1 Reporting Security Events to simplify and clarify who the agency shall initially report the incident to and in what time frame. Also add language to clarify roles and authorities of KBI and KHP personnel in the incident response process
3. Additional ad hoc discussions as arise.
5. Most recent changes to the CJIS Security Policy. Version 5.9

**SUMMARY OF CHANGES**

Version 5.9

**APB Approved Changes**

1. **Section 5.13.2 Mobile Device Management (MDM):** add clarifying language, Fall 2019, APB#18, SA#3, Mobile Device Management (MDM) Requirements in the CJIS Security Policy.

2. **Appendix II, Security Addendum:** add example of contract addendum, Fall 2019, APB#18, SA#7, Audit of Vendor Contracts with Authorized Criminal Justice Agencies (CJAs).

3. **NOTE:** There were no Spring 2019 APB actions.

**Administrative Changes**

1. **Section 5.6.2.2.2 Advanced Authentication Decision Tree:** updated the tree description to account for direct and indirect access to CJIS.

2. **Figures 9 and 10:** updated both figures to account for direct and indirect access to CJIS.

KEY TO APB APPROVED CHANGES (e.g. "Fall 2013, APB#11, SA#6, add language, Future CSP for Mobile Devices"): Fall 2013 – Advisory Policy Board cycle and year

APB# – Advisory Policy Board Topic number

SA# – Security and Access Subcommittee Topic number

Summary of change

**Topic title**

Between a Federal Government shutdown over budget in early 2019 that left no time to prepare for Spring sessions of Working Groups et al. and the desire to revamp the entire CSP. The changes to FBI CJIS Security Policy in 2019 are minimal.

Review of the 5.9 release yielded no immediate effects on KCJIS policy and procedures and could be incorporated into the KCJIS Policies and Procedures after a complete review.

---

5. Most recent changes to the CJIS Security Policy. Version 5.9

**APB Approved Changes**

1. **Section 5.13.2 Mobile Device Management (MDM):** add clarifying language, Fall 2019, APB#18, SA#3, Mobile Device Management (MDM) Requirements in the CJIS Security Policy.

**5.13.2 Mobile Device Management (MDM)**

Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency. Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time. User Agencies shall implement the following controls when directly accessing CJI from devices running a limited-feature operating system:

1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.

2. MDM with centralized administration configured and implemented to perform at least the following controls:
   - Remote locking of device
   - Remote wiping of device
   - Setting and locking device configuration
   - Detection of "tethered" and "jailbroken" devices
   - Enforcement of folder or disk level encryption
   - Application of mandatory policy settings on the device
   - Detection of unauthorized configurations
   - Enforcement of folder or disk level encryption
   - Ability to determine the location of agency-controlled devices
   - Automatic device wiping after a specified number of failed access attempts

**EXCEPTION:** An MDM is not required when receiving CJI from an indirect access information system (i.e. the system provides no capability to conduct transactional activities on state and national repositories, applications or services). However, it is incumbent upon the authorized agency to ensure CJI is delivered to the appropriate requesting agency or individual. The CSO will make the final determination of whether access is considered indirect.

KHP CJIS audits already assumed previous language ("Agencies") implied local agency responsibility for MDM.
5. **Most recent changes to the CJIS Security Policy. CHANGE IN AUDIT EMPHASIS**

**Private Sector entity (5.1.1.5) FBI CJIS Security Addendum (Policy Appendix H)**

Include by reference (and/or attachment) in actual contract.

---

**NO POLICY CHANGE (5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum)**

Only interpretation for AUDIT EMPHASIS Changed

From: Reviewing individual certification pages

To: Reviewing actual contract for inclusion of security addendum.

---

5. **Most recent changes to the CJIS Security Policy. Version 5.9**

APB Approved Changes

2. **Appendix H, Security Addendum**: add example of contract addendum, Fall 2019, APB#18, SA#7, Audit of Vendor Contracts with Authorized Criminal Justice Agencies (CJAs).

**APPENDIX H SECURITY ADDENDUM**

The following pages contain:

- The legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum;
- An example of a contract addendum;
- The Security Addendum itself;
- The Security Addendum Certification page.

To assist agencies with compliance of the new AUDIT EMPHASIS a sample amendment that originally appeared in CSP version 4.x was added in Appendix H. (Appendices aren’t official “policy” but should be used to ensure compliance with policy content)

If a brand-new contract, Language to the effect of subpoint d. in the sample must be included in the appropriate place of the contract.
5. Most recent changes to the CJIS Security Policy. Version 5.9

APB Approved Changes
Administrative Changes¹

1. Section 5.6.2.2.2 Advanced Authentication Decision Tree: updated the tree description to account for direct and indirect access to CJIS.
2. Figures 9 and 10: updated both figures to account for direct and indirect access to CJIS.

5.6.2.2.2 Advanced Authentication Decision Tree

The following AA Decision Tree, coupled with figures 9 and 10 below, assists decision makers in determining whether or not AA is required.

1. Is the access to CJ direct access or indirect access?
   a. If access is direct, proceed to question 2.
   b. If access is indirect, decision tree is completed. AA is not required.
2. Can request’s physical originating location be determined?
   If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 1.
   a. The IP address is attributed to a physical structure; or
   b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure.
   If neither (a) or (b) above are true then the answer is “no”. Skip to question number 5.

¹ Administrative changes are vetted through the Security and Access Subcommittee and not the entire APB process. They are NOT policy statements on their own accord. Rather they are grammatical, spelling, formatting corrections or changes intended to enhance the clarity and understanding of policy statements.

For further study

https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center/view
Please provide the following information when submitting a request for a policy review.

1. Clear statement of request
   Insert reference to NLets manual into KCJIS Policies and Procedures manual

2. How this is handled now (or description of problem being solved)
   NLets manual is available via the KCJIS web portal. Because NLets provides connections to state information not available directly via NCIC, it is a vital companion information system to NCIC and III for the administration of criminal justice. While similarities exist between NCIC and NLets, they are different and have their own operations manuals.

3. Scenario/example

4. Suggested solution
   Insert reference to The NLets manual (aka the NLets Wiki/Users Guide) into the KCJIS policies
   1. The Introduction and Overview section
   2. The actual policy INTRODUCTION section

5. Benefit to the criminal justice community
   The additional reference may provide those agencies who have questions and prefer to do their own research prior to contacting KCJIS agencies with a more complete list of suggested materials to review that may provide them with the answer they seek. Also is a reminder to all who may study the manual that NLets is a separate entity.

6. Impact on state system users, if known. (Time and resources)
   None

7. Importance/criticality

8. Contact Person
   Name: ___________________________ Phone: ___________________________
   Contact Email: ___________________________
Criminal Justice Agencies:

Proper Use of KCJIS

KCJIS shall be accessed on a need to know basis. KCJIS information may be accessed and used for any authorized purpose consistent with the inquiring agency’s responsibility. Improper access, use or dissemination of information provided through KCJIS is serious and may result in sanctions including, but not limited to, termination of services and/or criminal and civil penalties.

Policies and Procedures


1.3 Relationship to Local Security Policy and Other Policies

This document is a compendium of applicable policies in providing guidance on the minimum security controls and requirements needed to access FBI CJIS and KCJIS information and services. These policies include presidential directives, federal laws, FBI directives and the criminal justice community’s APB decisions. State, local, and Tribal CJA may implement more stringent policies and requirements. Appendix I contains the references while Appendix E lists the security forums and organizational entities referenced in this document.

The following documents are incorporated by reference and made part of this policy: (1) the NCIC 2000 Operating Manual; (2) Title 28, Code of Federal Regulations, Part 20; (3) the N-Dex Policy and Operating Manual, the NLets Manual (aka the NLets Wiki/Users Guide).

The ANNOTATIONS and GUIDANCE chapter of this KCJIS publication is intended to assist KCJIS users in the application of these policies. This will include explanations of current KCJIS governance interpretations and understandings of policies and regulations along with references to helpful resources. The required documentation for local policy and procedures listed in this manual and the NCIC operating manual shall be included in a local agency Standard Operating Procedures (SOP) manual. Refer to Part 2 (GUIDANCE) of this publication for further assistance.
REQUEST FOR KCJIS POLICY REVIEW

Please provide the following information when submitting a request for a policy review.

1. Clear statement of request
   Add specific conditions for how Personally Identifiable Information (PII) obtained via KCJIS systems can be used for public safety.

2. How this is handled now (or description of problem being solved)
   especially driver and vehicle information are obtained via KCJIS from non-CJIS sources as as KS Dept. of Revenue or through NLets from other states version of DMV/revenue. The access via KCJIS is possible by a MOA between KBI and KDOR that references several non-CJIS laws and regulations. Recent changes to that MOA now allow use beyond law enforcement to include public safety. KHP CJIS fields questions seemingly often on who CJAs can provide this PII to and how. Some agencies have strict policies restricting any sharing to NCJAs even with a valid need to know while others don't.

3. Scenario/example

4. Suggested solution
   FBI policy section 4.3 calls for agencies are to develop policies based on state and local privacy laws for handling extracted from CJI.

   Also add illustrative/example use cases at end of policy Area 4

5. Benefit to the criminal justice community
   The intent is to codify per FBI requirement allowed uses of CJI for official uses beyond law enforcement. Thus enabling agencies to know when they can disseminate further, promoting the interoperability required in today's operations.

6. Impact on state system users, if known. (Time and resources)
   No impact on systems. User agencies already have the access.

7. Importance/criticality

8. Contact Person Name: _____________________________ Phone: _____________________________
   Contact Email: ____________________________________________
4.3 Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an individual’s identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother’s maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

In the interest of public safety, PII obtained via KCJIS, may be shared with responders to public safety incidents under the following conditions:

1. The information being shared does not contain CHRI or otherwise link or imply a criminal history exists for any subject person(s).
2. Dissemination is subject to limitations outlined elsewhere in this policy manual and other regulations, policies and manuals previously included as part of this policy by reference.
3. An Information Exchange agreement is executed between the Agency accessing KCJIS and the responding agency receiving the information. The agreement shall outline the roles, responsibilities, dissemination methods and security controls to be used to ensure compliance to the policies and requirements described in this document.
4. Dissemination shall be logged according to Secondary Dissemination policy 5.1.3.
5. Security standards as described throughout this policy shall be used as appropriate for the information systems and dissemination methods.
6. Access controls exist to prevent unauthorized access to PII and to ensure personnel receiving the information are identified, authenticated and authorized in accordance with requirements described in these policies.
7. Information not pertinent to respondents’ mission shall be redacted prior to dissemination to ensure the release of only information required by the respondents to accomplish their public safety mission to include, but not be limited to, the following purposes:
   a. Verify identities of people or property requiring the attention of the respondents.
   b. Facilitate proper notification regarding people or property placed into the respondents’ custodial care as a result of the public safety incident (i.e.: relatives of people or registered owners of vehicles or other property).
c. For official reporting purposes

8. The information shall only be used within the scope of response to a single specific public safety incident and not repeated or re-used commercially or for personal curiosity or gain.

9. Misuse of information provided via KCJIS shall subject violators to disciplinary actions including possible fines and imprisonment as allowed by federal and state laws and regulations, such as but not limited to:

a. 18 USC CHAPTER 123 — Prohibition on release and use of certain personal information from state motor vehicle records (18 USC § 2721 -2725)

b. KSA 74-2012 Division of vehicles, records; disclosure; fees.

c. KSA 21-6002 Official misconduct.
Use Case 1 – Citizen inquiry
A citizen of Springfield went to the Springfield Police Department to request whether his new neighbor, who had been acting suspiciously, had an outstanding warrant. The Springfield Police Department ran an NCIC persons inquiry, which produced a response that included a Wanted Person File (non-restricted file) record and a Known or Appropriately Suspected Terrorist File (restricted file) record. The Springfield Police Department advised the citizen of the outstanding warrant, but did not disclose any information concerning the subject being a known or appropriately suspected terrorist.

Use Case 2 – PII to EMS Responder
During a traffic stop by City Police Department, the subject experiences a medical emergency, prompting the officer to request EMS be dispatched. EMS responds and takes over emergency medical care of the subject and transports them to a local hospital. Subsequently EMS requests PII of the subject to complete their required follow-up and reporting procedures. City PD transmits the subject’s driver license information to EMS over an encrypted circuit certified by NIST to meet FIPS 140-2.

Use Case 3 – PII to tow company
An abandoned vehicle is presenting a safety risk for other motorists. At the request of the County Sheriffs, a tow company contracted with the county is dispatched to remove the vehicle. The contract includes language to ensure proper use and security measures are in place to protect any vehicle information provided to the tow company. Vehicle registration information is relayed to the tow operator via cellular phone to facilitate verification of proper vehicle to be towed and then later used to notify the vehicle owner of its location.
KANSAS CRIMINAL JUSTICE INFORMATION SYSTEM
REQUEST FOR KCJIS POLICY REVIEW

Please provide the following information when submitting a request for a policy review.

1. Clear statement of request
   Modify KCJIS Security Event reporting policy to:
   1. Create single KCJIS Point of Contact (KBI) for local agency to report security incidents.
   2. Include a timeframe for intial reporting
   3. Clarify authorities of KBI and KHP roles in incident handling

2. How this is handled now (or description of problem being solved)
   Current policy states that local agencies are to promptly report to BOTH KBI and KHP. Promptly is a relative term and experience has shown that agencies miss reporting to one or the other of the state agencies.

3. Scenario/example
   Typically an agency discovers through anti-virus alert or ransomware notice that 1 or more devices have been compromised. They spend time trying to determine level of threat to KCJIS before reporting - sometime days pass before the KBI or KHP are notified. Then only KBI or KHP gets called, leaving the other KCJIS agency in the dark.

4. Suggested solution
   Correct language to simplify reporting POC and timeframe.
   See attachment of proposed changes. Addtions in underlined green, Deletions in red strike through

5. Benefit to the criminal justice community
   One less POC with a 24-7-365 capability. With some assurance that use case will be evaluated before disconnects occur.

6. Impact on state system users, if known. (Time and resources)
   minimal

7. Importance/criticality

8. Contact Person

   Name: Don Cathey, KHP Jared Meier, KBI
   Phone: ____________________
   Email: ____________________
   Fax: ____________________

KCJIS POLICY REVIEW REQUEST
Please return to: Kansas Highway Patrol CJIS Unit
122 SW 7th Street Topeka, KS 66603-3847
Email: khp.cjis@ks.gov
Fax: (785) 296-0958
Revised 11/1/2019
5.3 Policy Area 3: Incident Response

The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of a CJI-related incident to the FBI CJIS ISO.

Refer to Section 5.13.5 for additional incident response requirements related to mobile devices used to access CJI.

5.3.1 Reporting Security Events

The agency shall promptly report incident information to appropriate authorities. Security events including identified weaknesses associated with the event shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third-party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

KCJIS Security Incident, Event, and Security Event definitions and/or examples derived from the National Institute of Standards and Technology (NIST). Definitions for each are located in Appendix A – Terms and Definitions.

The individual at the local agency who observes or suspects a Security Incident shall immediately notify their agency supervisory personnel, who shall notify agency I.T. support, their agency LASO, and TAC. Steps shall be taken by the agency I.T. support, TAC and LASO to confirm, identify, contain, isolate, and document the incident as quickly as possible.

The LASO or TAC shall promptly notify their KHP Technical Security Auditor, and the KBI Help Desk when a Security Incident is suspected or has taken place, and the notification shall be made no later than 24 hours after initial discovery of the actual or suspected Security Incident. The local agency LASO or TAC shall also submit a completed KCJIS 139 Security Incident Notification form to their assigned KHP Technical Security Auditor as soon as possible. A KCJIS 139 Security Incident Notification form shall be completed and submitted to the agency’s KHP Technical Security Auditor as soon as possible.

The KBI may suspend the affected user and/or system(s) access to KCJIS resources, as a safeguard, when made aware of a Security Incident. The KHP shall work with the affected agency to determine the scope and potential vulnerability to KCJIS. When applicable, the KHP shall inform the KBI to reinstate the affected user and/or system(s) access once they determine the incident has been resolved; or when they determine the risk to KCJIS has been eliminated.

The KBI ISO, or designee(s) may authorize the suspension of any affected user and/or system(s) access to KCJIS resources, as a safeguard, when made aware of a Security Incident. They shall...
also develop procedures to ensure the KBI promptly notifies the KHP ISO, or designee of all reported KCJIS Security Incidents; including any actions taken to suspend access to KCJIS resources. These procedures shall also include steps to notify applicable local agencies of any actions taken to suspend their access to KCJIS resources.

The KHP ISO, or designee(s) shall develop procedures to coordinate with the local agency, and the KBI, to determine the scope of any reported incident(s), as well as the potential vulnerability to KCJIS. They should also develop procedures to ensure the prompt notification to the KBI Help Desk once it has been determined an incident has either been resolved or has been contained in a manner that eliminates the risk to KCJIS. The procedures shall also include a process for notifying the KBI, when applicable, to reinstate any suspended access. The KBI shall not reinstate access to KCJIS resources without authorization from the KHP ISO, or designee(s).

If an agency is unsure whether to report a specific event, they should promptly contact the KBI Help Desk for assistance in determining if the event is a Security Incident. Agencies should also consider notifying other potentially impacted entities regarding actual or suspected Security Incidents. These entities could include but are not limited to: CAD/RMS vendors, city/county IT representatives, and other connected agencies and/or organizations.

Examples of Security Incidents include, but are not limited to:

- A user’s credentials (e.g., Password, PIN, Token) have been, or are suspected to have been compromised.
- Users sharing credentials (e.g., Username, Password, PIN, Token) to access KCJIS resources.
- Antivirus software alerts when it detects that a host is infected with malware.
- Loss, theft, or unauthorized use of laptops, desktops, mobile devices, or other equipment used to process, store, or transmit CJI.
- An information system has been, or is suspected to have been compromised (e.g., ransomware infection, website defacement, abnormal pop-ups or notification banners, agency data suspected to have been breached).
- User transmits CJI to authorized recipient via email (unless secured in accordance with appropriate policies).

5.3.1.1 Reporting Structure and Responsibilities

5.3.1.1.1 FBI CJIS Division Responsibilities

The FBI CJIS Division shall:

1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
5.3.6 Sanctions

A sanction is a disciplinary measure from the State CSO or ISO directed against a specific Kansas criminal justice agency or its employees, as a result of being found in violation of KCJIS policies or FBI CJIS policies in the operation of its KCJIS system or use of information obtained from it. Penalties may vary depending on the severity of the violation. Sanctions include but are not limited to denial of new devices or system changes, loss of KCJIS access to an agency, and/or permanent loss of KCJIS access to specific individuals who are found to be in violation of KCJIS policies, procedures, and/or requirements.

5.3.6.1 When a sanction is placed on an agency, the sanctioning official (the ISO for security related matters, the State CSO for all other matters) KHP shall issue a written letter to the affected agency head documenting the sanction. Documentation shall include a description of the violation, how the agency failed to take the appropriate actions and a description of the sanction being levied. Copies of the letter shall be submitted to the KCJIS Committee Chairperson, and the KBI, and the CJIS CSO.

5.3.6.2 When a sanction is placed on an agency employee, the sanctioning official (the ISO for security related matters, the State CSO for all other matters) KHP shall issue a written letter to the affected individual(s) with a copy to the agency head documenting the sanction. This documentation shall include a description of the violation that occurred, and the sanction being levied. Copies of the letter shall be submitted to the KCJIS Committee Chairperson, the KBI ISO, the CJIS CSO, and all affected agencies.

5.3.6.3 Any appeal for the purpose of challenging a sanction shall be made in writing to the Superintendent of the Kansas Highway Patrol by the individual being sanctioned. Such letter shall state the following:

1. Admission or denial of the event leading to the sanction.
2. Any argument or evidence to why the penalty for the actions should be reconsidered.