

KCJIS Network Change Request

Agency Name _____ ORI _____

Current Physical Address _____ City/Zip _____

Anticipated date of change: _____ (Allow 45 business days for OITS changes)

Agency LASO: _____ Phone: _____

E-mail Address: _____

I.T. Contact: _____ Phone: _____

E-mail Address: _____

I.T. Agency or company: _____

The location of KCJIS access is changing:

New Physical Address: _____

City _____ Zip _____

The existing OITS connection will need to continue for _____ days after the change(s).

Current OITS Circuit ID: _____ Router ID: _____

Describe proposed changes to network security infrastructure below and attach a network schematic, KCJIS 105 Network Security Questionnaire, and KCJIS 232 Encryption Questionnaire.

Change Internet Service Provider (ISP) or Service levels

FROM: OITS (bandwidth _____ State Agency funded) Commercial ISP (Agency funded)

TO: OITS (bandwidth _____) Commercial ISP (Agency funded)

Current OITS Circuit ID: _____ Router ID: _____

If terminating an OITS connection, attach KCJIS155.

Other Changes as described below. List agencies and how they are affected by the change(s).

KCJIS Network Security Questionnaire

Agency Name _____ ORI _____
 LASO Name _____ phone _____
 LASO email _____
 I.T. Contact _____ phone _____
 I.T. email _____ I.T. Agency or Company Name: _____

How does your agency connect to KCJIS? (Check all applicable boxes below.)

- State of Kansas Office of Information Technology Services (OITS)
Does your agency have Management Control of a firewall between your network and the OITS network? YES NO
- Agency Procured Ground based Internet Service
- Agency Procured Wireless Service *(complete wireless supplemental questionnaire on page 3)*
- By way of another Agency or Entity Agency Name: _____

Is access allowed into your network containing CJJ from outside your physically secure location?

- None allowed
- Remote Access such as vendors or telecommuting¹
- Remote Access from branch offices or other agencies¹

¹Please provide agency policies and procedures for when and how remote access is allowed and a KCJIS 232 encryption questionnaire for each remote access method.

- Mobile Data Terminals - *complete KCJIS229 Mobile Data Device Questionnaire*
- Other – (describe :) _____

Are there devices in your network that contains CJJ that are used for unsolicited access from the internet or other outside sources (such as e-mail servers, web servers, FTP servers, etc.)? No Yes (show on network schematic)

What network firewall(s) are used? List all models and versions. *(See network schematic instructions below).* _____

If personal firewalls are used, list brand(s) and version(s): _____

Network Schematic Instructions Please provide a visual representation (schematic) of all wired networks containing CJJ.

1. Do not include any network resolvable addresses or device names.
2. Show a logical summary (don't list all devices) of workstations and servers by physical location groups, VLANs, or virtualized environment (hypervisors), and their connectivity within your local network containing CJJ.
3. Show all logical locations of access points to your network. Include connections to routers, firewalls, wireless access devices, or any other device that provide a path in or out of your network containing CJJ.
4. Indicate connections to non-criminal justice entities such as city or county departments or services like email.
5. Mark "FOR OFFICIAL USE ONLY" on the diagram and include agency name, ORI, and date submitted.

KCJIS Network Security Questionnaire

What brands & versions of Intrusion Detection tools does your agency use? _____

How often are your intrusion detection tools updated? _____

How are your intrusion detection tools updated? _____

Who monitors the intrusion detection tools? _____

What brands & versions of Anti-Virus/Malware protection does your agency use? _____

How often are your Anti-Virus/Malware definition lists updated? _____

Where do your devices get updates to the Anti-Virus/Malware definitions? _____

How often does your Anti-Virus software scan your devices entire hard drive? _____

How does your agency manage patches and updates to devices on your network containing CJI?

Please answer the following questions for all encryption products used by your agency.

KCJIS Provided Encryption

Agency will use the State-supplied SecuRemote client between agency devices and KCJIS. It is understood that, to protect the entirety of KCJIS, any device connected using this option may be disconnected from KCJIS in the event of a security incident involving the device.

Agency will use a site to site VPN configured between Agency network and KCJIS. It is understood that, to protect the entirety of KCJIS, the entire connection using this option may be disconnected from KCJIS in the event of a security incident involving any device

Agency Configured Encryption Product

Name of Product used to provide NIST/FIPS 140-2 encryption: _____

Name of cryptographic module performing the encryption: _____

Model and/or version # of cryptographic module performing the encryption: _____

This product will be deployed at the: _____ user device level _____ network device level to encrypt CJI;

While _____ **at rest** or _____ **in transit** outside Physically Secure Locations.

NIST Certificate Number(s) assigned to the cryptographic module: _____

Specific Encryption Algorithm Used _____ (3DES, AES, RSA etc.) Key size used _____

Please complete KCJIS232 Encryption Questionnaire for additional products.

KCJIS Network Security Questionnaire

Wireless Supplemental Questionnaire

Please answer the following questions to determine if your wireless implementation meets the 802.11 Wireless access requirements outlined in FBI and KCJIS policy area 5.13.1.1.

How many Wireless Access Points (WAPs) are in your network that contains CJJ? _____
(Please indicate all on the schematic)

Are all WAPs located in physically secure locations? No Yes

Can the WAPs be reached from outside your physically secure facilities? No Yes

What is the approximate range of your WAPs? _____

Has the management interface User ID been changed from factory default? No Yes

Is the management interface User ID unique from other administrative user IDs? No Yes

Do the password attributes for the management interface meet the following requirements?

At least 8 characters	<input type="checkbox"/> No <input type="checkbox"/> Yes	Expire within 90 days	<input type="checkbox"/> No <input type="checkbox"/> Yes
Not a dictionary word	<input type="checkbox"/> No <input type="checkbox"/> Yes	Not any of previous 10	<input type="checkbox"/> No <input type="checkbox"/> Yes
Not a proper name	<input type="checkbox"/> No <input type="checkbox"/> Yes	Not transmitted in the clear	<input type="checkbox"/> No <input type="checkbox"/> Yes
Not the same as the user ID	<input type="checkbox"/> No <input type="checkbox"/> Yes	Not displayed when entered	<input type="checkbox"/> No <input type="checkbox"/> Yes

Is the SSID set as the factory default? No Yes

Does the SSID identify the agency or location? No Yes

Is the SSID broadcast? No Yes

List all security features that are enabled on your WAPs: _____

Is the cryptographic module used NIST certified to meet the FIPS 140-2 standards?

No or Not used Yes - NIST cert. # _____ what is the encryption key size used? _____

Have the default encryption keys been changed? No Yes

Has AD HOC mode been disabled? No Yes

Are all nonessential protocols disabled? No Yes

Is HTTP disabled? Yes No If no, is it protected by authentication and encryption? No Yes

Is logging enabled? Not available No Yes

Please indicate on the network schematic how the wireless implementation is separated and insulated from any wired network containing CJJ.

KCJIS Encryption Questionnaire

Agency Name _____ ORI: _____

LASO: _____ I.T. Contact: _____

Email: _____ I.T. Email: _____

Phone: _____ I.T. Phone: _____

CJIS Security Policy requires the encryption of Criminal Justice Information (CJI) whenever saved or transmitted outside of Physically Secure Locations as defined in policy. The cryptographic module used must be certified by the National Institute of Standards and Technology (NIST) to meet the Federal Information Processing Standards (FIPS) encryption standard as outlined in FIPS publication 140-2. See the NIST CMVP website <http://csrc.nist.gov/groups/STM/cmvp/index.html> for more information including vendor lists.

Agencies may use products in combination to achieve CJIS security policy compliance. KCJIS and Agency products may be combined. For instance, a Mobile VPN product between MDT and local network can be used along with a site to site VPN to KCJIS for full transmission path encryption. Please note the following:

- SecuRemote may not be compatible for use with servers such as CAD/RMS.
- In the event of a security incident (such as a malware infection) the **connection** used to access KCJIS may be disconnected to protect the entirety of KCJIS, i.e.: single device using SecuRemote or a shared site to site VPN that affects several devices may need disconnected.

Please answer the following questions for all encryption products used by your agency.

KCJIS Provided Encryption

- Agency will use the State-supplied SecuRemote client between agency devices and KCJIS. It is understood that, to protect the entirety of KCJIS, any **device** connected using this option may be disconnected from KCJIS in the event of a security incident involving the device.
- Agency will use a site to site VPN configured between Agency network and KCJIS. It is understood that, to protect the entirety of KCJIS, the **entire connection** using this option may be disconnected from KCJIS in the event of a security incident involving any device

Agency Configured Encryption Product(s)

Name of Product used to provide NIST/FIPS 140-2 encryption: _____

Name of cryptographic module performing the encryption: _____

Model and/or version # of cryptographic module performing the encryption: _____

This product will be deployed at the: _____ user device level _____ network device level to encrypt CJI;

While _____ ***at rest*** / or _____ ***in transit*** outside Physically Secure Locations.

NIST Certificate Number(s) assigned to the cryptographic module: _____

Specific Encryption Algorithm Used _____ (3DES, AES, RSA etc.) Key size used _____

KCJIS Encryption Questionnaire

Agency Configured Encryption Product(s) continued

Name of Product used to provide NIST/FIPS 140-2 encryption: _____

Name of cryptographic module performing the encryption: _____

Model and/or version # of cryptographic module performing the encryption: _____

This product will be deployed at the: _____ user device level _____ network device level to encrypt CJI;

While _____ **at rest** / or _____ **in transit** outside Physically Secure Locations.

NIST Certificate Number(s) assigned to the cryptographic module: _____

Specific Encryption Algorithm Used _____ (3DES, AES, RSA etc.) Key size used _____

Name of Product used to provide NIST/FIPS 140-2 encryption: _____

Name of cryptographic module performing the encryption: _____

Model and/or version # of cryptographic module performing the encryption: _____

This product will be deployed at the: _____ user device level _____ network device level to encrypt CJI;

While _____ **at rest** / or _____ **in transit** outside Physically Secure Locations.

NIST Certificate Number(s) assigned to the cryptographic module: _____

Specific Encryption Algorithm Used _____ (3DES, AES, RSA etc.) Key size used _____

Name of Product used to provide NIST/FIPS 140-2 encryption: _____

Name of cryptographic module performing the encryption: _____

Model and/or version # of cryptographic module performing the encryption: _____

This product will be deployed at the: _____ user device level _____ network device level to encrypt CJI;

While _____ **at rest** or _____ **in transit** outside Physically Secure Locations.

NIST Certificate Number(s) assigned to the cryptographic module: _____

Specific Encryption Algorithm Used _____ (3DES, AES, RSA etc.) Key size used _____
