

Network Configuration Approvals

The Michigan State Police (MSP) requires that all Criminal Justice Information System (CJIS) current or proposed connectivity be approved by the MSP Information Security Officer (ISO) **prior** to implementation. The approval process ensures compliance with the federal CJIS security policies¹. The MSP is required to complete this process to remain in compliance with FBI requirements. Once a current network is approved, any changes must also be documented and approved **prior** to implementation by the agency.

Some examples of changes to an agency's connectivity include, but are not limited to:

- Indirect to direct Law Enforcement Information Network (LEIN) connectivity including desktop, secure tunnel, mobile or wireless access
- LEIN Interface Provider adding a new agency/subscriber
- Adding mobile devices
- Adding wireless devices (for example BlackBerries or similar devices)
- Converting from private radio frequency (RF) to a virtual private network (VPN) air-card technology
- Converting from a VPN to a fiber network
- Adding or modifying MiCJIN connectivity
- Adding or modifying live scan connectivity
- Requesting Automated Pistol Registration System (APRS) or Sex Offender Registry (SOR) to existing MiCJIN connectivity
- Adding remote locations or substations
- Moving the agency to a new location
- All IP moves, adds or changes

Network Configuration Approvals Instructions

This packet is designed to assist you in documenting your network diagram and accompanying narrative with the goal of ensuring your agency has documented the network in compliance with CJIS policy and to stream-line the approval process.

The packet consists of:

1. Documentation Checklist
The documentation checklist is designed to assist you in ensuring your diagram contains all the essential elements that are required to be depicted.
2. Network/Security Questionnaire
The questions asked are ones that typically are not depicted on a network diagram, but are essential for the approval of your request. Please complete this questionnaire and return it with your network diagram and any other supporting documentation.
3. Sample Network Diagrams
These are provided to assist you with the level of detail needed in your diagram. Do not replicate these and return them as your diagram as they will be rejected. Appendix C of the *CJIS Security Policy 5.0* also contains examples of the expected quality of the documentation.

¹ For a copy of the most recent CJIS Security Policy, please visit www.Michigan.gov/LEIN, and click on *Current FBI CJIS Security Policy (pdf)*. The accompanying document, *Security Policy Transition Information (pdf)* provides guidance on the implementation deadlines for the new policies.

Checklist for Network Diagrams

As required by the FBI CJIS Security Policies, agencies with direct CJIS connectivity must maintain a complete topological drawing (network diagram) which depicts the interconnectivity of the agency's network. Direct connectivity is defined as using a device (i.e. desktop computer, in-car/mobile terminal or laptop, BlackBerry, etc.) The network diagram must be maintained in a current status and must be agency specific.

In an effort to streamline the approval process, please use this checklist to ensure your diagram meets these requirements. Note: if your diagram does contain all of the following elements, additional clarification may still be needed and there is no guarantee your network will meet the security requirements. If you wish, Information that may be unclear on the diagram can be explained and elaborated more in a written narrative to accompany the diagram. This will assist when your network is reviewed and may require less follow-up from the ISO.

- All CJIS communication path, circuits, and other components used for the interconnection, beginning with the authorized user agency and traversing through all interconnected systems to the organization end-point (i.e. the Interface agency or the State of Michigan).
- All remote/satellite locations are identified, including any remote data storage locations.
- The logical location of all components including:
 - Firewalls
 - Routers
 - Switches
 - Hubs
 - Servers
 - Encryption devices
 - Electronic storage devices
 - Mobile/wireless devices and all MDTs or MCTs connecting to your network, listed by agency
 - Computer workstations (each workstation does not need to be individually listed)
- All connections to other agencies, depicted individually, including the type/method of connectivity to each agency (i.e. subscriber police department, city treasurer, county clerk, building inspector, etc.)
- Internet connections are identified.
- Connectivity to the State of Michigan is identified.
- Firewalls are identified and include the make and model, for each firewall on the diagram as well as the supplemental information requested on the questionnaire.
- Wireless Access Points are identified on the diagram as well as the supplemental information requested on the questionnaire.
- Mobile Access Points are identified on the diagram as well as the supplemental information requested on the questionnaire.
- If user/devices are establishing a VPN over the internet, please include the internet as part of the connections.
- Identify/confirm all CJIS traffic is encrypted to a minimum of 128 bit.
- Complete the Network Diagram questionnaire.
- The diagram must be labeled:

"FOR OFFICIAL USE ONLY"
AGENCY NAME
DATE OF THE DIAGRAM

Agency Name

ORI

Date

Contact Name

Phone

Email Address

Network Diagram Questionnaire

1. Do you have mobile devices (MDTs) or do any other agencies MDTs connect to your network? YES NO
 - a. Were the mobiles purchased or upgraded AFTER September 30, 2005?
 YES NO
 - b. How do the mobiles connect to the network?

 - c. How do the mobiles authenticate?

 - d. Are the MDTs secured in the vehicle by a locking vehicle mount?
 YES NO
 - e. If yes, how often are the MDTs removed from the vehicle?

 - f. If no, describe the advanced authentication you are using for these MDTs. Refer to section 5.6.2.2 of the *CJIS Security Policy 5.0* for information regarding advanced authentication.

 - g. What is the level/type of encryption for these devices?

 - h. Are you requesting access for the purpose of connecting your MDTs through your network to be able to access the MiCJIN Portal?
 YES NO

d. Is the SSID broadcast? YES NO

7. What are the make(s) and model(s) of your firewalls?

8. CJIS Firewall Requirements. Please read and certify your firewalls meet these requirements.

- a. Networks in which some terminals, and/or access devices have CJIS access and/or Internet access (e.g., peer to peer relationships, large mainframes and servers that house web sites) shall be protected by network firewall type devices. These devices shall implement a minimum firewall profile in order to provide a point of defense and a controlled and audited access to servers, both from inside and outside the CJIS networks.
- b. Network firewall architectures shall prevent unauthorized access to CJIS data and all network components providing access to the FBI CJIS Wide Area Network (WAN), either directly or indirectly through connections to other networks. Network firewall policies shall be concerned with securing the total site. This must include all forms of access, wireless, dial in, off site, Internet access, and others.
- c. Network firewall operating system builds shall be based upon minimal feature sets. (It is extremely important that all unnecessary operating system features are removed from the build prior to network firewall implementation, especially compilers.) All unused networking protocols shall be removed from the network firewall operating system build.
- d. Any appropriate operating system patches shall be applied before any installation of network firewall components, and procedures shall be developed to ensure that the network firewall patches remain current while the network firewall retains its statefulness.
- e. All unused network services or applications shall be removed or disabled. Only network services that are required shall be permitted through the network firewall. Allowed services shall be documented as to the service allowed, the description of service, and the business requirement for service.
- f. All unused user or system accounts shall be disabled.
- g. All default vendor accounts shall have the passwords changed prior to the network firewall going on line.
- h. Unused physical network interfaces shall be disabled or removed from the server chassis.
- i. Only network firewalls employing multiple network interfaces (a.k.a. dual homed) are permitted. A network firewall having less than two network interfaces or otherwise conducting inbound and outbound traffic on a single network line shall not be permitted.
- j. A network firewall implementation shall not reside on a shared server platform offering general network file and print services to a user community.
- k. All network firewalls shall be backed up immediately prior to production release. (As a general principle, all network firewall backups should be full backups as there is no real requirement or need for incremental backups.)

Our firewalls meet these criteria.

Our firewalls DO NOT meet these criteria.

Please explain how they DO NOT meet the criteria.

Sample Network Diagrams

This diagram is provided as a **sample only** of the level of detail required. Please use this as a guide only. Duplicates of these diagrams will not be accepted for approval for CJIS access. For more examples, refer to Appendix C of the *CJIS Security Policy 5.0*.

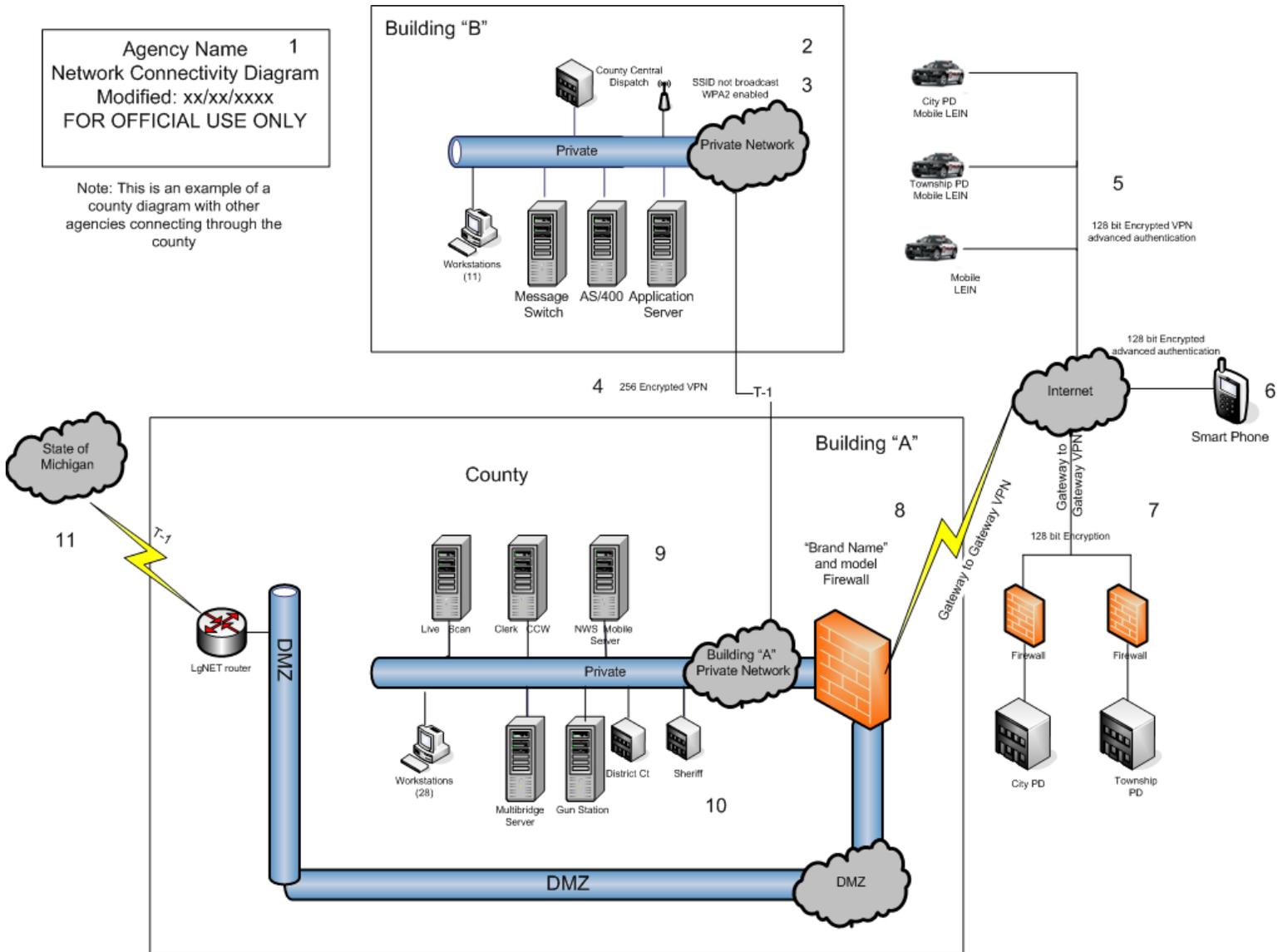


Diagram Key

1. **Agency Name, date of modification/creation , “For Official Use Only”** are required. The date of modification/creation must be within the last 12 months. The term “For Official Use Only” is a caveat applied to unclassified but sensitive information that should not be disclosed to anyone except government employees or contractors with a need to know. (See CJIS Security Policy 5.0, Appendix A, Terms and Definitions).
2. Identify any **auxiliary buildings** connected to the network, **servers** and **workstations**.
3. Identify how the **auxiliary building** is connected to the main building and the level of **encryption**.
4. Identify any **wireless access points** and identify if the SSID is or is not broadcast and the level of authentication (i.e. WPA, WPA2 etc.).
5. For **mobile devices (phones, car, laptop)** identify any other agencies connecting remotely through the agency, the level of **encryption** and identify what method of **advanced authentication** is in use.
6. **Smart Phones:** Identify what the smart phone is accessing on your system. (See CJIS Security Policy 5.0 section 5.5.7.3.1)
7. Connections to **other departments**. Indicate the **connection**, level of **encryption** and if **advanced authentication** is in use.
8. Identify the **brand and model of** firewall and identify if it has the ability to be **FIPS 140-2** compliant.
9. Identify **servers and workstations** on the network.
10. Identify all other **departments** on the network.
11. Identify the **connection to LEIN and/or the state** network.