



MICHIGAN STATE POLICE

333 South Grand Avenue
Lansing, Michigan 48909

Phone 517/241-0615
Fax 517/241-0865

Law Enforcement Agency Connection to the Michigan State Police Programs

This document is intended to assist Law enforcement and other qualified agencies in gaining access to various Michigan State Police programs (Live Scan, LEIN, and MiCJIN Portal).

TABLE OF CONTENTS

METHODS OF CONNECTING TO THE MSP NETWORK.....	4
LOCAL GOVERNMENT NETWORK (LGNET).....	4
What is the LGNET?.....	4
LGNET Connectivity.....	4
Responsibilities.....	4
Security.....	5
Changes.....	5
Advantages/Disadvantages.....	5
Connectivity Testing.....	5
Maintenance.....	5
GATEWAY-TO-GATEWAY VPN.....	5
What is a GATEWAY-to-GATEWAY VPN?.....	5
GW-to-GW VPN Connectivity.....	5
Responsibilities.....	6
Security.....	6
Changes.....	6
Advantages/Disadvantages.....	6
Connectivity Testing.....	6
Maintenance.....	6
SECURID® TOKEN.....	6
What is a SecurID® Token?.....	6
How to Order?.....	7
Responsibilities.....	7
Security.....	7
Changes.....	7
Advantages/Disadvantages.....	7
CLIENT-TO-GATEWAY VPN.....	7
What is a Client-to-Gateway VPN?.....	7
How to Order.....	7
Responsibilities.....	7
Security.....	8
Changes.....	8
Advantages/Disadvantages.....	8
CRIMINAL JUSTICE APPLICATIONS AVAILABLE BEHIND THE MICJIN PORTAL.....	9
SNAP.....	10
APRS.....	10
CPL.....	10
MIDIRS.....	11
MICR.....	11
SOR.....	11
LEIN.....	12
FINDAUTO.....	12
MICJIN PORTAL.....	13
NEW APPLICATIONS.....	13
REVISED APPLICATIONS.....	14
NEW APPLICATIONS.....	14
NEW OR REVISED APPLICATIONS (LIVE SCAN).....	15
CONNECTIVITY CONTACT LIST.....	16

MSP	Michigan State Police
MiCJIN	Michigan Criminal Justice Information Network
MSC	MiCJIN Service Center
LEIN	Law Enforcement Information Network
Live Scan	Electronic fingerprint submission program
CJIS	Criminal Justice Information Systems
CSA ISO	CJIS Systems Agency Information Security Officer
LGNET	Local Government Network
VPN	Virtual Private Network
DTMB	Michigan Dept of Information Technology, Management and Budget
GW-to-GW	Gateway-to-Gateway VPN
SecurID	Device for performing two-factor authentication for a user to a network resource
NAT	Network Address Translation
TELECOM	DTMB Network Center, Telecommunications Services
ISP	Internet Service Provider

Methods of Connecting to the MSP Network.

Local Government Network (LGNET).

- 1) Gateway-to-Gateway VPN.
- 2) SecurID token.
- 3) Client-to-Gateway VPN.

LOCAL GOVERNMENT NETWORK (LGNET)

What is the LGNET? The primary method of connection to the State is through the LGNET. This method uses secure lines and circuits between the host agency and the State. The routers at both ends are managed by AT&T. These connections are monitored 24/7 by AT&T and the State. Agencies can access all available MSP programs via an LGNET connection. LGNET circuits are available in two capacities, 512k or T1.

LGNET Connectivity An LGNET circuit is typically located at the Sheriffs' office or the Central Dispatch/911 office in the county. Some larger police departments, such as Detroit PD or Grand Rapids PD, host their own LGNET circuit. Law enforcement agencies within the county can gain access to the host circuit either by dedicated land line, VPN, or using an approved wireless connection. All connections to the MSP must be approved by the CJIS Systems Agency Information Security Officer (CSA ISO).

Responsibilities After installation of the circuit and routers by AT&T, the State has the responsibility of maintaining the router and firewalls based in Lansing. AT&T manages the router at the host site and assigns NATed IP addresses to the incoming IP addresses from the host site. AT&T is responsible for the 24/7 monitoring of the circuit. The host agency is responsible for maintaining a secure location for the circuit and 24/7 access to the circuit should AT&T need to service the device. Also, the host agency will provide the State with a contact name and number for troubleshooting purposes.

Security Firewalls are maintained by both the MSP and the DTMB Telecom Section on the State side of the LGNET circuit. Only pre-authorized IP addresses are allowed through these firewalls. The host agency is responsible for maintaining the firewall on the county side of the router informing the State what IP addresses will be presented for what applications. In addition to the host agency, other agencies in the county that wish to connect to the State network through the county LGNET must also submit a network diagram with approved firewalls, prior to gaining access.

Changes Any changes in the access to the LGNET router must first be submitted to the MSP, and then the MSP will submit the request to the DTMB Telecom section. A revised network diagram must accompany any requests and be approved by the MSP CSA ISO. There are no costs for any changes made to T1 circuits.

Advantages/Disadvantages One advantage of the LGNET circuit is that it is monitored 24/7 by AT&T, who often detect and initiate remedial action before the agency is aware of a problem. Another advantage is that the DTMB Telecom section has become familiar with dealing with the routers and circuits that make up the LGNET. One disadvantage with the LGNET circuit is the cost. A 512K capacity circuit costs \$11,500 per year. A T1 circuit costs \$21,000 yearly*. Another disadvantage is that a smaller agency must have the permission of the host agency in order to connect to the LGNET.

Connectivity Testing When the DTMB Telecom section notifies the MSP that the connection request has been completed, the agency network administrator is sent instructions on how to modify the host file in order to navigate to the secure log-in screen for MiCJIN access. The instructions direct the network administrator to notify us if the connectivity test is successful. If the connectivity test is not successful, then further testing with the State DTMB Telecom section and the agency IT staff is indicated. For Live Scan connections, the Live Scan analyst works with the agency and their Live Scan device vendor. For connections to the LEIN servers, the LEIN Field Services staff will provide assistance.

Maintenance Maintenance of the LGNET router is the responsibility of AT&T. The host agency is responsible for maintaining a secure location for the circuit and allowing AT&T 24/7 access, if needed. Normal maintenance and 24/7 monitoring are included in the cost of the circuit.

GATEWAY-to-GATEWAY VPN

What is a GATEWAY-to-GATEWAY VPN? A GW-to-GW VPN is a virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and information transmitted between networks. It allows agencies to use their existing high-speed Internet connection to access the State network. All VPNs must encrypt their data communications.

GW-to-GW VPN Connectivity Agencies using a GW-to-GW VPN to connect to the State network do so as an LGNET circuit may not be available to them. The agency will have to acquire a static IP address assigned to them by their Internet Service Provider (ISP). The agency's ISP can help them configure the VPN or the IT support staff for the agency can configure the VPN.

* All costs referenced in this document current as of 8/31/2011.

Responsibilities The agency is responsible for installing and maintaining the router and firewall at their location. They are responsible for any changes or modifications necessary and to only use software/hardware that meets CJIS Security Policy specifications. The local agency is responsible for the fees charged by the State for the connection. At the present time the agency will be billed a one-time charge of \$306.00 for the GW-to-GW VPN setup and an ongoing monthly charge of \$129.00.

Security The State DTMB Telecom Section will maintain the router and firewall on the State end of the GW-to-GW VPN. The local agency is responsible for ensuring:

- That their connection abides by the current CJIS Security Policy for GW-to-GW connectivity.
- That any CJIS applications traversing the GW-to-GW tunnel have user authentication that meets the level specified by the current CJIS Security Policy.
- That the VPN/firewall server is a dedicated piece of hardware. A VPN tunnel from a web or e-mail server is not allowed.

Changes The local agency must notify the CSA ISO prior to any changes being made in the agencies network or connection to the State. Any changes in their firewalls must have the prior approval of the CSA ISO.

Advantages/Disadvantages The GW-to-GW VPN connection was intended for those agencies that do not have access to a LGNET circuit. All the MSP applications and programs can be accessed through a GW-to-GW VPN, at a lower cost than a LGNET circuit. The disadvantages are that the agency must rely on their ISP for reliable Internet access. Typically, the ISP may change the public IP addressing for the agency with little or no warning. The public IP address is recognized by the State VPN router. If the public IP address is changed, the VPN connection is lost until the MiCJIN Service Center can submit a request to list the new IP address. This may take a significant amount of time as it must pass CJIS ISO approvals. Also, the local agency is responsible for maintaining the hardware installed at their location. **Additionally, the state side of the GW GW VPN is only monitored Monday-Friday 0800-1700. Any problems occurring after hours or on holidays will not be addressed until the next business day.**

Connectivity Testing All testing for GW-to-GW VPNs are handled by the State DTMB Telecom Section. The Telecom Section staff will work with the agency IT staff to ensure that the VPN tunnel is up and running prior to returning the request back to the MSP.

Maintenance The State is responsible for the VPN routers on the State end of the VPN. The local agency is responsible for the hardware on their end of the VPN. The monthly charge for the GW-to-GW VPN helps to defray the cost of the hardware and the on-going support and maintenance for the VPN devices on the State side.

SecurID® TOKEN

What is a SecurID® Token? A SecurID® token provides two-factor authentication and allows a user to access the MiCJIN portal over the Internet from any location as allowed by CJIS Security Policy and is issued to a specific person and is not to be shared with other users. A SecurID® token is a small, approximately one square inch in size, key fob that displays six digits that change every minute, synchronizing with a server at the State. The current cost for a SecurID® token is \$11.00 per month, per token.

How to Order? Contact the MSP Token Coordinator and provide the following information for each individual needing a token:

- Name
- Email Address
- Physical Address
- Telephone Number
- Last four digits of the Social Security Number
- The Month and Date (MMDD) of the Date of Birth*

The process to order tokens takes approximately two weeks.

Responsibilities The individual users assigned the tokens are responsible for the physical control of their tokens. They are not to share the tokens with other users and if the token is lost, the MiCJIN Service Center is to be notified immediately. The token access is cancelled and the agency billed \$75.00 for the lost token. Tokens not returned will continue to be billed regardless of usage.

Security The assigned user is responsible for keeping the token physically secure, not sharing the PIN associated with the token; also, do not keep the PIN with the token.

Changes The agency may transfer a token from one user to another. Please contact the MSP Token Coordinator for assistance in transferring tokens.

Advantages/Disadvantages The advantage of the SecurID® token is that it can be used anywhere the user has Internet access within CJIS Security Policy guidelines. It provides the user with a cost effective method of connecting to the MiCJIN portal. The disadvantage with the token is that it provides limited LEIN access. The user will not receive and cannot send unsolicited LEIN messages (administrative messages). All out-of-state hits will go back to the main agency terminal. Another disadvantage is that each token is assigned to one user and may not be cost effective for larger agencies to provide every user with a token. Also, the user is accountable for the use and safekeeping of the token.

CLIENT-to-GATEWAY VPN

What is a Client-to-Gateway VPN? A Client-to-Gateway VPN is used primarily to submit fingerprints from a Live Scan device to the State. The Client-to-GW VPN uses a combination of a SecurID® token and a Client VPN software that is installed on the user's Live Scan device. The Client-to-GW VPN does not require a static IP address, so it can be used by agencies using a mobile Live Scan device to collect and transmit fingerprints. Like SecurID® only access, the token is assigned to a specific individual and is not to be shared with other users.

How to Order The Client-to-GW VPN is ordered through the MSP Token Coordinator and is similar to the process described for ordering SecurID® Tokens.

Responsibilities The individual users assigned the tokens are responsible for the physical control of their tokens. They are not to share the tokens with other users and if the token is lost, the MiCJIN Service Center is to be notified immediately. The token access is cancelled and the

* The last four of the SSN and the MMDD of the DOB are used by DTMB as challenge response questions in case technical assistance is ever required.

agency billed \$75.00 for the lost token. Tokens not returned will continue to be billed regardless of usage.

Security The assigned user is responsible for keeping the token physically secure, and not sharing the PIN associated with the token. Also, do not keep the PIN with the token.

Changes The agency may transfer a token from one user to another. Please contact the MSP Token Coordinator for assistance in transferring tokens.

Advantages/Disadvantages The advantage of the SecurID® token is that it can be used anywhere the user has Internet access within CJIS Security Policy guidelines. It provides the user with a cost effective method of connecting to the Live Scan application. One disadvantage is that each token is assigned to one user and may not be cost effective for larger agencies to provide every user with a token. Also, the user is accountable for the use and safekeeping of the token.

Chapter

3

AVAILABLE MiCJIN APPLICATIONS

Criminal Justice Applications Available Behind the MiCJIN Portal

- SNAP (Statewide Network of Agency Photos)
- APRS (Automatic Pistol Registration System)
- CCW (Carrying Concealed Weapon)
- MiDIRS (Michigan Digital Image Retrieval System)
- MICR (Michigan Incident-based Crime Reporting)
- SOR (Sex Offender Registry)
- LEIN (Law Enforcement Information Network)
- FindAuto

SNAP



Mugshots help solve crimes but are of no use if they can't be put in the hands of the law enforcement professional that needs them. Criminals don't stay in one place, which makes the sharing of information critical. The Statewide Network of Agency Photos (SNAP) is a tool that allows agencies to share digital criminal images across jurisdictional boundaries. Images are submitted digitally, using live scan terminals, along with fingerprints. After positive identification is made, the image is stored in a database that can be searched through a web browser. SNAP will store not only mugshots, but also images of scars, marks and tattoos. Sharing of images throughout the state will increase the efficiencies and effectiveness of all agencies (Note: To encourage participation in this statewide system, SNAP is only available to agencies contributing photos).

APRS



The Automated Pistol Registration System (APRS) is a tool that interfaces with LEIN to automatically perform queries of the National Crime Information Center (NCIC), National Instant Criminal Background Check System (NICS), Corrections Management Information System (CMIS), and criminal history records, including outstanding warrants. The system automates the issuance of required forms. APRS enables data to be captured at the point of entry, builds the State of Michigan's pistol registration database, and greatly reduces the redundant typing of similar data.

CPL



Licenses to carry a concealed pistol can be entered directly by county clerks after county gun boards have made their decision to issue or deny a license. This provides an immediate update to the state database so investigators and officers on the street have current information. Clerks can also query information on any license holder in the state. In addition, clerks can run reports to find out who is actively holding a permit in their county, who's permit is pending, and when certain permits are coming up for renewal.

MiDIRS



Sometimes, an agency needs to identify a suspect, but a mugshot is unavailable or out of date. The Michigan Digital Image Retrieval System (MiDIRS) provides a secondary photo source. MiDIRS utilizes a direct connection to the Secretary of State's Driver License Photo database to assist law enforcement. This valuable tool, formerly available only through the Michigan State Police posts, is now available through the MiCJIN portal to all law enforcement agencies.

MICR



The Michigan Incident Crime Reporting (MICR) program is designed to identify with precision when and where crime takes place, what form it takes, and the victims' and offenders' characteristics.

MICR access through the MiCJIN portal will allow an agency who does not have a records management system to enter crime information directly into the MICR database using a standard web browser. The system also now electronically captures Law Enforcement Officers Killed and Assaulted (LEOKA) data. Additionally, agencies can now retrieve reports from the MiCJIN Portal MICR application.

SOR



The Sex Offender Registry (SOR) provides for registration of sex offenders in Michigan. Additionally, processing of signature forms required to be submitted to the State have been streamlined and agencies can generate reports as needed from the SOR application.

LEIN



LEIN is a statewide repository of missing persons; persons for who warrants have been issued; and vehicles that are abandoned, stolen, or impounded. LEIN interfaces with a multitude of databases and information is available from multiple sources including various state, federal and international databases. Users can retrieve and enter data from these sources.

LEIN is a valuable tool that all law enforcement agencies need to ensure the safety of their officers and the citizens they protect and serve. During a time when Homeland Security is at the forefront of all our minds, LEIN can provide an information network to assist with officer and citizen safety.

FindAuto



FindAuto is a program that will retrieve all stolen, abandoned and impounded vehicles that meet certain criteria. County of entry, color, low and high theft date, partial VIN, Make, Model, Style and Vehicle Year are all searchable. Results are returned in an Excel Spreadsheet.

Chapter
4

APPLICATION PROCESS

MiCJIN PORTAL

New Applications

(Excluding LEIN and Live Scan)

A new MiCJIN Service Application (RI-092) must be completed and submitted, along with a signed MiCJIN User Agreement (RI-093). These documents may be obtained by calling the MiCJIN Service Center at 517/241-0615 or by e-mailing a request to MiCJINMAIL@Michigan.gov with 'application' in the subject line. A current network diagram, which depicts all connections outside of the agency's network and current firewalls, must also be submitted. To assist agencies in preparing these diagrams, please see Appendix C, Checklist for Network Diagrams.

If connecting through a Gateway-to-Gateway VPN, the VPN questionnaire must also be completed. See Appendices B and C for additional information.

Once received at the MSC, the documents are reviewed for accuracy and completeness. Requests are then sent to the different business owners of the applications that the agency has applied for. Once all the necessary information is gathered, the connectivity request can be submitted for CSA ISO approval and then processing by DTMB Telecom. An agency will always be notified and permission requested if it becomes necessary to share the network diagram with DTMB Telecom.

The approximate length of time for requests to be completed can vary from 4 to 8 weeks. Any incomplete Service Application or diagram will slow the process. The CSA ISO will not approve any request until any deficiencies in the network security are corrected.

Agencies who connect to the MiCJIN Portal using SecurID® tokens do not have to submit a network diagram as they will connect to our Portal using their Internet service. Please contact the MSP Token Coordinator with the required information for each person needing a token. The tokens are not to be shared between users. Each user must have a token assigned to him or her.

When the LGNET connectivity request is reported to the MSC as completed, an e-mail will be sent to the local contact and the network administrator at the agency. The e-mail will contain the instructions for modifying the host file to access the secure log-in screen. The local contact is then directed to call us for their initial password and training on the portal and their assigned applications.

For a Gateway-to-Gateway VPN, the process is essentially the same. However, the DTMB Telecom technician who sets up the VPN will contact the agency's IT network administrator and ensure that the VPN is up and running prior to returning the request back to the MSC.

Revised Applications

(Excluding LEIN and Live Scan)

Agencies are requested to submit a revised Service Application whenever they ask for a new application or if their connectivity is changing.

Along with the revised Service Application, if any changes have occurred in the agency's network or more than six months have elapsed since the last diagram has been submitted, the agency should attach a revised network diagram to the Service Application.

For an agency that would like a new application and keep the same connectivity, we will ask the business owner of the application for approval for the agency to have access to the application. Upon approval, the MSC will set up the local administrator with the application rights.

Any changes in connectivity will go through the approval process outlined above.

New Applications

(LEIN):

All new requests for LEIN access or changes in LEIN connectivity must be approved by the Michigan State Police. Prior to obtaining that approval, the agency will have to submit a completed LEIN User Agreement, LEIN Agreement to Pay, LEIN Agency Survey, and a network diagram. These forms can be obtained by contacting LEIN Field Services.

There are three methods of obtaining full service LEIN:

- Direct station access via the MiCJIN Portal.
- Host a LEIN server at your worksite.
- Become a subscriber off another agency's LEIN server.

New or Revised Applications (Live Scan)

All new or revised requests for Live Scan access must go through the Identification Section. They will assist the agency in completing the Live Scan Interface Application. Once we have the completed application, the connectivity process is the same as for the MiCJIN Portal or LEIN. However, an agency can also access Live Scan using a Client-to-Gateway VPN token.

CONNECTIVITY CONTACT LIST

AGENCY/SECTION TITLE	NAME	PHONE NUMBER	E-MAIL
MSP/MSC Manager	Mitzi Goldstein	517/241-0693	GoldsteinM@Michigan.gov
MSP/MSC Analyst	David Bennett	517/241-0615	BennettD5@Michigan.gov
MSP/MSC Analyst	Amanda Noxon	517/241-0813	NoxonA@Michigan.gov
MSP/MSC Technician	Therese Hudak	517/241-0798	HudakT@Michigan.gov
MSP/MSC Technician	Thomas Bur	517/241-0764	BurT@Michigan.gov
MSP/CSA ISO	Terri Smith	517/241-0607	SmithT39@Michigan.gov
MSP/LEIN Specialist	Charles Hoffmeyer	517/241-0703	HoffmeyerC@Michigan.gov
MSP/LEIN Analyst	Elizabeth Canfield	517/241-0639	CanfieldE@Michigan.gov
MSP/LEIN Analyst	Pamela Cruz	517/241-0658	CruzP@Michigan.gov
MSP/Identification Manager	Scott Blanchard	517/241-0620	BlanchardS1@Michigan.gov
MSP/Live Scan Analyst	Keith Kramer	517/241-0723	KramerK3@Michigan.gov

Broadband Requirements

Security Requirements:

- The connection must abide by the CJIS Security Policy for Gateway-to-Gateway connectivity.
- Any CJIS applications traversing the tunnel must have user authentication that meets the level specified by the CJIS Security Policy.
- The VPN/Firewall server must be a dedicated piece of hardware. A VPN tunnel from a web or email server is not allowed.
- Private network addresses on the remote end must be translated to public address(es) for routing on Lansing Metropolitan Area Network (LMAN), via network address translation (NAT).
- Remote control of LMAN resources is not allowed via vendor Gateway-to-Gateway tunnels (PCAnywhere, Timbuktu, or Terminal Services Clients).
- DTMB will need a list of all LMAN assets and ports that will need to be reached via the Vendor Gateway-to-Gateway tunnel

Hardware Requirements:

Network Switch/Hub

- Must be large enough to handle all network connections at location (including network printers and servers).

VPN/Firewall

- Must be able to handle IPSEC protocols.
- Authentication = ESP/MD5/HMAC-128
- Type = Preshare
- Encryption = 3DES-168
- IKE Proposal = IKE-3DES-MD5-DH2

Hardware that has been proven to work with the State of Michigan VPN gateway device:

- Cisco IOS based devices (any Cisco router)
- Cisco PIX Firewall devices
- Checkpoint firewalls
- Firebox firewalls
- Cisco VPN gateway devices
- Netscreen firewalls
- Sonicwall firewalls
- Nortel Contivity VPN server

Static IP address:

- In order to use a gateway-to-gateway VPN, you must have a static IP connection to the Internet. This will be provided by the ISP.

VPN Questionnaire

Questions for any non-STATE OF MICHIGAN VPN concentrator connection to a STATE OF MICHIGAN VPN concentrator.

1. Agency Name:
2. Is there any remote control software used from the local source to a STATE OF MICHIGAN resource within this VPN connection?
3. Is there a formal process for gaining and/or denying access to the network equipment by the site personnel?
4. If so who is responsible for maintaining this process?
5. What STATE OF MICHIGAN applications IP address and port numbers will the site need to connect to?
6. Is there an access control list for this device that would only allow access to the designated IP address locations and application's port number, used at this site?
7. If not, how is the access to this connection controlled?
8. Does the site do Network Address Translation (NAT) of the device's IP address, prior to the connection of the VPN concentrator?
9. If so, how is the NAT being translated (one-to-one, match host or many-to-one)?
10. Is there logging, of administration access on the site's network equipment?
11. If so who reviews these logs?
12. Is there an automated process notifying administrator of errors or warnings? If so what is the process to notify the STATE OF MICHIGAN of potential threats?
13. Does the site have a signed agreement with the STATE OF MICHIGAN on how the information that will be accessed, will be used and/or disposed of?
14. If so, who will be responsible for monitoring this agreement at the site?
15. Does the site have an incident reporting process to notify the STATE OF MICHIGAN if an incident has happened?
16. If so, has this process been explained to the users?
17. Does the STATE OF MICHIGAN and site personnel have a regular scheduled security awareness training program?

18. If so, how often is the training conducted?
19. Is there a formal process for a user to apply for or terminate access to this connection?
20. If so, how often is the user access list reviewed?
21. Who is responsible for maintaining the user access list?
22. Does the site device that accesses this VPN connection use a screen saver?
23. If so, what is the length of time that the screen saver is set for?
24. Does the site device have up-to-date Anti-virus software running on them?
25. If so, please provide what software and updates are currently being used.
26. Does the site device have the OS service packs upgraded to the current vendor recommended level?
27. The OS and service pack of the device is required.
28. Do you have a process in place to notify the STATE OF MICHIGAN of any network changes?
29. A diagram of the network infrastructure is required.
30. List Agency VPN administrator and contact information?

Appendix

C

Checklist for Network Diagrams

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

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

c. How is it secured?

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*.

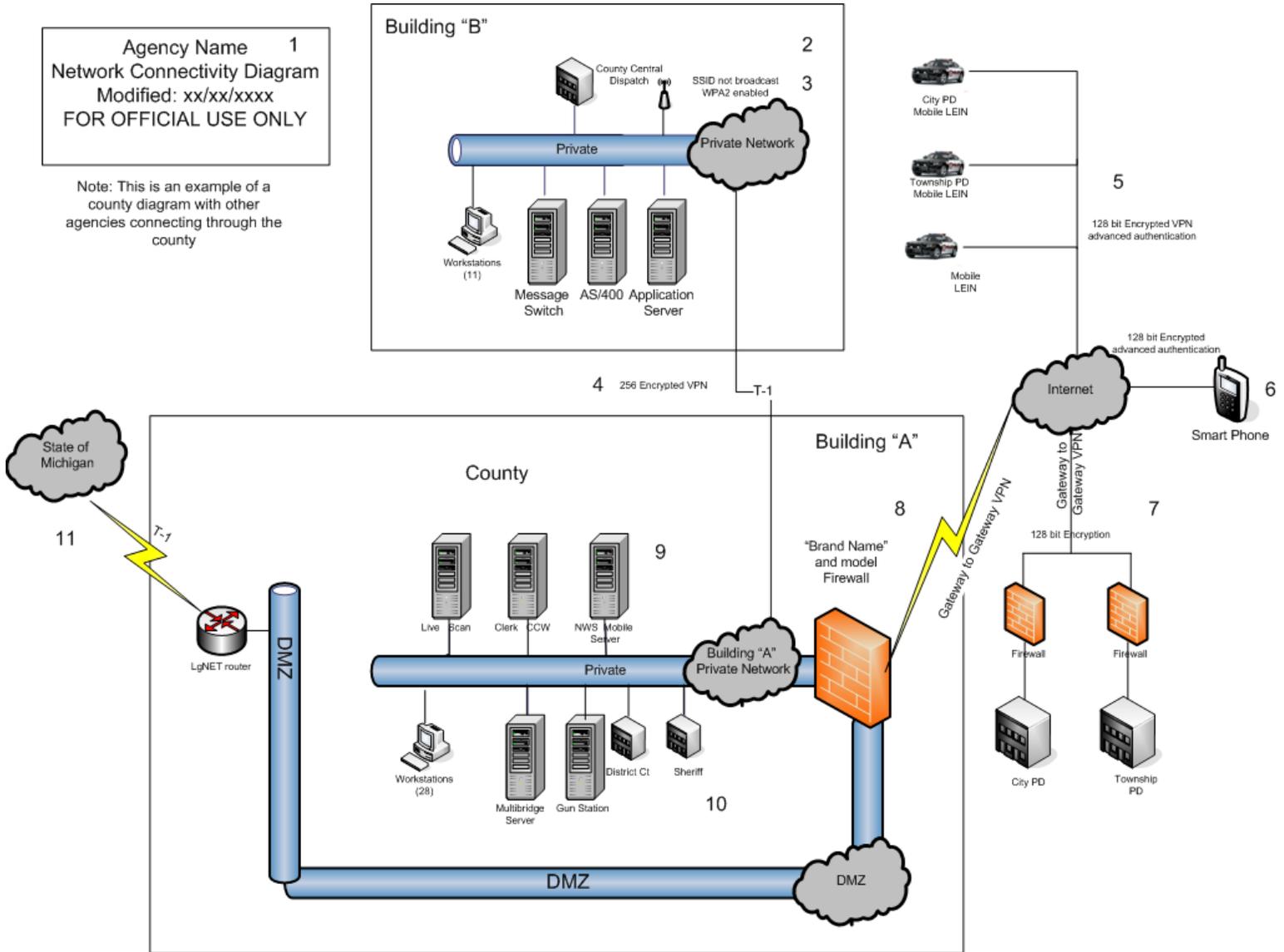


Diagram Key

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.