Mississippi Department of Public Safety
Mississippi Criminal Information Center (CIC)

MJIC Message Switch
Remote Server
Interface Control Document (ICD)

Version 6.00 R02

April 12, 2018

TABLE OF CONTENTS

CHANGE LOG

Date	*Version*	*Change*
December 10, 2012	6.00 R01	Revised for directly-connected workstations and trusted servers (no longer supports terminals and terminal servers).
April 12, 2018	6.00 R02	Encryption is now required for all current and future installations of remote servers. Requires use of Encryption Header within Extended Message Header and use of Encryption Key Book. Terminology changed to "remote server". Removed directly-connected workstation section. Modified document title. Terminology updated to more closely align with DMPP-2020 Interface Specification. Imbedded photos may now be included in messages from the remote server to the Message Switch. Support for this is optional. (Previously, imbedded photos might be included only in messages from the Message Switch to the remote server. Support for this continues to be optional.) Updated acknowledgement messages. Data Portion of transmission is zero length. Updated "prefix" in law enforcement request, response and error messages. One information item in prefix.

1.0 SCOPE

This document and the documents it references provide requirements for the interface between law enforcement remote servers and the Mississippi Justice Information Center (MJIC) Message Switch. This interface provides the capability to send law enforcement messages including messages to the FBI NCIC or III systems, member sites on the Nlets network, the Mississippi Department of Motor Vehicles (DMV), or the Mississippi Criminal History System (MCHS).

The MJIC Message Switch is operated by the Mississippi Department of Public Safety (MDPS) Criminal Information Center (CIC) located in Pearl, Mississippi. The CIC may be reached by telephone at (601) 933-2601. Prospective vendors seeking certification to provide message switch services in the State of Mississippi should contact the CIC Business Systems Analyst at 601-933-2601.

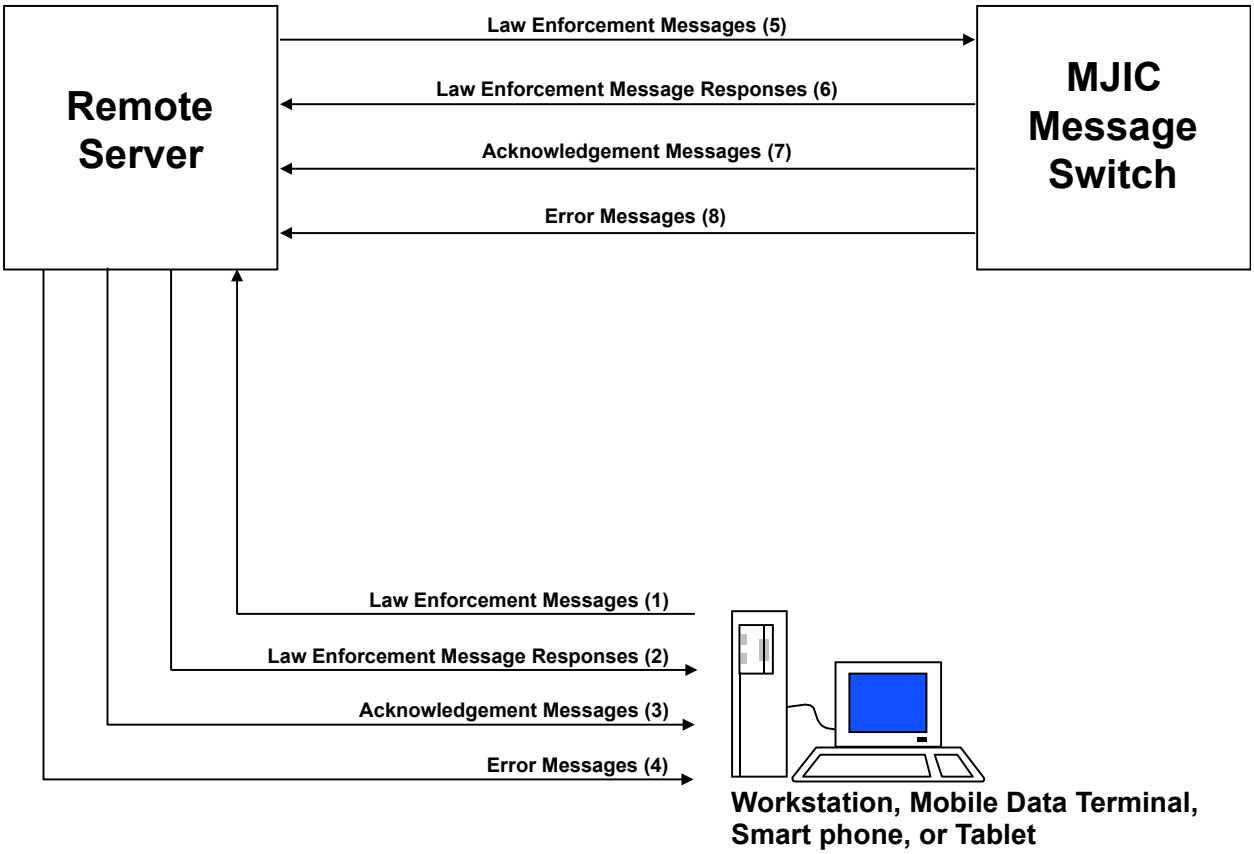
2.0 REFERENCES

The following references apply to the interfaces described in this document. The applicable version is the version in effect at the time of certification. Contact CIC to verify the correct versions of these documents.

1. Interstate Identification Index (III) Operational and Technical Manual, US Department of Justice (DOJ), Federal Bureau of Investigation (FBI), Identification Division.
2. National Crime Information Center (NCIC) Operating Manual, US Department of Justice (DOJ), Federal Bureau of Investigation (FBI), Identification Division.
3. Nlets Users Guide.
4. MCHS Security Policy.
5. CJIS Security Policy.
6. Datamaxx Message Processing Protocol® DMPP-2020 Interface Specification, Datamaxx Applied Technologies Inc. Version 9.0.
7. Datamaxx Standard Embedded Object® DSEO-2020 Object Processing in the Law Enforcement Environment Technical Specification, Datamaxx Applied Technologies Inc.
8. MJIC Message Switch Remote Server Certification Test Procedures.

3.0 INTERFACE OVERVIEW

This brief overview of the data flows provides a context for understanding the detailed interface requirements.



The MJIC Message Switch communicates with workstations/devices through a remote server. Remote servers support messaging functions for workstations, mobile data terminals, and other devices such as smart phones or tablets. The above diagram shows the data flows between the Message Switch, remote servers, and their connected workstations/devices.

A workstation/device sends a law enforcement message (1) to the remote server. The remote server in turn passes it on to the Message Switch (5). Under certain conditions, the Message Switch acknowledges receipt of a message (7) and the remote server may pass this acknowledgement on to the workstation/device (3). The Message Switch then forwards the message to its destination - the FBI NCIC or III systems, member sites on the Nlets network, the Mississippi Department of Motor Vehicles (DMV), or the Mississippi Criminal History System (MCHS). When a response is received by the Message Switch, the response (6) is delivered to the remote server and the remote server then forwards the message (6) to the workstation/device. However, if the Message Switch detects an error in a message it receives from the remote server, it returns an error message (8) to the remote server and the remote server passes error messages (4) on to the workstation/device.

It is not required that a remote server use the same formats for messages (1) through (4) as are required for messages (5) through (8). If the remote server provides alternative formats for its workstations/devices, it is the responsibility of the remote server to convert the messages between workstation/device and remote server ((1) through (4)) into the formats specified in this document for messages between the remote server and the Message Switch ((5) through (8)).

4.0 INTERFACE REQUIREMENTS

A remote server uses this interface to submit law enforcement messages to the Message Switch on behalf of a user at an attached workstation/device.

A remote server must be capable of sending any of the NCIC, III, and Nlets messages unless CIC waives this requirement and permits only a defined subset of these messages.

Section 4.1 describes the communication protocol for transmitting a message to the Message Switch. Then, section 4.2 provides more detail regarding the format of the NCIC, III, and Nlets messages that are contained in the transmission.

4.1 Communication Protocol

This section documents the manner in which communications are handled between a remote server and the Message Switch. The method of communication between the workstations/devices and the remote server is not within the scope of this ICD.

The connection between a remote server and the Message Switch is via TCP/IP socket streams. The transmission protocol is DMPP-2020. The Message Switch acts as the server, the remote server as the client. The requirements for the DMPP-2020 transmission protocol are found in the DMPP-2020 Interface Specification. References to the DMPP-2020 specification are included in the overview of the Framing Structure and Encrypting Transmissions in sections 4.1.2 and 4.1.3 below.

The Coded Messages described in DMPP-2020 Interface Specification section 6.0 item 5 are not applicable to remote server communication with the MJIC Message Switch.

4.1.1 Establishing a Connection

A remote server connects to the Message Switch using the Message Switch floating IP address and a designated TCP port number. The Message Switch will grant the connection if the remote server IP address has been configured into the Message Switch. If the connection attempt by the remote server fails, the remote server should wait for a short time and try to connect again, repeating this process until the connection is established. A single bi-directional socket stream is used for the interface.

Once the connection has been established, the remote server should insure that the connection stays alive by periodically sending a transmission with DMPP-2020 Function Code 'Request status of system' (Keep Alive). The Message Switch may also send a DMPP-2020 status request to which the remote server must respond.

The Message Switch will send transmissions to a remote server as soon as it recognizes that a connection has been established. This could occur before the remote server has sent a transmission.

4.1.2 Transmission Protocol Framing Structure

When a connection has been established, the remote server transmits messages enclosed in the DMPP-2020 framing structure. The framing structure (also referred to as the message block) is described in DMPP-2020.

Prior to Interface Control Document version 2.0, the Encryption Header portion of the Extended Message Header was optional. As of the date of this ICD, a remote server that interfaces with the MJIC Message Switch must implement Encryption Type 1 and therefore the Encryption Header is now always required.

The transmission framing structure is summarized below.

1. A four byte binary Start Pattern, hex bytes \xFF\x00\xAA\x55, indicating the start of a transmission. (Refer to DMPP-2020 sec. 3.0)
2. A 32-bit binary value specifies the Total Transmission Length. The total length includes the lengths of the Start and Stop Patterns, the length of this Total Transmission Length itself, and length of the Extended Message Header (including the Encryption Header) and the length of the

Data Portion of the transmission. The value is transmitted in network order (i.e., most significant byte first). (Refer to DMPP-2020 sec. 3.0 Block Length)

Example: Hex bytes \x00\x00\x01x66 for a binary count of 358.

3. A DMPP-2020 Header which must include:
   - the Extended Message Header (Refer to DMPP-2020 sec. 3.0 and sec. 4.0 items 1 – 7)
     - plus -
   - the Encryption Header which is contained within the Extended Message Header (Refer to DMPP-2020 sec. 3.0 and sec. 4.0 items 8 – 9).
     The Encryption Header includes all of the parameters that are defined for Encryption Type 1 in DMPP-2020 sec. 4.0 item 9b.
4. The Data Portion of the transmission which contains the NCIC, III, Nlets, or Switch message. (Refer to DMPP-2020 sec. 3.0)

   The messages in the Data Portion are further described in sections 4.2.1 and 4.2.2 of this document. Binary information, as described in section 4.3, will be included in some responses and may be included in some message transmissions.
5. A four byte binary Stop Pattern, hex bytes \x55\xAA\x00\xFF, indicating the end of the transmission. (The Stop Pattern is the reverse of the Start Pattern.) (Refer to DMPP-2020 sec. 3.0).

4.1.3 Encrypting Transmissions

As of the date of this ICD, transmissions between a remote server and the MJIC Message Switch must be encrypted. A remote server must implement the DMPP-2020 Encryption Header and encrypt transmissions using DMPP-2020 Encryption Type 1.

The Encryption Header is contained within the Extended Message Header as outlined in section 4.1.2 of this document and described in detail in section 4 of the DMPP-2020 Interface Specification. Encrypting a transmission includes the use of the text format of the Encryption Key Book as described in DMPP-2020 Appendix A.

Encryption keys can be dynamically selected from the Key Book so that the same key is not used over and over again.

4.1.4 Logon, Logoff, and Password Change

A remote server must begin each session by sending a 'DOPS' logon message. The logon establishes the privileges of the user that is sending messages via the remote server. Only those privileges authorized for both the user and the remote server are allowed. The message format is:

<*dac*>.DOPS/MCH/<*user id*>/<*password*>/<*workstation/device*>

The remote server will receive a response indicating:

LOGON ACCEPTED

When the user is finished using the workstation/device, the remote server must terminate the session with the Message Switch by sending an 'OPX' message. The message format is:

<*dac*>.OPX

It is important to send the OPX message to end a session. Since all messages sent via a remote server during a session are logged on the Message Switch as having been sent by the user logged on to the device connected to the remote server, the OPX message prevents any subsequent use of the device from being associated with that user.

The remote server must be able to send requests to change a user password to the Message Switch using the 'DPWD' message. The message format is:

<*dac*>.DPWD/<*new password*>/<*old password*>/<*confirm*>

where <*new password*> is a new password, <*old password*> is the current password and <*confirm*> repeats the <*new password*> value for confirmation purposes.

The remote server will receive a response indicating:

Password Change Succeeded

4.1.5 Handling Network Errors

In the event of network errors, loss of network connections, or other serious errors, it is recommended that the remote server close the TCP/IP socket stream and re-establish the connection with the Message Switch. The currently logged-on user is retained by the Message Switch across TCP/IP reconnects.

4.2 Messages

Request, response, acknowledgement, and error messages are included in the Data Portion of the DMPP-2020 transmission as defined in section 4.1.2 of this document. Messages must be in the formats described in the following subsections.

4.2.1 Law Enforcement Request Messages to the Message Switch

Messages from a remote server to the Message Switch begin with the following prefix:

<*dac*>.

where <*dac*> is the Destination Address Code (DAC), an identifier assigned by CIC to identify the originating workstation/device attached to the remote server. The angle brackets shown above (and in the remainder of this section) are metasyntactic only and are not present in the prefix.

The law enforcement message itself follows the prefix. The NCIC, III, and Nlets message formats are discussed the subsections below.

4.2.1.1 NCIC and III Request Message Formats

These messages must be structured in accordance with the following documents:

- NCIC Operating Manual
- III Operational and Technical Manual

The format of the NCIC and III request messages is summarized below.

Field	***Description or Value***
<*pass*>	The <*pass*> prefix is optional. If it is present, it must have a value of `NCIC`. It signifies that the user wishes to bypass the validation of the message data elements. In addition, if the PASS prefix is present, the message will only be sent to NCIC or III, it will not be spawned to any other destination.
<*field delimiter*>	Period. (Required only if the optional <Pass> field is included.)
<*mke*>	NCIC or III message key.
<*field delimiter*>	Period.
<*sender ori*>	ORI sending the request message. This field is optional and if not present in the input data stream, the Message Switch will automatically insert the ORI associated with the DAC. If an ORI is provided in the message, the Message Switch will validate it.
<*field delimiter*>	Period.
<*control*>	Optional Control field up to 10 characters. The presence of the control field is signified by an asterisk in the first position. If the message key is an inquiry, i.e., a response is expected, the Message Switch will include the control field in the message response or responses.
<*field delimiter*>	Period. If the control field is not present, the delimiting period must not be supplied.

Field	Description or Value
<*text*>	The text of the message as defined in the NCIC Operating Manual or III Operational and Technical Manual except that fields in inquiry messages can be in any order because the Message Switch reorders these into the correct order.

4.2.1.2 Nlets Request Message Format

These messages must be structured in accordance with the following documents:

- Nlets Users Guide

The format of the Nlets request messages is summarized below.

Field	Description or Value
<*pass*>	The <*pass*> prefix is optional. If it is present, it must have a value of 'NLET'. It signifies that the user wishes to bypass the validation of the message data elements. In addition, if the <*Pass*> prefix is present, the message will only be sent to Nlets, it will not be spawned to any other destination.
<*field delimiter*>	Period. (Required only if the optional <Pass> field is included.)
<*mke*>	Nlets message key.
<*field delimiter*>	Period.
<*sender ori*>	OR sending the request message. This field is optional and if not present in the input data stream, the Message Switch will automatically insert the workstation/device default ORI. If an ORI is provided in the message, the Message Switch will validate it.
<*field delimiter*>	Period.
<*destination*>	Destination address. If multiple destinations are specified, they must be separated with commas. Each destination is either a two-letter state abbreviation, a full ORI, a broadcast group name, or an in-state station name. If the destination is not within Mississippi, the Message Switch will send the message to Nlets for delivery.
<*field delimiter*>	Period.
<*control*>	Optional Control field up to 10 characters. The presence of the control field is signified by an asterisk in the first position. If the message key is an inquiry, i.e., a response is expected, the Message Switch will return the control field in the message response or responses.
<*field delimiter*>	Period. If the control field is not present, the delimiting period must not be supplied.
<*txt*>	Literal text "TXT". Optional, signifies start of text fields.
<*text*>	The text of the message as defined by the Nlets User Guide. If the message key indicates that the message is an inquiry, the Message Switch will reorder message field codes (MFCs) into the proper order before sending the message to the destination.

4.2.2 Law Enforcement Response Messages from the Message Switch

Messages from the Message Switch to a remote server begin with the following prefix:

<*dac*>.

where <*dac*> is the Destination Address Code, an identifier assigned by CIC to identify the originating workstation/device attached to the remote server. The angle brackets shown above (and in the remainder of this section) are metasyntactic only and are not present in the prefix.

The law enforcement message follows the prefix. The response message format is described in sections 4.2.2.1. Examples of messages are found in subsections 4.2.2.2 through 4.2.2.4.

4.2.2.1 Response Message Format

The format of a response message is shown below.

Message Segment	***Field***	***Description or Value***
Source Information	<*field delimiter*>	Newline.
	<*src*>	Source of response.
	<*field delimiter*>	Space.
	<*isn*>	Five character input sequence number.
	<*field delimiter*>	Space.
	<*itd*>	Input time and date stamp in the format: HHMM:SS DD/MM/YY.
	<*field delimiter*>	Newline.
Source Header	<*original header*>	The header as received from the source interface (e.g. NCIC, or Nlets). The control field in the Source Header will be the same as supplied by the originating workstation/device.
	<*field delimiter*>	Newline.
Text	<*text*>	Request message text.
Trailer	<*mri tag*>	Literal text "`MRI`".
	<*field delimiter*>	Space.
	<*mri number*>	The master reference ID.
	<*field delimiter*>	Space.
	<*dac*>	Workstation/device id of requestor.
	<*field delimiter*>	Space.
	<*osq*>	Four character output sequence number.
	<*field delimiter*>	Space.
	<*otd*>	Output time / date stamp in the format: HH:MM:SS DD/MM/YY.
	<*field delimiter*>	Newline.
Exception Information	<*exception*>	Under certain circumstances, the following exceptions may be added after the trailer. If the message has been sent to the recipient as a result of the alternate route command the following will appear: ALTERNATE ROUTED MESSAGE... If the message has been sent to the recipient as a result of the Set Station Copy command, one of the two following lines will appear. OUTPUT COPY OF STATION OSN's MESSAGE INPUT COPY OF STATION ISN's MESSAGE If the message was sent to the recipient as a result of a Find command, one of the two following lines will appear. RETRIEVAL: ORIGINALLY OUTPUT - OSN OSQ AT OTD RETRIEVAL: ORIGINALLY INPUT - ISN ISQ AT ITD

4.2.2.2 Example of NCIC and III Response Messages

An annotated example of a response from NCIC or III is shown below.

Message Segment	*Example*
Prefix	20001.
Source Information	NCIC 01998 0010:00 02/10/04
Source Header	1L01008A,MRI123456789<*nl*>MS00000000
Text	*<response message text>*
Trailer	MRI 0010000 20001 0004 00:10:01 02/10/04

4.2.2.3 Example of Nlets Response Message from Out-of-State

An annotated example of a response from Nlets is shown below.

Message Segment	*Example*
Prefix	20001.
Source Information	NLET 01998 00:10:00 02/10/04
Source Header	RR.XYLIC0000 15:45 02/10/2004 00199 15:45 02/10/2004 00019 MS0000000 *control234567. TXT
Text	*<response message text>*
Trailer	MRI 0010000 20001 0004 00:10:01 02/10/04

4.2.2.4 Example of Nlets Response Messages from In-State Mississippi DMV and MCHS

The format of a response message from the Mississippi DMV in response to a DQ, KQ, and RQ has a slightly different format than a response message from out-of-state.

An annotated example of a response from the Mississippi DMV is shown below.

Message Segment	*Example*
Prefix	20001.
Source Information	DMVIN 01998 00:10:00 02/10/04
Source Header	RR.MSLIC0000.MS0000000.*control234567.TXT
Text	*<response message text>*
Trailer	MRI 0010000 20001 0004 00:10:01 02/10/04

The format of a response message from MCHS in response to an IQ and FQ has a slightly different format than a response message from out-of-state. An annotated example of a response from the MCHS is shown below.

Message Segment	*Example*
Prefix	20001.
Source Information	CCHIN 01998 00:10:00 02/10/04
Source Header	RR.MSLIC0000.MS0000000.*control234567.TXT
Text	*<response message text>*
Trailer	MRI 0010000 20001 0004 00:10:01 02/10/04

4.2.3 Acknowledgement Messages from the Message Switch

The Switch may send acknowledgement messages to the remote server.

Acknowledgements are reported in the Status Code for Responses Messages field of the DMPP-2020 Extended Message Header. (Refer to DMPP-2020 section 4 item 6) The Data Portion of the transmission will be zero length.

4.2.4 Error Messages from the Message Switch

If the Message Switch detects an error, it will send an error message to the remote server.

Some errors are reported in the Status Code for Responses Messages field of the DMPP-2020 Extended Message Header. (Refer to DMPP-2020 section 4 item 6) There may be text in the Data Portion of the transmission or the Data Portion may be zero length.

Error messages that contain information in the Data Portion are formatted as follows.

Error messages begin with the following prefix:

<*dac*>.

where <*dac*> is the Destination Address Code, an identifier assigned by CIC to identify the originating workstation/device attached to the remote server. The angle brackets shown above (and in the remainder of this section) are metasyntactic only and are not present in the prefix.

The error message itself follows the prefix and has the structure shown below.

Field	***Description or Value***
<*dac*>	Workstation/device id of requestor
<*field delimiter*>	Newline (one or more)
<*error message*>	Message with the text "`REJECTED BY MCHS –` " followed by the error message itself.
<*field delimiter*>	Space (one or more) followed by literal text "`AT`", followed by a space.
<*itd*>	Input Time / Date Stamp in the format HH:MM:SS DD/MM/YYYY.
<*field delimiter*>	Newline.
<*mri tag*>	Literal test "MRI-"
<*mri number*>	The master reference ID.
<*field delimiter*>	Newline.

4.3 Photos Imbedded in Messages

4.3.1 Photos Imbedded in Messages from the Message Switch – Optional

Some law enforcement messages, such as messages from the Mississippi DMV, may include photos. Optionally, these may be supported by the terminal server. They must be packaged in accordance with the DSEO-2020 Interface Specification. If the vendor chooses to support photos, this capability must be certified when the remote server is certified.

4.3.2 Photos in Messages to the Message Switch – Optional

Photos can be included in some messages transmitted to the message switch. (For example, Nlets AM messages may include photos.) Optionally, these may be supported by the remote server. They must be packaged in accordance with the DSEO-2020 Interface Specification. If the vendor chooses to support photos, this capability must be certified when the remote server is certified.

5.0 LOGGING REQUIREMENTS

Separate logs must be maintained on the remote server – one that records criminal history message activity and one that records non-criminal history message activity. The logs must be either password protected or encrypted. The log entries must be automatically written by the remote server software and must not be allowed to be updated by a user.

For certification purposes, if the vendor's software alters or synopsizes the response in a material way, there must be a log or other mechanism to display the actual response sent to the workstation/device.

6.0 SECURITY REQUIREMENTS

Remote servers must meet the requirements specified in the version of the MCHS Security Policy that is in effect at the time of certification. The MCHS Security Policy fully incorporates the FBI's CJIS Security Policy that dictates security requirements for systems that access the FBI's NCIC and NGI data.

Security policy includes requirements for network security between a remote server and the Message Switch and between a remote server and its attached workstation/device. It also includes requirements for operator authorization and authentication, any required audit trail or log, and requirements if attached workstations/devices or the remote server itself hosts other applications in addition to the Message Switch interface software.

Mobile data terminals and similar devices, such as smart phones and tablets, that communicate with the Message Switch via a remote server must use Two-Factor authentication.

As of the date of this ICD, transmissions between a remote server and with the MJIC Message Switch must be encrypted. A remote server must implement the DMPP-2020 Encryption Header and encrypt transmissions using DMPP-2020 Encryption Type 1. The Encryption Header is contained within the Extended Message Header as outlined in section 4.1.2 of this document and described in detail in the DMPP-2020 Interface Specification. Encrypting a transmission includes the use of the text format of the Encryption Key Book as described in DMPP-2020 Appendix A. Encryption keys can be dynamically selected from the Key Book so that the same key is not used over and over again.

Depending on the configuration at the local agency where the remote server is installed, CIC may impose additional security requirements beyond those stated in the MCHS Security Policy. The vendor must first contact the local agency where the remote server and workstations/devices are to be installed to determine the network configuration and then coordinate with CIC to determine an acceptable implementation of the security requirements.

7.0 INSTALLATION CHECKLIST

The following checklist gives the steps and responsible parties for connecting a remote server to the MJIC Message Switch. It is recommended that a local agency contact MDPS/CIC to discuss the process of adding a remote server to the network.

Step	Responsible Party	Action
1	Local Agency, Vendor, and CIC	The vendor must send a notice to the MDPS/CIC within 10 days of any installation at a customer site. The notice must provide a schematic of the installed system with an explanation detailing any changes from the configuration used by the vendor in the certification process. The CIC will review the installed configuration. If there are any changes from the certified configuration, the customer site may not operate in a live mode until the CIC approves the configuration The local agency, vendor, and CIC determine where the remote server is to be installed, scope of functionality required (i.e., full message capability or specialized subset), and the network configuration to be used. CIC verifies whether any additional security requirements must be met.
2	Local Agency	Procures remote server, workstations/devices, and any needed network equipment.
3	Local Agency	Provides user ids and workstations/devices that will be connected to the remote server to CIC.
4	CIC	Assigns IP numbers, workstation/device ids (DACs), user ids, and passwords in the Message Switch. Sets encryption flag for each DAC.
5	CIC	Configures security profile of user ids and remote server.
6	CIC	Informs local agency and vendor of remote server IP number, Message Switch IP and port numbers, workstation/device ids, and user ids.
7	Vendor	Notifies CIC of the installation date of the remote server.
8	CIC and Vendor	(If needed) Makes Encryption Key Book available to vendor via secure email/file exchange. Vendor installs.
9	Local Agency and Vendor	Submits test messages and CIC monitors initial operations and assists with problems.
10	Local Agency	Begins normal operations.