EXHIBIT 13

Test Plan

ASSURE911

NG9-1-1/CSI Test Plan

January 31, 2012

Table of Contents

1.0 Overview 4
2.0 Next Generation 9-1-1 System Requirements Test Cases 5
2.1 Network and Carrier Configuration Test Scenarios 6
2.2 PSAP Configuration Test Scenarios 8
2.3 Future PSAP Configuration Test Scenarios 10
2.4 TDD/TTY Configuration Test Scenarios 11
2.5 Computer Aided Dispatch and Mapping Integrations Test Scenarios 12
2.6 Logging and Instant Recall Recorders Test Scenarios 13
2.7 Management Information Systems Test Scenarios 13
2.8 System Administration Test Scenarios 16
2.9 System Performance Test Scenarios 18
2.10 Maintenance and Support Test Scenarios 19
2.11 System Monitoring Test Scenarios 21
2.12 Master Clock Test Scenarios 21
2.13 Administrative Reports Test Scenarios 22
3.0 Testing at IIT (In Progress as of filing with ICC for Pilot Application) 24
Figure 3.1 - IIT Test Lab Configuration 25
3.1 Resiliency Test Plan 26
3.2 Security Test Plan 28
3.3 Performance Test Plan 29
4.0 Vendor Testing 30
5.0 Part 725 Compliance 31
Table 5.1 Cross Reference of Carriers, NXXs, and PSAP in the CSI Territory 32
References 36

This page intentionally left blank

1.0 Overview

This Test Plan has been developed to test the functionality of the Next Generation system being deployed by the Counties of Southern Illinois, (CSI). The intent of CSI is to deploy an IP-Based Next Generation 9-1-1 communication system in the 15-county southern Illinois area. CSI intends to upgrade aging analog 9-1-1 telephony systems with an IP-based solution that meets NENA NG 9-1-1 standards, including the emerging NENA IP-Capable PSAP standards. The desired results will be increased functionality, redundancy, diversity, and scalability.

Section 2.0 provides a series of test cases that are designed to validate that the system matches the original requirements as determined by CSI in their original Request For Proposal, (RFP). Each test case has been identified with the applicable section in the RFP, with a specific Test Case number, Test Case Description, the expected successful outcome of the test case and the actual outcome of the test case. There are some tests that do not require any traffic or call attempt results, and those can be performed any time. Tests that validate call handling can be performed after the system is turned up, and operators and support persons are trained. Test calls will be employed to test certain cases while others will be performed after access carrier facilities have been turned up. Other tests involve the review of information collected by handling calls over a large period of time and will be scheduled later in the testing cycle.

Section 3.0 describes the testing that is being performed in association with the Illinois Institute of Technology, (IIT), which will determine if key components of the design function in a resilient and secure fashion, and perform well under a simulated load.

Section 4.0 describes the testing that will be performed with various vendors of components of the system, taking advantage of tools and automated procedures used during installation validation.

Section 5.0 describes call through testing, so that CSI 9-1-1 system management can ensure that, prior to the 9-1-1 system being able to announce its availability to the public, call through and field testing has been performed to the extent, and in the areas, that are specified by Title 83 Administrative Code Part 725.

2.0 Next Generation 9-1-1 System Requirements Test Cases

The following sections provide a brief description of the various functions related to the ESInet and i3 specifications as well as test cases and expected responses for each function. The test cases have also been ordered such that they build on data that is produced by a previous test case, rather than based on the order as defined in the RFP document. The areas to be tested are listed below.

1. Network and Carrier Configuration Test Scenarios
2. PSAP Configuration Test Scenarios
3. Future PSAP Configuration Test Scenarios
4. TDD/TTY Configuration Test Scenarios
5. Computer Aided Dispatch and Mapping Integrations Test Scenarios
6. Logging and Instant Recall Recorders Test Scenarios
7. Management Information Systems Test Scenarios
8. System Administration Test Scenarios
9. System Performance Test Scenarios
10. Maintenance and Support Test Scenarios
11. System Monitoring Test Scenarios
12. Master Clock Test Scenarios
13. Administrative Reports Test Scenarios

<u>Note on adherence to applicable standards:</u>

It should be noted that the test cases performed below serve also as test cases for the NENA standards that comprise the Next Generation 9-1-1 system functional elements and protocols. In particular, this test plan will validate the following list of NENA standards as they apply to this project. (For terminology definitions refer to the NENA Standards Exhibits and the Design Plan - Assure911.net-DG-CSI/NG911-001.)

- Flexible Call routing via Services Routing Protocol (ESRP)
- Database queries into the Emergency Call Routing Function (ECRF) using the Location to Service Translation (LoST) protocol
- Origination using legacy signaling through the Legacy Network Gateway (LNG)
- SIP Origination using SIP Protocol, through the Border Control Function (BCF)

2.1 Network and Carrier Configuration Test Scenarios

The following test cases align with the requirements specified in Section III of the RFP to support various Network and Access Carrier Configurations. These tests will be performed after the system has been installed; operators and support persons are trained, and as facilities are turned up. The test cases that are relevant to a particular type of carrier facility can be tested as those particular facilities are activated. If feasible, the Test cases that represent a facility type for which there are multiple carriers and may be repeated for each carrier.

Test Case #	Test Description	Expected Test Outcome Notes	Results
III-NC-001	Demonstrate the ability to support multiple types of inbound and outbound analog or digital Central Office or End Office provisioning, such as SS7, PRI/ISDN, CAMA, Feature Groups C & D, etc.		
III-NC-001-1	SS7 – Work with carrier to place test call from Central Office or End Office locations that are linked to the Data Centers via SS7 signaling		
III-NC-001-2	CAMA - – Work with carrier to place test call from Central Office or End Office locations that are linked to the Data Centers via CAMA signaling		
III-NC-002	Demonstrate the ability to provide a local termination/demarcation point for carriers while maintaining overall call routing configuration.		

III-NC-003	Test that the solution is capable of receiving both 9-1-1 and administrative calls in a native SIP format upon installation.		
III-NC-004	Test that the system can provide selective routing of inbound 9-1-1 calls based on customer-provided Emergency Service Zones (ESZ)		
III-NC-005	Test for the ability to accept automated update of Selective Routing information from MSAG processing.		
III-NC-006	Test for a situation where a primary PSAP is out of service, or that all circuits to that PSAP are out of service, 9-1-1 calls can be routed to an alternate PSAP.		
III-NC-007	Test that the system can provide the ability to test inbound call routing of all carriers on an ongoing basis after implementation.		
III-NC-008	Test for the ability to support additional one-button transfers to other entities.		
III-NC-009	Test that transferred calls can provide original caller's ANI/ESRK rather than the PSAP's ID.		
III-NC-010	Test that emergency callers can receive automated announcement or other indication of call status if their call is queued or not answered.		
III-NC-011	Test for real-time measurement of Quality of Service for network infrastructure.		
III-NC-012	Test for applicable bandwidth requirements including between PSAPs and support facilities.		
III-NC-013	Test for reliable call handling in the case of hardware or application with a call in progress.		
III-NC-014	Test that System provides a native IP environment for the receipt of Voice over Internet Protocol (VoIP) 9-1-1 calls with associated data is available.		
III-NC-015	Test for applicable integration options		

	with administrative telephone systems for consolidation of call taking platforms		
III-NC-016	Test that the System is be capable of expansion to multiple additional counties/PSAPs by adding additional software and hardware.		

2.2 PSAP Configuration Test Scenarios

The following test cases align with the requirements specified in Section III of the RFP to support various PSAP Equipment configurations. These tests will be performed after the system has been installed; operators and support persons are trained, and as facilities are turned up. The test cases that are relevant to a particular type of call origination type can be tested as those particular facilities are activated.

Test Case #	Test Description	Expected Test Outcome Notes	Results
III-PSAP-001	Validate that all material respects to current NENA recommendations for PSAP Equipment.		
III-PSAP-001-1	Validate that all material respects to current NENA recommendations for NENA 04-001, Standards for PSAP Equipment		
III-PSAP-001-2	Validate NENA 04-004, Standards for PSAP Intelligent Workstations		
III-PSAP-001-3	Validate NENA 08-002, Functional and interface Standards NG9-1-1 (i3)		
III-PSAP-001-4	Validate NENA 08-501, Network Interface to IP capable PSAP		
III-PSAP-001-5	NENA 08-502, E9-1-1 Requirements.		
III-PSAP-001-6	Validate that a back-up SIP phone that is located at each call taker position. can display ANI/ALI.		
III-PSAP-002	Validate the backup telephone instruments are		

	provided with handsets and function independently or in parallel with the Intelligent Work Stations.		
III-PSAP-003	Validate the ability to place calls on hold for retrieval by any call taker (Call Park).		
III-PSAP-004	Test for the delivery of Automatic Number Identification (ANI) and Automatic Location Identification (ALI) data display in a consistent format regardless of the originating carrier or routing of the call.		
III-PSAP-005	Validate that PSAP equipment can retrieve ALI equivalent information from customer's database system.		
III-PSAP-006	Validate that PSAP equipment can provide for ALI retrieval from Caller ID (Business Lines) or manually entered telephone number.		
III-PSAP-007	Validate that the System can accommodate the handling and display of Wireless 9-1-1 Phase I and Phase II information, including Confidence and Uncertainty calls from other jurisdictions.		
III-PSAP-008	Test for the ability to support access to multiple ALI databases (e.g., to query ALI of transferred wireless 9-1-1		
III-PSAP-009	Validate that an Intelligent Workstation provides history of prior calls at time of call presentation to call taker.		
III-PSAP-010	Validate the presence of an Intelligent Workstation platform to support the installation of third-party applications.		
III-PSAP-011	Validate that peripheral network components (such as telephone instruments) outside of centralized equipment rooms deliver supplemental electrical power via Power Over Ethernet (POE) provisioning.		
III-PSAP-012	Test the ability to monitor the audio of call taking at another position, with or without		

	muting.		
III-PSAP-013	Test the ability to 'barge-in' to a call in progress by supervisory personnel.		
III-PSAP-014	Test the ability to conference calls with unlimited outside party's vendor to describe any limitations.		
III-PSAP-015	Test the ability to support separate inbound call queues if circuit provisioning is deployed.		
III-PSAP-016	Test the ability to support one-button re-dialing of recent calls, including abandoned calls.		
III-PSAP-017	Validate the ability to capture abandoned call information for call taker use.		
III-PSAP-018	Test the ability to display location information at each call taker position for calls pending.		
III-PSAP-019	Test the ability to provide system-wide status at each PSAP, reflecting system availability, calls in progress, call taker availability, and calls in queue.		
III-PSAP-020	Validate the Creation of Incoming Call Queues		
III-PSAP-021	Validate the Creation of Spatial Incoming Call Queues		
III-PSAP-022	Test the ability to integrate two-way audio from telephone calls and radio traffic into one headset		

2.3 Future PSAP Configuration Test Scenarios

The following test cases align with the requirements specified in Section III of the RFP to support various future PSAP Equipment configurations. These test cases can be performed at any time after the system is delivered, as they may not involve the testing of any physical portion of the system.

Test Case #	Test Description	Expected Test Outcome Notes	Results
III-FP-001	Validate that the Vendor has described how their solution aligns with the current NENA, ESIF, ATIS, IETF standards today.		
III-FP-002	Validate that the Vendor has described their migration path to receive Automatic Crash Notification and Telematics information with 9-1-1 calls.		

2.4 TDD/TTY Configuration Test Scenarios

The following test cases align with the requirements specified in Section III of the RFP to support various TDD/TTY configurations. These tests will be performed after the system has been installed; operators and support persons are trained, and as facilities are turned up.

Test Case #	Test Description	Expected Test Outcome Notes	Results
III-TDD-001	Validate the ability to support Baudot–format TDD/TTY dialogue from callers at every position.		
III-TDD-002	Validate the ability to provide TDD/TTY detection and alerting at each call taker position		
III-TDD-003	Validate the ability to capture and provide permanent record of TDD/TTY dialogue; vendor to describe approach to TDD/TTY call logging. Ability to support Instant Messaging (IM) and Short Messaging Service (SMS) and text		

	messaging dialogue from public ‘callers.’		

2.5 Computer Aided Dispatch and Mapping Integrations Test Scenarios

The following test cases align with the requirements specified in Section III of the RFP to support various Computer Aided Dispatch and Mapping configurations. These tests will be performed after the system has been installed; operators and support persons are trained, and as facilities are turned up.

Test Case #	Test Description	Expected Test Outcome Notes	Results
III-CAD-001	Test for the ability to transfer all of the available ANI/ALI data into a CAD incident entry application, including location lat-long data.		
III-CAD-002	Test for the ability to interface to third-party or vendor mapping application for real-time display of inbound call information		
III-CAD-003	Test for the ability to interface to an Integrated mapped ALI display.		
III-CAD-004	Test for the ability to support integrated mapping application co-resident on Intelligent Workstation.		

2.6 Logging and Instant Recall Recorders Test Scenarios

The following test cases align with the requirements specified in Section III of the RFP to support Logging and Instant Recall Recorders. These tests will be performed after the system has been installed; operators and support persons are trained, and as facilities are turned up.

Test Case #	Test Description	Expected Test Outcome Notes	Results
III-LOGIR-001	Test the data logging system to ensure it has capability to handle multi-media recording in the future.		
III-LOGIR-002	Test the Instant Recall Recording and playback application software at each workstation position with the ability to integrate with existing analog voice logging recorder at each PSAP.		

2.7 Management Information Systems Test Scenarios

The following test cases align with the requirements specified in Section III of the RFP to support Management Information Systems. These tests will be performed after the system has been installed; operators and support persons are trained, and as facilities are turned up. Further, since some of these tests involve the review of information collected by handling calls, those tests cases should be performed after earlier test cases that generate calls.

Test Case #	Test Description	Expected Test Outcome Notes	Results
III-MIS-001	Validate the System Management Information System (MIS) reporting of transaction volumes and system performance for overall system as		

	well as significant components.		
III-MIS-001-a	Test that the MIS and reporting application can allow access to all captured database elements.		
III-MIS-001-b	Test the Detail of MIS reporting to provide for both individual PSAP and system-wide transaction volumes and call handling performance.		
III-MIS-001-c	Test that the MIS reporting can provide for time and day of week in tabular and graphical formats.		
III-MIS-001-d	Test that the Reporting application can provide for selection of indexing and sorting keys by any formatted field.		
III-MIS-001-e	Test that the MIS can capture and report System Availability, including alarms, error reports, and platform status.		
III-MIS-001-f	Test that the MIS can capture response time to PSAP ALI database inquiries and re-bids.		
III-MIS-001-g	Test that the MIS is be capable of capturing data from all circuits within the system, including inbound 9-1-1trunks, administrative lines and dedicated ring down circuits, as well as outbound calling.		
III-MIS-002	Test that access to information shall be acquired remotely by permissions.		
III-MIS-002-a	Test that the MIS can collect data on the Number of total calls received		
III-MIS-002-b	Test that the MIS can collect data on the Number of abandoned calls		
III-MIS-002-c	Test that the MIS can collect data on the Number of calls on a per trunk/per circuit basis		
III-MIS-002-d	Test that the MIS can collect data on the Number of calls on a call type (wire line, wireless, VOIP, etc.) basis		
III-MIS-002-e	Test that the MIS can collect data on the Number of calls conference/transferred		

III-MIS-002-f	Test that the MIS can collect data on the Calls conference/transferred by destination (e.g.,secondary PSAPs)		
III-MIS-002-g	Test that the MIS can collect data on the Number of calls on a log-on or per position basis		
III-MIS-002-h	Test that the MIS can collect data on the Average time to answer		
III-MIS-002-i	Test that the MIS can collect data on the Average length of call and average hold time		
III-MIS-003	Test that each data center is equipped with a Call Detail Record (CDR) function that provides for capture, search and retrieval, display, and printing of information regarding each 9-1-1 call. The MIS be able to process data with the following configurations.		
III-MIS-003-a	Test that the MIS can collect data on the Date received		
III-MIS-003-b	Test that the MIS can collect data on the Trunk seize/call appearance time		
III-MIS-003-c	Test that the MIS can collect data on the Caller's telephone number		
III-MIS-003-d	Test that the MIS can collect data on the ANI, ESRK or other routing identification		
III-MIS-003-e	Test that the MIS can collect data on the Answer time		
III-MIS-003-f	Test that the MIS can collect data on the Answering position identification		
III-MIS-003-g	Test that the MIS can collect data on the Trunk/circuit identification		
III-MIS-003-h	Test that the MIS can collect data on the Time call was released		
III-MIS-003-i	Test that the MIS can collect data on the Time call was transferred		
III-MIS-003-j	Test that the MIS can collect data on the Transfer destination		

III-MIS-003-k	Test that the MIS can collect data on the Abandoned call indicator		
III-MIS-003-l	Test that the MIS can collect data on the Ringing start time		
III-MIS-003-m	Test that the MIS can collect data on the Time call was placed on hold and taken off hold and by what position		
III-MIS-003-n	Test that the MIS can collect data on the All ALI data, including name, address, community, ESN, Class of Service, etc. Data may be accessed remotely from the PSAPs with permissions.		
III-MIS-004	Test the ability to direct MIS reports or Workstation printouts to any Local Area Network-attached printer.		
III-MIS-005	Test the ability to export formatted detailed records or summary report tables for analysis with third-party applications (e.g., Microsoft Office)		
III-MIS-006	Test the ability of the MIS reporting to be fully initialized prior to operational use of system; this includes any procedures, routines and scripts for daily, monthly and annual periodic reporting.		

2.8 System Administration Test Scenarios

The following test cases align with the requirements specified in Section III of the RFP to support System Administration. These tests will be performed after the system has been installed; operators and support persons are trained, and as facilities are turned up. Further, since some of these tests involve the review of information collected by handling calls, those tests cases should be performed after earlier test cases that generate calls.

Test Case #	Test Description	Expected Test Outcome Notes	Results
III-SA-001	Test the ability for the customer to administer appropriate system features and configuration without voiding warranty or support agreements.		
III-SA-002	Test the ability for customer to administer call queuing and call routing parameters.		
III-SA-003	Test the ability to support centralized and customer administered backup and recovery policies.		
III-SA-004	Test the ability to support on-line centralized backup		
III-SA-005	Test the ability of the System to support use of generally available third-party platform protection products, such as anti-virus, spyware and Trojan protection applications. Vendor to specify responsibility for updates to applications and signature files.		
III-SA-006	Test that the Vendor can describe the implementation of end-to-end security and authentication in the proposed configuration.		
III-SA-007	Test the Ability to automatically provide outbound pager and email notification to support personnel of system events and alarms.		
III-SA-008	Test that the system can provide real-time call volume and call status information at remote locations		
III-SA-008-a	Test that the system can provide Positions Logged On/Ready/Available		
III-SA-008-b	Test that the system can provide Positions Busy/Off Hook		
III-SA-008-c	Test that the system can provide Positions Not Ready/Out of Queue		
III-SA-008-d	Test that the system can provide Calls in		

	Queue/Calls Pending		
III-SA-008-e	Test that the system can provide Calls Holding/Calls Parked		
III-SA-008-f	Test that the system can provide PSAP Status (e.g., system OK, connectivity good)		
III-SA-009	Test that the system can provide the Ability to provide a real-time display of system availability, call taker availability & calls in progress.		

2.9 System Performance Test Scenarios

The following test cases align with the requirements specified in Section III of the RFP to support System Performance. These tests will be performed after the system has been installed; operators and support persons are trained, and as facilities are turned up. Further, since some of these tests involve the review of information collected by handling calls over a large period of time, of after a large volume of calls, those tests cases should be performed after earlier test cases that generate calls, or scheduled to be performed later in the project cycle.

Test Case #	Test Description	Expected Test Outcome Notes	Results
III-SP-001	Test the system's ability to provide overall 99.999% availability, measured on a 24 hour per day, 7-day per week basis, accumulated over a one year period. Vendor to clarify compliance and/or describe any exceptions.		
III-SP-002	Test the ability of the system to support automated, unassisted restoration from stoppages or outages, including significant network components and application software.		
III-SP-003	Test the ability of the system to provide positive/affirmative alert to each call taker position of off-line status, error conditions or		

	conditional events.		
III-SP-004	Test the ability of the system to support localized supervision and reporting of ANI and ALI failures, network outages, etc.		
III-SP-005	Test the ability of the system to provide in each PSAP readily visible and (selectable) audible indicators of emergency and non-emergency calls pending.		
III-SP-006	Validate that the vendor has described their recommended approach to node and link redundancy to meet Availability Performance Requirements.		
III-SP-007	Validate that the vendor has described their system architecture as it relates to failover and fault tolerance, including the gateway into the 9-1-1 IP network, traffic paths to the network endpoints, and any crucial devices within the scope of the relevant network fabric.		

2.10 Maintenance and Support Test Scenarios

The following test cases align with the requirements specified in Section III of the RFP to support Maintenance and Support. These tests will be performed after the system has been installed; operators and support persons are trained, and as facilities are turned up. Further, since some of these tests involve the review of information collected by having the system in place for a large period of time, those tests cases should be performed later in the project cycle.

Test Case #	Test Description	Expected Test Outcome Notes	Results
III-MS-001	Validate that the vendor has provided a fixed cost for annual tier 2/tier 3 maintenance after the warranty period.		
III-MS-001a	Validate that the vendor has provided a proposed Maintenance and Support scope of		

	services statement with proposal response.		
III-MS-002	Validate that the vendor has provided full and complete set of technical and maintenance documentation at each primary installation location.		
III-MS-003	Validate that an on-going trouble report tracking system and historical records of trouble reports and problem resolution can be maintained.		
III-MS-004	Validate that the vendor has recommended a complement of essential and recommended spare parts and component assemblies to be locally maintained; on-site secure storage will be made available at each PSAP		
III-MS-005	Validate that a remote access for system and application diagnostics and maintenance can be established. Vendor to coordinate Virtual Private Network (VPN) or other secure access requirements with the CSI Information Technology staff.		
III-MS-006	Validate that the vendor has recommended anticipates the need for on-site, factory-trained staff, capable of diagnosing and supporting the installation of this platform.		
III-MS-007	Validate that the vendor has the ability to coordinate all maintenance activities with each PSAP. Vendor and PSAP to agree on migration checklist and notification schedule for any activities impacting operations.		

2.11 System Monitoring Test Scenarios

The following test cases align with the requirements specified in Section III of the RFP to provide System Monitoring. These tests will be performed after the system has been installed; operators and support persons are trained, and as facilities are turned up. Further, since some of these tests involve the review of information collected by handling calls over a large period of time, of after a large volume of calls, those tests cases should be performed after earlier test cases that generate calls, or scheduled to be performed later in the project cycle.

Test Case #	Test Description	Expected Test Outcome Notes	Results
III-MON-001	Test that the system can provide error logs and diagnostic information sufficient to support vendor troubleshooting.		
III-MON-002	Test that the system collects sufficient information to give the CSI IT staff an end-to-end view of the ability of incoming calls to be completed		

2.12 Master Clock Test Scenarios

The following test cases align with the requirements specified in Section III of the RFP to provide the Master Clock. These tests will be performed after the system has been installed.

Test Case #	Test Description	Expected Test Outcome Notes	Results
III-MC-001	Test to ensure that the master clock subsystem can provide NTP (Network Time Protocol) and SNTP (Simple Network Time Protocol) time synchronization outputs for additional		

	information systems.		
III-MC-001-a	Test to ensure that the master clock subsystem can provide timing to the Computer Aided Dispatch		
III-MC-001-b	Test to ensure that the master clock subsystem can provide timing to the Database and Communications Servers		
III-MC-001-c	Test to ensure that the master clock subsystem can provide timing to the Logging Recorders		
III-MC-002	Test to ensure that the master clock subsystem can provide a time synchronization source to all PSAPs		

2.13 Administrative Reports Test Scenarios

The following test cases align with the requirements specified in Section III of the RFP to provide various Administrative Reports.

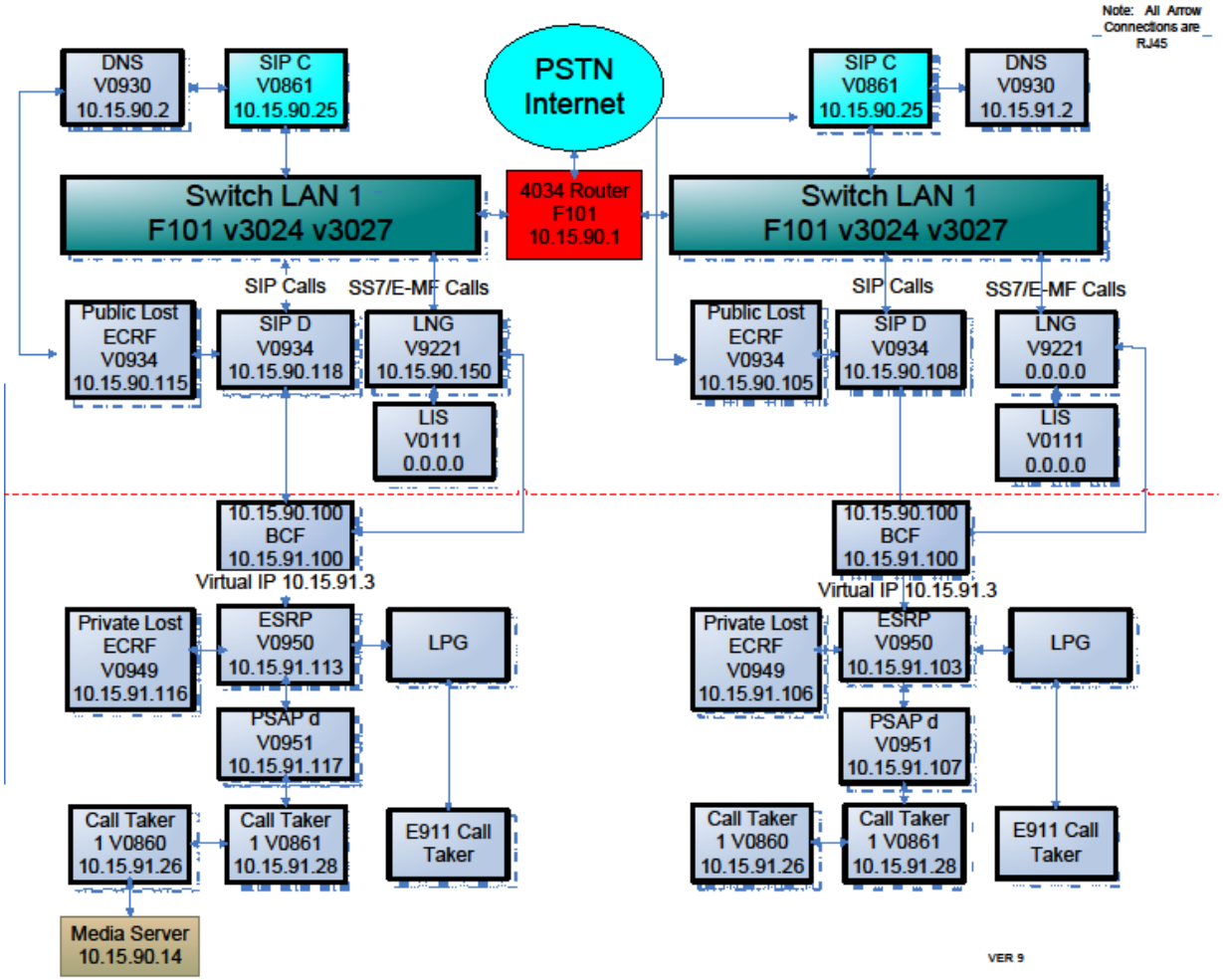
Test Case #	Test Description	Expected Test Outcome Notes	Results
III-AR-001	Test that a TN Tally Report can be generated.		
III-AR-002	Test that a TN Tally Report by Community can be generated.		
III-AR-003	Test that a Service Order Fallout Report can be generated.		
III-AR-004	Test that a Service Order Update Report can be generated.		
III-AR-005	Test that a Service Order Updates 24 Hour Report can be generated.		
III-AR-006	Test that a Service Order Processing Statistics Report can be generated.		
III-AR-007	Test that a Service Order Corrections Statistics		

	Report can be generated.		
III-AR-008	Test that a Service Order Processing Errors Report can be generated.		
III-AR-009	Test that a Service Order Error Codes Report can be generated.		
III-AR-010	Test that an MSAG Updates Report can be generated.		
III-AR-011	Test that an NRF Summary and Detail Reports can be generated.		
III-AR-012	Test that an MSAG Overlaps Audit Report can be generated.		
III-AR-013	Test that an MSAG Parity Report can be generated.		
III-AR-014	Test that an MSAG Change Requests Report can be generated.		
III-AR-015	Test that an ALI Audit: GIS site match Report can be generated.		
III-AR-016	Test that a TNs by Community for Liaisons Report can be generated.		
III-AR-017	Test that an Unnumbered Addresses Report can be generated.		

3.0 Testing at IIT (In Progress as of filing with ICC for Pilot Application)

Testing will be conducted in the Illinois Institute of Technology (IIT) Real-Time Communications Lab (RTCL). IIT students will have the goal of validating the design and configuration of ESInet components based on the real-world NG911 network being deployed for CSI. IIT will configure a lab to match real world conditions, and iteratively identifying and testing failure mitigation strategies. IIT Testing and results will be provided to CSI via NG 911, Inc. upon completion.

Figure 3.1 - IIT Test Lab Configuration



The components of the CSI network design that will be tested at the IIT RTCL Lab are:
1. Resiliency to Network Element failures, and failures of layer 1 and layer 2 transport systems.
2. Performance of the design under heavy load conditions.
3. Security of information, and security from attacks that affect performance.

The lab may also participate in field-testing of the real-world CSI NG911 System components by interconnection of lab-based test fixtures with the actual ESInet components as they are being turned up in the field. Connectivity between the RTCL and the CSI ESInet will be procured by CSI or NG9-1-1, Inc.

3.1 Resiliency Test Plan

Test Case #	Test Description	Expected Test Outcome	Results
IIT-001	Place 911 test call from SIP UA and remove power from the ESRP IP address 10.15.91.113 Place 2nd test call and record both results	911 call is routed to the alternate ESRP IP address 10.15.91.103 via Virtual IP address 10.15.91.3	911 call is routed to the alternate ESRP IP address 10.15.91.103 via Virtual IP address 10.15.91.3
IIT-002	Place 911 test call from SIP UA and remove the RJ45 connection from ESRP to Switch 101 v3024 IP address 10.15.91.113 Place 2nd test call and record both results	911 call is routed to the alternate ESRP IP address 10.15.90.103 via Virtual IP address 10.15.90.3	911 call is routed to the alternate ESRP IP address 10.15.91.103 via Virtual IP address 10.15.91.3
IIT-003	Place 911 test call from SIP UA and remove power from the PSAP IP address 10.15.91.117 Place 2nd test call and record both results	911 call is routed to alternate PSAP IP address 10.15.90.107 via Virtual IP address 10.15.91.7	911 call is routed to alternate PSAP IP address 10.15.91.107 via Virtual IP address 10.15.91.7 Call Takers have to re-register to alternate PSAP after failover
IIT-004	Place 911 test call from SIP UA and remove the RJ45 connection from PSAP to Switch 101 v3024 IP address 10.15.91.117 and record both results	911 call is routed to alternate PSAP IP address 10.15.91.107 via Virtual IP address 10.15.9.7	911 call is routed to alternate PSAP IP address 10.15.91.107 via Virtual IP address 10.15.91.7 Call Takers have to re-register to alternate PSAP after failover
IIT-005	Place 911 test call from SIP UA and remove power from Call taker 1 IP Address 10.15.9.26 Place 2nd test call and record both results	The 911 call is routed to the 2nd Call Taker 10.15.91.28	The 2nd 911 test call is received by the 2nd call taker and the 3rd call routes to Queue

IIT-006	Place 911 Test call from SIP UA and remove RJ 45 connection from Call taker position to Switch 101 v0324 Place 2nd test call and record both results	911 call is routed to alternate Call Taker 10.15.91.28	The 2nd 911 test call is received by the 2nd call taker and the 3rd call routes to Queue
IIT-007	Place 911 CAMA/MF test call from the 314A CAMA test set and remove power from the ESRP. Place 2nd test call and record both results	911 Call is routed to the alternate ESInet	CAMA/MF 911 Call Routes to Alternate ESRP after power is removed from Primary ESRP
IIT-008	Place 911 CAMA/MF test call from the 314A CAMA test Set and remove the RJ45 connection from the ESRP Place 2nd test call and record both results	911 call is routed to the Alternate ESInet	CAMA/MF 911 Call Routes to Alternate ESRP after the ESRP looses connectivity to the Network
IIT-009	Test case reserved for future Pilot testing.		
IIT-010	Test case reserved for future Pilot testing.		
IIT-011	Place 911 Test call with manual location set and remove power to the private lost server ECRF function IP address 10.15.91.116 Place 2nd test call and record both results	911 call is routed to the alternate private lost server IP Address 10.15.91.106 via Virtual IP address 10.15.91.6 but the alternate private LOST location information will be used to forward the call instead.	911 call is routed to the alternate private lost server IP Address 10.15.91.106 via Virtual IP address 10.15.91.6 but the alternate private LOST location information will be used to forward the call instead.
IIT-012	Place 911 test call with manual location set and remove the RJ45 connection to the private lost server ECRF function IP address 10.15.91.116 Place 2nd test call and record both results	911 call is routed to the alternate private lost server IP Address 10.15.91.106 via Virtual IP address 10.15.91.6 but alternate private LOST location information will be used to forward the call instead.	911 call is routed to the alternate private lost server IP Address 10.15.91.106 via Virtual IP address 10.15.90.6 but alternate private LOST location information will be used to forward the call instead.

3.2 Security Test Plan

Test Case #	Test Description	Expected Test Outcome	Results
IIT-013	Access LNG using Telnet or SSH to IP Address 64.131.109.217	Access to the LNG management port is allowed for Authorized IP addresses	Access to LNG is allowed to IP address 64.131.109.217
IIT-014	Login to LNG with Root Login and Non-authorized Password	Access is denied except for users with authorized passwords	Access is Denied to users without the proper credentials
IIT-015	Login to LNG using non-authorized login and Password	Access is denied except for users with authorized logins and passwords	Access is Denied to users without The proper credentials
IIT-016	Login to LNG using authorized login and password	Access is allowed with Authorized Logins and Passwords	Access is allowed with Authorized Logins and Passwords.
IIT-017	Restrict Access to the BCF and ESInet from outside the network by denying access to other than authorized IP addresses.	Access BCF from outside the network using Non-Authorized IP Address.	An Access control list was created for Authorized IP address access. Attempts to access the BCF from non-authorized IP addresses are refused.
IIT-018	Login to BCF Management port using non-authorized logins and passwords	Access is Denied for non authorized users	Access is not allowed when attempting to access the BCF Management port
IIT-019	Allow Authorized Access to management port of the BCF	Users with non-Authorized Logins and passwords are denied access to the BCF Management port	Non Authorized users are denied. Only users listed in the SSH file are allowed
IIT-020	Restrict user privileges in the BCF on a per user login and password basis	Authorized users are restricted to their allowed access privileges	BCF Commands are restricted by assigned user privileges.
IIT-021	Call Taker/PSAP initiates outbound SIP call	Call completes from PSAP	Call completes to an available call taker when an outbound call is initiated.
IIT-022	PSAP/ Call Takers attempt to access Internet	Call takers cannot complete to the Internet	A call taker cannot complete to the internet when access is attempted
IIT-023	Allow normal inbound SIP call traffic and block unauthorized SIP sessions	SIP traffic allowed for trusted IP addresses only	Normal inbound SIP call traffic allowed and unauthorized SIP sessions blocked

3.3 Performance Test Plan

Test Case #	Test Description	Expected Test Outcome	Results
IIT-023	Generate multiple SIP test calls to the ESInet and observe performance.	SBC should forward all SIP Calls to the PSAP Call Takers	All Calls are sent to the available call takers
IIT-024	Generate Multiple SIP calls to the Session Boarder Controller (SBC)	SBC should forward all SIP Calls to the PSAP Call Takers	All Calls are sent to the available call takers
IIT -025	Generate Multiple test Calls to the Call taker positions until all are busy	Calls should Queue and release as positions become available	All calls Queue when available call takers are busy.
IIT-026	Verify the ability of the Call Taker to transfer a call to another PSAP	Call Taker successfully transfers A call	A call taker successfully transferred a call to a 3rd call taker
IIT-027	Generate Multiple invite messages to the ESRP and observer performance.	The ESRP should accept all invites until limits are reached.	The ESRP accepted approx. 16000 invite messages and then reached a Q full status. Rebooted ESRP as a result of failure
IIT-028	Generate Multiple Invite messages to the SBC and ESInet to simulate a DDoS attack and then observe performance.	The SBC should accept all invite messages until failure. The SBC is not configured to prevent a DDoS attack during this test	The SBC forwarded approx 16000 invite messages from the MU-8000 to the ESInet and then generated 503 server busy and 408 timeout messages. Rebooted BCF as a result of failure
IIT-029	Generate registrations without authorization to Call takers	The Call takers should register to PSAP.	62000 registrations were generated by the MU-8000. 40,000 passed with 22,000 errors Rebooted PSAP
IIT-030	Generate Multiple Invite messages to the SBC and ESInet to simulate a DDoS attack with the SBC configured to throttle requests	The SBC should allow multiple invite request based on the programmed parameters of the SBC	Multiple Invite messages generated to the SBC and ESInet simulates a DDoS attack with the SBC configured to throttle requests

4.0 Vendor Testing

The system being installed is comprised of components from a variety of manufacturers, each of which has their requisite installation validation test plan. The test cases contained therein will be performed as part of the overall project testing activities, at the time that the installations are made, or after the components are configured properly to perform their function in the system.

Test Case #	Test Description	Expected Test Outcome Notes	Results
IV-VENDOR-001	Test that vendor Session Border Control equipment passes vendor installation test		
IV-VENDOR-002	Test that vendor Emergency Services Routing Proxy equipment passes vendor installation test		
IV-VENDOR-003	Test that vendor PSAP equipment passes vendor installation test		

The system will further be tested after the components are turned up and integrated using certain vendor tools. The database and call routing functions will be tested using a call generator. This vendor utility is capable of simulating originating calls from multiple varied locations representing the different served communities.

Test Case #	Test Description	Expected Test Outcome Notes	Results
IV-VENDOR-004	Test that calls from each served origination point is routed to the correct PSAP.		

5.0 Part 725 Compliance

In the event that CSI must perform testing to be compliant with Title 83 Administrative Code Part 725, this section provides the plan for testing with originating service providers to achieve the call through testing is required prior to going on-line. The table listing the NPA-NXXs, table 5.1, which has been developed based on information provided by CSI, will be further refined as conversations with carriers take place.

This section describes how CSI 9-1-1-system management will perform the testing set forth in Title 83 Administrative Code Part 725.

The test cases below allow CSI 9-1-1 system management to ensure that, prior to the 9-1-1 system being able to announce its availability to the public, call through and field testing has been performed on:

1. A minimum of 40% of all access lines in the 9-1-1 service area
2. Each NXX for every participating telecommunications carrier
3. For every ESN within each telecommunications carrier's service

Test Case #	Test Description	Expected Test Outcome Notes	Results
V-SECT725-000	Perform Call Through Testing for NXXs, Carrier, and PSAP combinations shown on the table below		

Table 5.1 Cross Reference of Carriers, NXXs, and PSAP in the CSI Territory

Test Case #	Carrier	NXX	Target PSAP	Percent of Service Area	Results
V-SECT725-001	AT&T CAIRILCFDS0	Mound City 618-748	Pulaski CSO Dept. Union County Sheriff		
V-SECT725-001	AT&T CAIRILCFDS0	Mounds 618-745	Pulaski CSO Dept. Union County Sheriff		
V-SECT725-002	AT&T CAIRILCFDS0	Olmsted 618-742	Pulaski CSO Dept. Union County Sheriff		
V-SECT725-003	AT&T CAIRILCFDS0	Tamms 618-747	Union County Sheriff Pulaski County Sheriff		
V-SECT725-004	AT&T TBD	McClure 618-661	Union County Sheriff Pulaski County Sheriff		
V-SECT725-005	Citizen WDLWILXEDS0	Dubois 618-787	Perry County Sheriff Duquoin City Police Administration Office		
V-SECT725-006	Citizen WDLWILXEDS0	Tamaroa 618-496	Perry County Sheriff Duquoin City Police Administration Office		
V-SECT725-007	Crossville TBD	Crossville 618-966	White County Sheriff Wabash County Sheriff		
V-SECT725-008	Egyptian BLDWILXEDS0	Glenn 618-763	Jackson County Sheriff Murphysboro PD Carbondale PD SIU PD		
V-SECT725-009	Egyptian BLDWILXEDS0	Oakdale 618-329	Perry County Sheriff Duquoin City Police Administration Office		
V-SECT725-010	Egyptian BLDWILXEDS0	Rice 618-336	Perry County Sheriff Duquoin City Police Administration Office		
V-SECT725-011	Frontier ALMTILXEDS0	Edgewood 618-238	Flora Police Dept Richland County Sheriff		
V-SECT725-012	Frontier ALMTILXEDS0	Farina 618-245	Flora Police Dept Richland County Sheriff		
V-SECT725-013	Frontier LRVLILXEDS0	Chauncey 618-947	Wabash County Sheriff Richland County Sheriff		
V-SECT725-014	Frontier LRVLILXEDS0	Sumner 618-936	Wabash County Sheriff Richland County Sheriff		
V-SECT725-015	Frontier TBD	W. Salem 618-456	Wabash County Sheriff Richland County Sheriff		
V-SECT725-016	Frontier OLNYILXEDS0	Calhoun 618-863	Wabash County Sheriff Richland County Sheriff		
V-SECT725-017	Frontier OLNYILXEDS0	Claremont 618-869	Wabash County Sheriff Richland County Sheriff		
V-SECT725-018	Frontier OLNYILXEDS0	Noble 618-723	Wabash County Sheriff Richland County Sheriff		
V-SECT725-019	Frontier OLNYILXEDS0	Parkersburg 618-442	Wabash County Sheriff Richland County Sheriff		
V-SECT725-020	Frontier WNDNILXEDS0	Dundas 618-754	Wabash County Sheriff Richland County Sheriff		
V-SECT725-021	Hamilton DHLGILXEDS0	Blairsville 618-757	White County Sheriff Wabash County Sheriff		
V-SECT725-022	Hamilton DHLGILXEDS0	Broughton 618-647	Saline County Detention Johnson County Sheriff		

V-SECT725-023	Shawnee RSCLILXEDS0	Cave-In-Rock 618-289	Saline County Sheriff Johnson County Sheriff		
V-SECT725-024	Shawnee RSCLILXEDS0	Equality 618-276	Saline County Detention Johnson County Sheriff		
V-SECT725-025	Shawnee RSCLILXEDS0	Equality 618-276	Saline County Sheriff Johnson County Sheriff		
V-SECT725-026	Shawnee RSCLILXEDS0	Leamington 618-273	Saline County Sheriff Johnson County Sheriff		
V-SECT725-027	Shawnee RSCLILXEDS0	Leamington 618-276	Saline County Detention Johnson County Sheriff		
V-SECT725-028	Shawnee SMSNILXEDS0	Renshaw 618-949	Johnson County Sheriff Saline County Detention		
V-SECT725-029	Verizon ANNAILXEDS0	Cobden 618-893	Jackson County Sheriff Murphysboro PD Carbondale PD SIU PD		
V-SECT725-030	Verizon ANNAILXEDS0	Cobden 618-893	Unon County Sheriff Pulaski County Sheriff		
V-SECT725-031	Verizon ANNAILXEDS0	Cypress 618-657	Johnson County Sheriff Saline County Detention		
V-SECT725-032	Verizon ANNAILXEDS0	Cypress 618-657	Pulaski CSO Dept. Union County Sheriff		
V-SECT725-033	Verizon ANNAILXEDS0	Cypress 618-657	Unon County Sheriff Pulaski County Sheriff		
V-SECT725-034	Verizon ANNAILXEDS0	Dongola 618-827	Pulaski CSO Dept. Union County Sheriff		
V-SECT725-035	Verizon ANNAILXEDS0	Dongola 618-827	Unon County Sheriff Pulaski County Sheriff		
V-SECT725-036	Verizon ANNAILXEDS0	Karnak 618-634	Johnson County Sheriff Saline County Detention		
V-SECT725-037	Verizon ANNAILXEDS0	Karnak 618-634	Massac County Sheriff Metrolpolis Police		
V-SECT725-038	Verizon ANNAILXEDS0	Karnak 618-634	Pulaski CSO Dept. Union County Sheriff		
V-SECT725-039	Verizon ANNAILXEDS0	Ullin 618-845	Pulaski CSO Dept. Union County Sheriff		
V-SECT725-040	Verizon ANNAILXEDS0	Villa Ridge 618-342	Pulaski CSO Dept. Union County Sheriff		
V-SECT725-041	Verizon CARMILXEDS0	Enfield 618-963	White County Sheriff Wabash County Sheriff		
V-SECT725-042	Verizon CARMILXEDS0	Grayville 618-375	White County Sheriff Wabash County Sheriff		
V-SECT725-043	Verizon CARMILXEDS0	Maunie 618-968	White County Sheriff Wabash County Sheriff		
V-SECT725-044	Verizon CBDLILXEDS0	Desoto 618-867	Jackson County Sheriff Murphysboro PD Carbondale PD SIU PD		
V-SECT725-045	Verizon CBDLILXEDS0	Hurst 618-987	Jackson County Sheriff Murphysboro PD Carbondale PD SIU PD		
V-SECT725-046	Verizon CBDLILXEDS0	Roylton 618-984	Jackson County Sheriff Murphysboro PD Carbondale PD SIU PD		
V-SECT725-047	Verizon CRDLILXEDS0	Ava 618-426	Jackson County Sheriff Murphysboro PD Carbondale PD SIU PD		
V-SECT725-048	Verizon CRDLILXEDS0	Ava 618-426	Perry County Sheriff Duquoin City Police Administration Office		
V-SECT725-049	Verizon CRDLILXEDS0	Hurst 618-987	Williamson County Sheriff Herrin Police Dept		
V-SECT725-050	Verizon CRDLILXEDS0	Royalton 618-984	Williamson County Sheriff Herrin Police Dept		
V-SECT725-051	Verizon DUQNILXEDS0	Elkville 618-568	Jackson County Sheriff Murphysboro PD		

			Carbondale PD SIU PD		
V-SECT725-052	Verizon DUQNILXEDS0	Elkville 618-568	Perry County Sheriff DuQuoin City Police		
V-SECT725-053	Verizon ELRDILXEDS0	Ridgeway 618-272	Saline County Detention Johnson County Sheriff		
V-SECT725-054	Verizon ELRDILXEDS0	Shawneetown 618-269	Saline County Sheriff Johnson County Sheriff		
V-SECT725-055	Verizon FLORILXEDS0	Clay City 618-676	Flora Police Dept Richland County Sheriff		
V-SECT725-056	Verizon FRFDILXEDS0	Burnt Prairie 618-896	White County Sheriff Wabash County Sheriff		
V-SECT725-057	Verizon HRBGILXEDS0	Carrier Mills 618-994	Saline County Detention Johnson County Sheriff		
V-SECT725-058	Verizon HRBGILXEDS0	Carrier Mills 618-994	Williamson County Sheriff Herrin Police Dept		
V-SECT725-059	Verizon HRBGILXEDS0	Stonefort 618-777	Johnson County Sheriff Saline County Detention		
V-SECT725-060	Verizon HRBGILXEDS0	Stonefort 618-777	Saline County Detention Johnson County Sheriff		
V-SECT725-061	Verizon HRBGILXEDS0	Stonefort 618-777	Williamson County Sheriff Herrin Police Dept		
V-SECT725-062	Verizon MARNILXE1ED	Creal Springs 618-996	Johnson County Sheriff Saline County Detention		
V-SECT725-063	Verizon MARNILXE1ED	Creal Springs 618-996	Williamson County Sheriff Herrin Police Dept		
V-SECT725-064	Verizon MARNILXE1ED	Goreville 618-995	Johnson County Sheriff Saline County Detention		
V-SECT725-065	Verizon MARNILXE1ED	Goreville 618-995	Unon County Sheriff Pulaski County Sheriff		
V-SECT725-066	Verizon MARNILXE1ED	Goreville 618-995	Williamson County Sheriff Herrin Police Dept		
V-SECT725-067	Verizon MARNILXE1ED	Marion-South 618-964	Marion Police Marion Fire Department		
V-SECT725-068	Verizon MARNILXE1ED	Marion South 618-964	Williamson County Sheriff Herrin Police Dept		
V-SECT725-069	Verizon MARNILXE1ED	Vienna 618-658	Johnson County Sheriff Saline County Detention		
V-SECT725-070	Verizon MARNILXE1ED	Vienna 618-658	Massac County Sheriff Metrolpolis Police		
V-SECT725-071	Verizon MRRSILMSDS0	Omaha 618-962	Saline County Sheriff Johnson County Sheriff		
V-SECT725-072	Verizon MTRPILXEDS2	Brookport 618-564	Massac County Sheriff Metrolpolis Police		
V-SECT725-073	Verizon MTRPILXEDS2	Joppa 618-543	Massac County Sheriff Metrolpolis Police		
V-SECT725-074	Verizon MTRPILXEDS2	Joppa 618-543	Pulaski CSO Dept. Union County Sheriff		
V-SECT725-075	Verizon TBD	Carbondale 618-529;453;457;536;549	Unon County Sheriff Pulaski County Sheriff		
V-SECT725-076	Verizon TBD	Carterville 618-985	Jackson County Sheriff Murphysboro PD Carbondale PD SIU PD		
V-SECT725-077	Verizon TBD	Carterville 618-985	Williamson County Sheriff Herrin Police Dept		
V-SECT725-078	Verizon TBD	El Dorado 618-273	Saline County Detention Johnson County Sheriff		
V-SECT725-079	Verizon TBD	Herrin 618-942;988	Williamson County Sheriff Herrin Police Dept		

V-SECT725-080	Verizon TBD	Murphysboro 618-565;684;687	Jackson County Sheriff Murphysboro PD Carbondale PD SIU PD		
V-SECT725-081	Verizon TBD	Murphysboro 618-565;684;687	Unon County Sheriff Pulaski County Sheriff		
V-SECT725-082	Verizon TBD	New Haven 618-265	White County Sheriff Wabash County Sheriff		
V-SECT725-083	Verizon TBD	New Haven 618-365	Saline County Sheriff Johnson County Sheriff		
V-SECT725-084	Verizon TBD	Norris City 618-378	White County Sheriff Wabash County Sheriff		
V-SECT725-085	Verizon TBD	Pinckneyville 618-357	Jackson County Sheriff Murphysboro PD Carbondale PD SIU PD		
V-SECT725-086	Verizon TBD	Pinckneyville 618-357	Perry County Sheriff Duquoin City Police Administration Office		
V-SECT725-087	Verizon TBD	Raleigh 618-268	Saline County Detention Johnson County Sheriff		
V-SECT725-088	Verizon TBD	Wendelin 618-752	Flora Police Dept Richland County Sheriff		
V-SECT725-089	Verizon NRCYILXEDS0	Omaha 618-962	White County Sheriff Wabash County Sheriff		
V-SECT725-090	Verizon OLNYILXEDS0	Noble 618-723	Flora Police Dept Richland County Sheriff		
V-SECT725-091	Verizon OLNYILXEDS0	Sailor Springs 618-689	Flora Police Dept Richland County Sheriff		
V-SECT725-092	Verizon PERCYIL0000	Steeleville 618-965	Jackson County Sheriff Murphysboro PD Carbondale PD SIU PD		
V-SECT725-093	Verizon PERCYIL0000	Steeleville 618-965	Perry County Sheriff Duquoin City Police Administration Office		
V-SECT725-094	Verizon RLGHILXEDS0	Paulton 618-982	Williamson County Sheriff Herrin Police Dept		
V-SECT725-095	Verizon SPRTILXE50T	Coulterville 618-758	Perry County Sheriff Duquoin City Police Administration Office		
V-SECT725-096	Verizon WFFTILXEDS0	Johnston City 618-983	Williamson County Sheriff Herrin Police Dept		
V-SECT725-097	Verizon WFFTILXEDS0	ThompsonVille 618-627	Saline County Detention Johnson County Sheriff		
V-SECT725-098	Verizon WFFTILXEDS0	Thompsonville 618-627	Williamson County Sheriff Herrin Police Dept		
V-SECT725-099	Wabash CISNILXEDS0	Mount Erie 618-854	Wabash County Sheriff Richalnd County Sheriff		
V-SECT725-100	Wabash CISNILXEDS0	Mt. Erie 618-854	Flora Police Dept Richland County Sheriff		
V-SECT725-101	Wabash LSVLILXEDS0	Bible Grove 618-686	Flora Police Dept Richland County Sheriff		
V-SECT725-102	Wabash LSVLILXEDS0	Xenia 618-678	Flora Police Dept Richland County Sheriff		

References

Documents filed by CSI

1. Next Generation Design Plan, Assure911.net-DG-CSI/NG911-001
2. Next Generation Access Plan, Assure911.net-DG-CSI/NG911-002
3. Test Plan Document, Assure911-STP-CSI/NG911-001
4. NG9-1-1/CSI Cutover Strategy, Assure911-STP-CSI/NG911-002

Title 83 Administrative Code Part 725:

1. http://www.ilga.gov/commission/jcar/admincode/083/08300725sections.html

NENA and SIP References, included in the filing as Exhibit 12

1. NENA i3 standards, “Detailed Functional and Interface Standards for the NENA i3 Solution Version 1.0,” Standard number: 08-003 v1“, approved June 16, 2011, http://www.nena.org/stories/technical/executive-board-approves-i3-standard
2. NENA Glossary of terms document, http://www.nena.org/sites/default/files/NENA%2000-001_V16.pdf.
3. NENA: “The NENA 75-001 Security for Next-Generation 9-1-1 Standard (NG-SEC) contains a number of sections which apply to ESInets including; Security Policies, Information Classification, Safeguarding Information Assets, Physical Security Guidelines, Network and Remote Access Security Guidelines, Change Control Documentation, Compliance Audits and Reviews. ESInets should be NG-SEC compliant. http://www.nena.org/?page=ng911_security&terms=security+and+standards
4. NENA Operations Standards for NG9-1-1, NENA 57-750 NG9-1-1 System and Operational Features and Capabilities Requirements pdf. Rick Jones - lead.
5. IP-PBX / Service Provider Interoperability, "SIPconnect 1.1 Technical Recommendation", SIP Forum Document Number: TWG-2
6. NENA ESInet Design for NG9-1-1 draft document NENA 08-506 Version 1, August 16, 2011.

7. ESInet Design for NG9-1-1 NENA 08-506, Version 1
8. CSI Narrative including Future Benefits not covered in CSI ICC Pilot application Design Plan

List of Exhibits included in this filing:

1. Exhibits 1-9 Legal and Regulatory References.
2. Exhibit 10 Assure911 Test Plan
3. Exhibit 13 CSI RFP - This document defines the Network Design as described in the *"REQUEST FOR PROPOSAL FOR AN IP-BASED NEXT GENERATION 9-1-1 COMMUNICATION SYSTEM for Counties of Southern Illinois NG9-1-1 Association,"* submitted on September 21, 2010 by: Ken Smith – Chairman, 300 N. Park Ave., Herrin, Illinois 62948, 618-988-6911, document dated August 2, 2010.
4. Exhibit 14 Design Plan
5. Exhibit 15 Access Plan
6. Exhibit 16 Cutover Strategy
7. Exhibit 17 CSI Contracts