FLORIDA DEPARTMENT OF TRANSPORTATION

EXHIBIT “A”

TECHNICAL SPECIFICATIONS

FOR

NETWORK MANAGEMENT SYSTEM REPLACEMENT PROJECT

November 11, 2015

FILE PATH:
\\DOTSCOTEOSERVER\TRAFFIC_OPS_DATA\PUBLIC\ITS\TELECOMMUNICATIONS\STATEWIDE_TELECOMMUNICATIONS_NETWORK\NETWORK MANAGEMENT UPGRADE 2010\2015\NMS_RFP-20151009_DSM.DOCX

TABLE OF CONTENTS PAGE

1 GENERAL

The Florida Department of Transportation (FDOT) is in the process of upgrading the Statewide Telecommunications Network (STN). To support the STN upgrade, the Network Management System (NMS) is being replaced.

The current NMS is used to monitor and control the FDOT STN by connecting to Ethernet and Serial Data connections using SNMP, SCAN, TL1, and ASCII protocols. The NMS monitors and controls components of the STN, including microwave radios, fiber optic equipment, networking equipment, and site infrastructure systems including fire alarm, intrusion detection, temperature monitoring, power systems, and more.

This RFP details the requirements for the NMS replacement, and related support equipment.

It is the intent of this project to replace the current STN NMS, NetBoss Manage.IT, with an integrated turnkey system which shall include all equipment, connecting/mounting hardware, installation supplies, and all work necessary to complete configuration and deployment.

1.1 Terms

Department:	The Purchaser (or Owner) State of Florida Florida Department of Transportation (FDOT)
Project Consultant:	TBD
Vendor	The individual, firm, partnership, corporation, company, association, or other legal entity to whom the contract is awarded by the FDOT and who is subject to the terms thereof.

1.2 Acronyms

ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode

CSV	Comma Separated Values
CWDM	Coarse Wave Division Multiplexing
DACC	Digital Access Cross Connect
DC	Direct Current
DVD	Digital Versatile Disc
DWDM	Dense Wave Division Multiplexing
FDOT	Florida Department of Transportation
FO(C)	Fiber Optic (Cable)
FTP	File Transport Protocol
IDE	Integrated Development Environment
ITS	Intelligent Transportation System
LDAP	Lightweight Directory Access Protocol
LOM	Lights Out Management
MFN	MyFlorida Network
NEC	National Electric Code
NFPA	National Fire Protection Association
NMS	Network Management System
NOC	Network Operations Center
OAM	Operations, Administration and Management
OAMP	Operations, Administration, Management & Provisioning
OEM	Original Equipment Manufacturer
OSHA	Occupational Safety and Health Administration
PDF	Portable Document Format
RADIUS	Remote Authentication Dial-In Service
RTU	Remote Terminal Unit
SITSN	Statewide ITS Network
SNMP	Simple Network Management Protocol
SPD	Surge Protection Device
SQL	Standard Query Language
STN	Statewide Telecommunications Network
TDM	Time Division Multiplexing
TFTP	Trivial File Transport Protocol
TL1	Transaction Language 1
UPS	Uninterruptable Power System

USB	Universal Serial Bus
VAC	Voltage Alternating Current
VDC	Voltage Direct Current
VNC	Virtual Network Computing
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network

1.3 Applicable Publications and Standards

The latest issues of the following publications and standards, unless otherwise specified, shall be part of this Technical Specifications. In the event of inconsistencies between this Technical Specifications and these publications and standards, the requirements of this specification shall take precedence.

A. National Electric Code (NEC) (NFPA 70).

B. Applicable Occupational Safety and Health Administration (OSHA) Regulations

1.4 Vendor's Responsibility and Qualifications

It is understood, and the Vendor hereby agrees, that the Vendor is solely responsible for all equipment, materials, and services proposed. Notwithstanding the details presented in these specifications, the Vendor shall be responsible for verifying the completeness of the materials required and suitability of devices to meet these specifications. The Vendor shall provide and install, without claim, any additional equipment required for operation in accordance with these specifications.

The Vendor shall be responsible for furnishing, installing, and configuring all new NMS components and software required for the upgrade of the FDOT's network management system. The Vendor is responsible for performing the configuration necessary for the NMS to communicate with all protocols present on the STN.

1.5 Sites of Work

The Vendor is responsible for familiarizing themselves with all pertinent aspects of the two sites involved in this project.

Site	Address
McArthur Interchange	Sunrise Blvd. and Turnpike Interchange in Ft. Lauderdale, Florida 26-08-15.3 N, 80-13-03.2 W (NAD 83)
Tallahassee FHP	2100 Mahan Drive (US-90), Tallahassee, FL 30-27-18.9 N, 84-14-43.2 W (NAD 83)

1.6 Coordination Requirements

The Vendor is responsible for coordinating field visits with the Florida Department of Transportation at least 2 weeks in advance to permit the FDOT time to schedule the necessary site visits.

Before entering a site each day the Vendor shall inform the FDOT or their representative. Upon exiting a site at the end of each day the Vendor shall inform the FDOT or their representative.

The Vendor shall coordinate all work activities with the personnel listed below:

Name	*Organization*	*Telephone Number*
Randy Pierce	Florida Department of Transportation	(850) 410-5608
Danielle Morales	Florida Department of Transportation	(850) 410-5617

2 SYSTEM OVERVIEW

2.1 STN Overview

The existing NMS is managing the FDOT's STN, a statewide microwave and fiber optic system consisting of up to 143 microwave radio links and multiple fiber optic links. Much of the microwave equipment was installed in the 1980's as part of the construction of the Statewide Motorist Aid Call Box System. This system was upgraded between 2000 and 2005 to reconfigure the network, add IP-based routers and ATM-based switches to facilitate the use of excess bandwidth for Intelligent Transportation System (ITS) projects. Between 2003 and the present day, the FDOT also constructed a fiber-optic based wide area network, called the ITS WAN, which connected each of the FDOT's independent district systems together. Where fiber is not available to tie the district systems together, the ITS WAN utilizes excess capacity from the microwave system's ATM switches.

The STN is comprised of equipment from various vendors. The following is a high-level summary of the equipment and systems:

- 77 hops of Harris DVM6-45/Excell/ microwave radios
- 6 hops of Harris Constellation microwave radio
- 20 links of Nortel OM5200 optical transport
- 68 Nortel ASN Routers
- 2 Nortel 8800 network switches
- 11 Nortel 8600 network switches
- 14 Nortel Passport 15000 ATM Switches
- 36 Carrier Access Corporation M13 multiplexers
- 14 Larus 5800 network clocks
- 68 Nortel BPS 2000 Ethernet switches
- 68 Nortel Baystack network hubs
- 82 DPS Telecom NetGuardian 832A alarm RTUs
- 68 Multitech 210/410 VoIP units
- 52 Access 60 Channel Banks
- 14 Sycamore DNX-11 Digital Cross Connect

Moving forward, the FDOT plans to replace legacy equipment, particularly the microwave radios, routers and ATM switches with Ethernet/IP-based equipment. However, this is a multi-year plan and support for this legacy equipment will continue for a number of years.

2.2 NMS Overview

The equipment and systems that comprise the STN support varying levels of management. Though SNMP is predominant, the Harris DVM6-45 and Constellation microwave radios utilize Harris' SCAN protocol and the Larus network clocks utilize TL1. The microwave system is a legacy product and is not SNMP capable. The NMS shall support the Harris SCAN protocol to provide the necessary monitoring and control of the existing microwave radios. Other required protocols are detailed elsewhere in this RFP.

The STN is currently monitored by a multi-server Harris NetBoss system. The NetBoss system was initially installed with four servers configured for load sharing and in a four-way failover capability (any server could provide backup to any or all other servers). However, the NetBoss system was installed on Sun hardware which is no longer supported. Two of the four servers have failed and the system is currently managed by the remaining two servers.

The NetBoss system notifies the FDOT's microwave maintenance contractor of system trouble via email messages. The FDOT and the microwave maintenance contractor utilize two VPN access points (for redundancy and load-sharing) into the network for remote monitoring and management of the NetBoss system.

In addition to the NetBoss servers, the FDOT also maintains a NetBoss developmental server and a Nortel Preside (Ericsson MDM) server. The NetBoss developmental server is used to implement changes to the NetBoss configuration and develop new management drivers (Harris refers to these drivers as SmartAgents). The Nortel Preside server is used as an element manager for the Passport 15000 ATM network switches.

Management traffic only uses a single T1 between servers and the microwave system is subject to fading. The Vendor should consider this limitation for synchronization and failover between geographically distanced servers.

The NMS serves a team of support technicians (NMS users) with responsibilities for different regions and systems on the STN. The system shall provide for the configuration of a role-based view/scene on a per-user basis, including the ability to limit the view for a particular user. These limits shall have the ability to be dynamically modified by administrative control, should circumstances dictate.

Users shall see a custom/preferred view, and be able to access any needed view, limited to their role, for troubleshooting. The system shall provide access/action logging capabilities. Administrative users need to be able to limit views per user.

Notifications, including alarms from the NMS must be delivered through email to the appropriate individual(s) or groups. The NMS shall include the required email servers. The NMS exists separate from the public Internet, and the notification facility shall provide secure outbound communication from each of the remote sites. The Vendor shall ensure that the correct notification is provided in the event of NMS system failure. All necessary security shall be in place to protect access to the STN including Firewall and VPN services.

The NMS shall also include a developmental server and two remote workstations for creation and testing of new scenes, scripts, upgrades and any of other modifications to any software aspect of the NMS, including OS and related utilities and procedures, prior to deploying any of these to the NMS remote sites.

3 FUNCTIONAL REQUIREMENTS

The new network management system shall meet the FDOT's functional requirements in the following areas:

- Method of Access
- Fault Management
- Protocol Support
- Trouble Ticket Management, Alarm Notification and Escalation
- Performance Monitoring
- Security and User Policy Management
- Report Generation
- Scalability Requirements
- Redundancy, Resiliency and Backup
- Remote Access and Client Requirements
- Development Capabilities

3.1 Method of Access

The NMS shall provide a client-based and/or Web-based interface for remote access to the fault management views and scenes and remote retrieval of fault management network information with a graphical view. Client-based access shall support the

download and caching of graphical elements to minimize the traffic across the network and maximize the performance of the client. Updates to scenes and configuration shall be automatically downloaded by the client when required.

Access via clients and/or to the web-based interface shall be available directly via a VPN connection, with no intermediate remote desktop login through a third system. Multiple simultaneous remote sessions shall be supported by fault management, with administrator control to disconnect a session if needed.

The use of remote desktop sessions (e.g., Windows Remote Desktop, VNC, etc.) as the means to access the network management system is not acceptable.

3.2 Fault Management Requirements

3.2.1 General

The network management system shall monitor and display the network status via its graphics display and text messages. The NMS shall automatically characterize and classify alarms by a minimum of five levels of severity. Based on the alerts, severity levels, and messages generated by the network devices, the NMS shall automatically update its graphical fault management views to reflect the current state of the network and devices. The NMS shall distinguish various severity levels by different color messages and indicators.

The NMS shall provide for access to monitor, reset/restart, review logs, and perform other system-level and software administrative tasks, including access to alarm status and logs and/or the database used by the NMS to generate reports in a non-graphical manner.

3.2.2 Graphical Scene Requirements

The NMS shall allow the user to monitor multi-vendor network resources graphically using scenes and views organized in a parent-child hierarchy. The network shall be illustrated using icons and graphics, such as a router or a channel bank, and symbols, such as a rack diagram or a state map, to represent the network resources and devices. The NMS shall continually update the current status of the network resources using combinations of color and text to display alert messages and alarms.

The NMS shall display a hierarchy of scenes as defined by the FDOT. The scenes shall be designed such that the user will be presented with one or more system-level scenes and drill-down to site and then equipment-level scenes.

The FDOT has developed an extensive set of graphical scenes for the current network management system (approximately 600 top-level, systems, regional, site and equipment scenes[1]). Figure 1 illustrates the general hierarchy of the FDOT's current NMS.

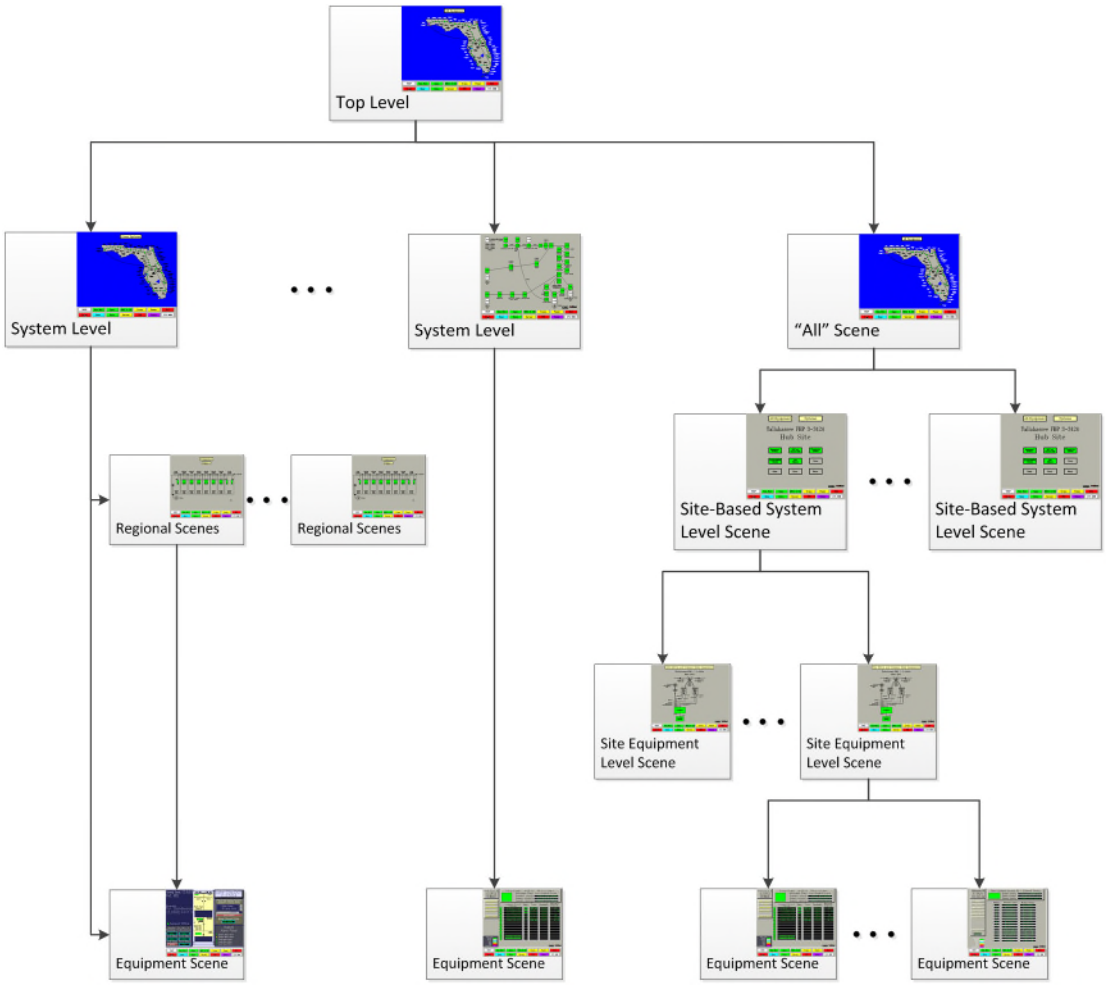

Figure 1 - FDOT NMS Scene Hierarchy

An example of a site equipment level scene for the management system is shown in Figure 2 - Example Site Equipment Level SceneFigure 2. Note that only the management

[1] Each equipment scene is counted only once. For example, only one alarm RTU scene is included in this count even though there are over 70 alarm RTUs in the network.

equipment shown on the scene have indicators. Other equipment is being shown for informational purposes to provide the technician with additional connectivity information.

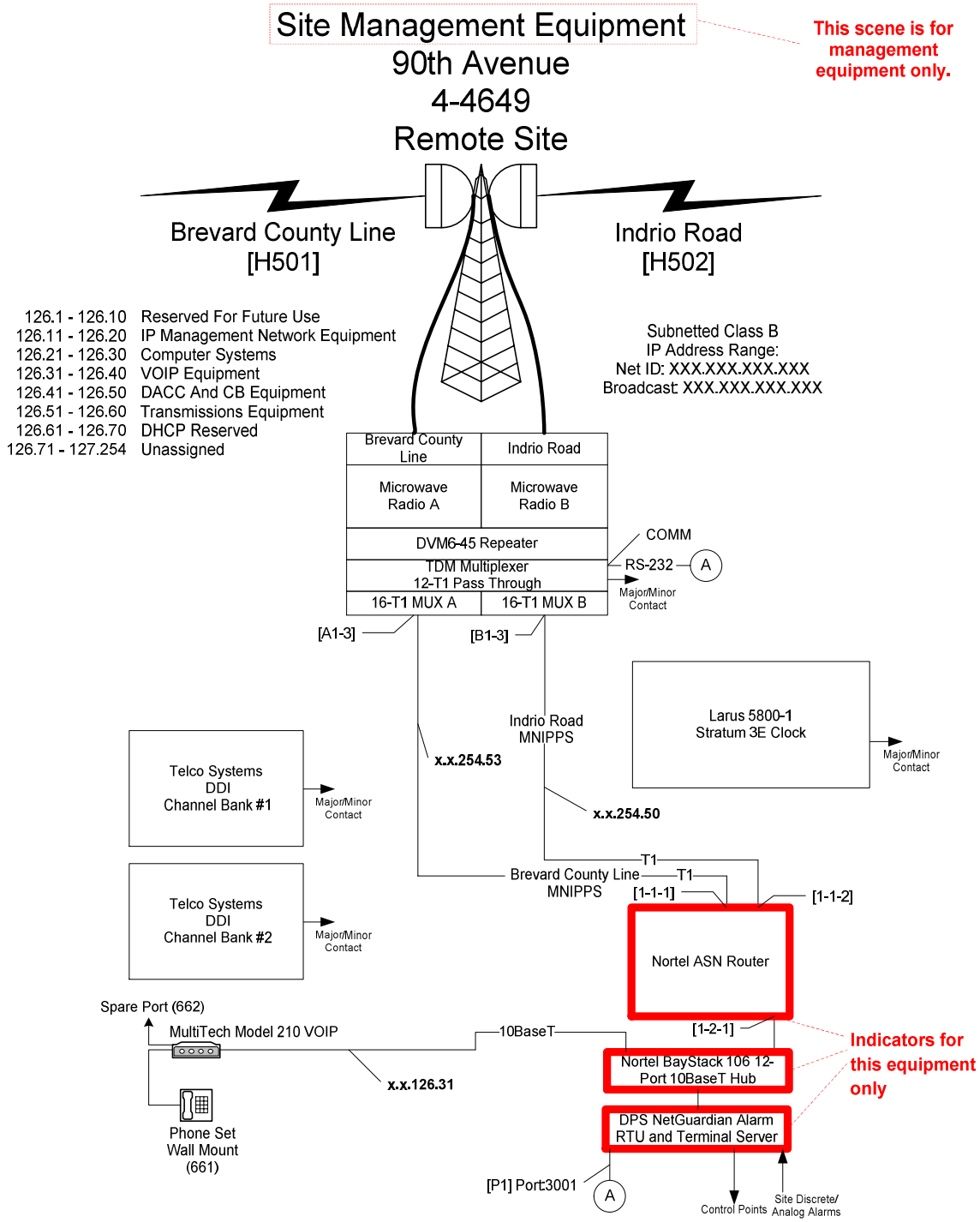

Figure 2 - Example Site Equipment Level Scene

An example system level diagram is provided in Figure 3. All equipment in the diagram have indicators (shown bold with red outline), however, the diagram also include

annotations (shown in black) to provide information on system connectivity to the technicians.

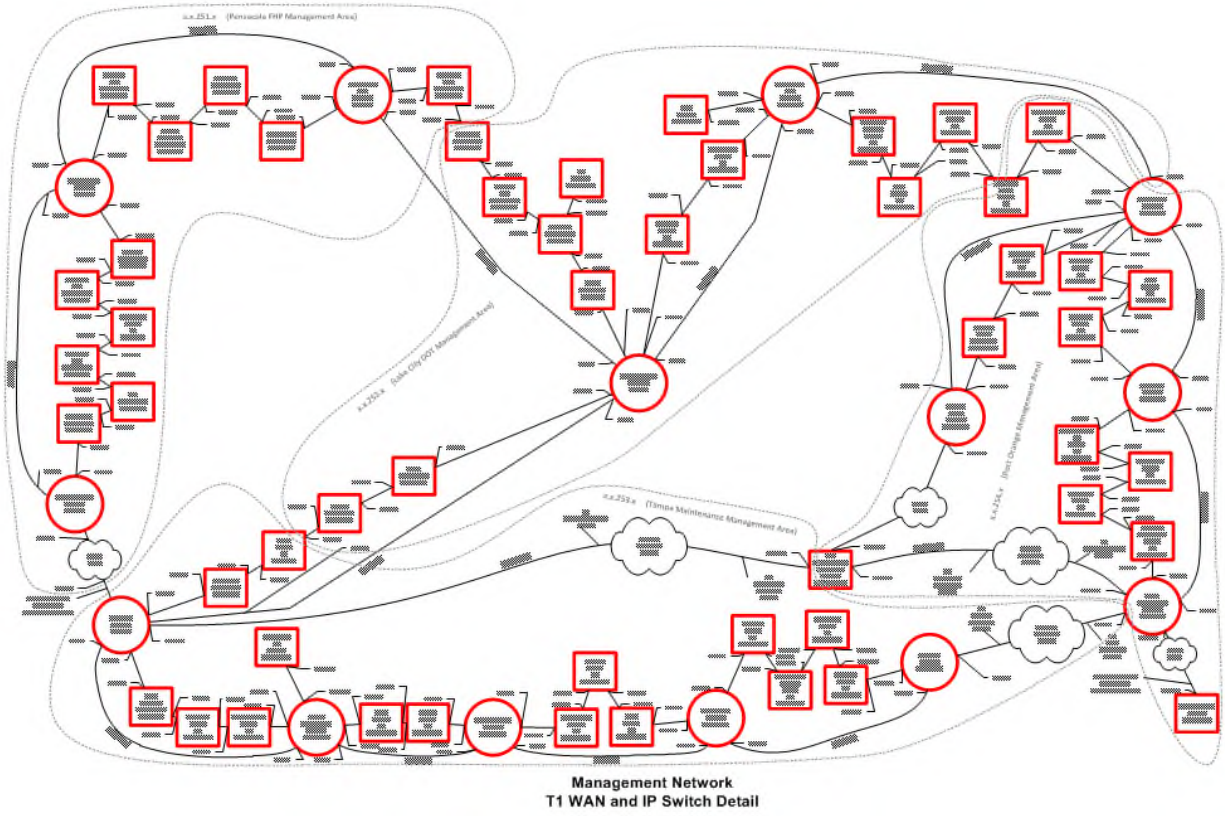

Figure 3 - Example System Level Diagram

The FDOT has maintained their scenes in their native Microsoft Visio format. The FDOT will optimize the scenes and remove and/or consolidate scenes to improve the user experience. This work has not been completed so the final number of scenes to be incorporated into the initial system is unknown; however, the number of scenes should not exceed 600. The NMS shall support a minimum of 1,000 scenes. The FDOT will provide the scenes to the Vendor, for the Vendor to incorporate into the initial system.

In general, the customized FDOT hierarchy will include 12 top level views for the following systems:

- All Equipment (this view will include all alarms for all systems)
- Management Network

- TDM Synchronization
- DACC and Channel Bank
- Microwave Transmission
- ITS STN/Fiber Transmission
- Power System
- Tower Lights
- Door Intrusion
- Land Mobile Radio
- VoIP
- NMS Server Status

Each system top level view shall have a customized geographical or logical map with active buttons to customized region views and managed device graphics. Buttons and/or indicators shall change color based on the alarm severity of the equipment alarm being monitored or the child scenes it represents. All alarms shall "bubble-up" through the scene hierarchy structure so that an alarm at the lowest equipment level is reflected on each parent scene all the way to the top-level scene.

3.2.3 Managed Device Drivers and Scenes

For the purposes of this RFP, the FDOT considers a Managed Device Driver to be the functionality that parses the particular devices management protocol (such as SNMP or TL1) and processes the management functionality in the appropriate equipment-level scene for display and notification. An example of a managed device driver would be a NetBoss Technologies Smart Agent.

3.2.3.1 Scene Construction

Scenes for the managed device drivers (i.e., equipment-level scenes) shall be generated by a template that can be automatically populated by the system, or user populated if the device being monitored does not provide for the ability to auto-discover its configuration. The scenes shall depict the front view of the equipment and, where possible, shall auto-populate cards, slots, and ports, based on the actual cards, slots, and ports installed on that particular device. The managed device scenes shall have auto-populated fields based on MIBs or specific information entered in the equipment.

3.2.3.2 Indicators

The indicators on each device driver scene shall be representative of the indicators on the actual device. If necessary, indicators can be added to the device driver scene in the event that:

- The equipment does not provide for a means to map device driver indicators to actual device indicators (i.e., the equipment does not provide an alarm that can be parsed by the device driver such that the NMS will know when a particular indicator is active), or
- If some alarms are not associated with actual device indicators (e.g., there is no indicator on the device when there is a minor alarm and therefore a "minor alarm" global indicator is required to be added to the scene).

3.2.3.3 Reporting and Control

The device driver scenes shall also provide full reporting capability of the state of the device beyond the required indicators. For example, device driver scene(s) for the NetGuardian 832A alarm RTU shall report the status of discrete inputs, relay controls and analog inputs and ping host alarms. The ability to perform basic control of devices is desired by the FDOT in order to minimize the need to access element managers (e.g., separate element manager systems, Telnet, Web sessions). For example, the FDOT desires to be able to activate relay controls on the NetGuardian 832A alarm RTU using the NMS. Similarly, the FDOT desires to be able to issue manual SCAN commands to the device driver of the DVM6-45 microwave radios using the NMS.

3.3 Protocol Support

The NMS shall support, at a minimum, the monitoring and/or control of the equipment that comprise the STN through following protocols:

- SNMP
- TL1
- Telnet
- Harris SCAN
- Serial (RS-232)

SNMP protocol support shall include auto-discovery, set commands, get commands and verification of network connectivity (ping alerts).

Both the Harris SCAN and Serial (RS-232) protocols are currently mediated through Telnet sessions to RS-232 ports on the NetGuardian 832A alarm RTUs/terminal servers. Therefore, the NMS servers will not be required to provide physical RS-232 interfaces for network management interfaces; however, the NMS system shall support the serial protocols through the terminal servers.

The SCAN protocol support shall include monitor (i.e., autopoll and selectpoll) and control (i.e., manual commands). It is the FDOT's desire that this functionality be directly included in the NMS and not via a northbound interface.

The Serial protocol support shall include the ability to issue serial commands and parse the responses to determine alarm state.

The TL1 protocol support shall include monitor and control capability.

3.3.1 Generic Protocol monitoring

The NMS shall include functionality for the FDOT to create its own device drivers for SNMP, TLI, and ASCII supported equipment. This functionality will allow the FDOT to build its own scenes and device drivers for specific equipment. For example, the Generic SNMP would enable the FDOT to create a device driver for a UPS smart card that supports SNMP protocol. The functionality shall enable the FDOT to build scenes that parse the SNMP traps and indicate alarms, such as major, minor, and no communications based on the MIB.

3.4 Trouble Ticket Management, Alarm Notification and Escalation

The NMS shall include a trouble ticket management system that provides a remote Web-based interface for field technicians to submit, track, query, view, update and escalate issues. Trouble tickets shall be created dynamically based upon one or more system alarms. The trouble ticket management system shall track the status of the issue, including type of issue, severity of issue, time the ticket was created, time the ticket was closed, technician/entity assigned to the ticket and description of the trouble resolution. The trouble ticket management system shall generate reports and enable the user to review, forward, and print reports from the trouble ticket database.

The NMS shall utilize a rules-based process by which administrators can set policies for determining which action to take upon location, type, severity and time and day of an alarm. The NMS shall provide for automatic escalation of notifications, if required actions

are not taken by field technicians to respond. The network management system shall have the capability to create rules to send notifications under specific alarm conditions, for example if two specific minor alarms are active at the same time, send notification. Another example would be if an intermittent alarm is active five times within a ten-minute period of time.

The NMS shall provide e-mail based alerting (See Section 3.13 regarding email server requirements) of alarms to technicians. The NMS shall provide scheduling capability such that alerting policies can be different based upon a combination of all of the following:

- Time (time-of-day, day-of-week or specific days such as holidays),
- Type (door alarm, power failure, etc.)
- Priority (critical, major, minor, etc.)
- Number of iterations of alarms
- Technician (e.g., notify certain technicians between certain hours)
- Escalation (e.g., if no acknowledgement after two attempts to notify technicians then notify technician supervisor)

3.5 Performance Monitoring

The NMS shall provide for the ability to monitor in real-time and log for long-term analysis the performance of equipment being managed. The NMS shall allow for capture of raw data of various elements and provide charting capability. All metrics that can be captured by the NMS, such as the bit error rate (BER) of a T1 interface, shall be available for performance monitoring. The NMS shall provide a dashboard view of Quality of Service metrics.

3.6 Server Health Monitoring

The NMS system shall monitor the servers for processor usage, memory usage, storage volume usage, file system usage, failure status and running processes. The NMS shall indicate alarms when values exceed Vendor recommended thresholds.

3.7 Security and User Policy Management

3.7.1 Access and Capability Policies

The NMS shall provide a robust security and user policy management system. The NMS shall provide for a hierarchy of groups and users such that access and capability policies

are assigned to groups and users are assigned to one or more groups based upon their needs.

The NMS shall provide for user/group access and capability policies to be centrally managed. Access policies shall allow for user/groups to be limited to specified equipment/systems. Capability policies shall allow for user/groups to be limited to read-only or read/write access to the equipment they are allowed to access. Capability policies shall also allow for the ability to limit user/groups to write to only specific fields of equipment they are allowed to access.

The Vendor shall include all email hardware and software as part of the NMS and as part of the security policy.

3.7.2 Activity Tracking

The NMS shall track all users' activity including logins, login failures and actions taken by users. The NMS system shall provide the capability of producing audit reports on security and policy management.

3.7.3 Access Authentication

The NMS shall provide for user authentication using either Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial-In User Service (RADIUS). The authentication of the user shall allow for the user to gain their appropriate access and capability privileges. The NMS shall include the required authentication server functionality (i.e., the FDOT does not currently have an LDAP or Radius server). The authentication server may be separate from the NMS, however, remote access to the authentication server for administrative purposes, such as adding, deleting and changing passwords for users, shall be provided. In addition, the authentication server shall be monitored by the NMS for alarms.

3.7.4 Managed Device Security Management

Where managed devices require authentication for access and alarming, the NMS shall provide centralized user name and password management to allow the FDOT to quickly change the passwords on any and all managed devices.

3.8 Report Generation

The NMS shall provide for the ability to generate reports from its database. The NMS shall provide pre-defined reports as well as for the ability to produce custom reports. Pre-defined reports shall include:

- Equipment inventory
- Equipment performance/alarm history
- Equipment information
- Equipment status
- User and security information

For custom reports, the NMS shall provide a user-friendly approach to defining and generating the desired reports. The methodology shall not depend upon the user manually generating SQL-like queries; however, the NMS database shall support SQL. Reporting capability shall include the generation of pie, bar and line charts, as appropriate for the data to be displayed. Reports shall be produced in electronic format (Adobe PDF, Microsoft Word or other suitable format to allow for emailing and printing) as well as export of information in CSV and/or Microsoft Excel format. All licensed clients with access to the NMS shall have report generation and review capability.

3.9 Scalability and Performance Requirements

The NMS shall be scalable and capable of supporting the quantity of equipment in use today, and a future growth factor of a minimum of 100%. The NMS database shall be capable of ensuring that all alarms are captured and recorded. The FDOT does not have historical data available on the number of alarms per second that the network management system shall support. Alarms are generally “bursty” in nature and during relatively inactive periods, alarms may appear on the system on minutes or tens-of-minutes basis. When a significant event occurs, such as a microwave fade, an inrush of alarms occurs likely at the order of tens-per-second for a short period of time.

3.10 Redundancy, Resiliency and Backup

The NMS shall be based upon a minimum of a two-server, geographically redundant configuration. The servers can be configured in either a load-sharing or hot-standby configuration. **In either configuration, each NMS server shall be capable of supporting the load of the entire system**.

3.10.1 Database Synchronization

The NMS servers shall communicate with each other and maintain synchronization of the databases. Administrative and configuration changes to one NMS server shall be propagated to the other NMS server(s). The FDOT will work with the Vendor to ensure adequate WAN capacity to support the synchronization. The FDOT currently allocates approximately 3 Mbps of WAN capacity to support the current network management system. This capacity supports the existing NMS server-to-server synchronization, polling/alarm reporting to the servers from the managed equipment, remote access to elements (element managers, Telnet and/or Web), remote desktop sessions to the current NMS, and a VoIP system utilized by the maintenance technicians when on-site.

3.10.2 Resiliency

The failure of one of the NMS servers shall be detected quickly by the other NMS server and the failover/redundancy plan shall be enacted. The Vendor shall provide a detailed failover/redundancy plan for approval by FDOT. The NMS shall be designed to accommodate intermittent outages and degraded performance associated with microwave systems without causing unnecessary switching. The desire of the FDOT is to not lose alarm information from equipment that can report alarms to multiple servers because of a NMS server failure. When the failed NMS server is restored to operation, the NMS server shall automatically synchronize its database with the other server(s).

3.11 Backup and Archiving

3.11.1 Server Backup and Archiving

The NMS shall provide for backup of the configuration of the NMS in the event that an NMS server is required to be reconstructed. If the NMS server requires extensive operating system installation and software installation to restore the operation of the NMS server, it is the FDOT's desire that the NMS include the capability of producing an image backup of each NMS server (to external USB hard drive or DVD) to facilitate a quick reinstallation of the system. The FDOT desires the backup of the configuration of the system be such that the backups can be performed remotely on a regular basis (i.e. the configuration can be downloaded or exported from the server(s) using the NMS client or other tool).

The NMS shall also provide a means to archive historical alarm information and performance data to reduce server storage requirements and to allow for long-term trend analysis.

3.11.2 Managed Devices Configuration Backup and Restoration

For devices that support remote configuration download, the NMS shall provide for automatic, scheduled backup of managed equipment devices. The NMS shall maintain multiple historical versions of the configuration of each managed device. For devices that support remote configuration upload, the NMS shall provide a means to upload an archived configuration to the managed device to allow for quick restoration. The NMS shall also allow for technicians to upload and download copies of the configurations for devices that require local access to perform configuration.

3.12 Development Capabilities

The NMS shall provide for the FDOT to generate and import their own scenes and device drivers. The NMS shall provide for an integrated development environment (IDE) and graphical editor that allows for the importation of scenes from Microsoft Visio format, placement of buttons and indicators, and the development and testing of the scripting/programming required to process alarm messages from the managed equipment. The FDOT prefers that the imported Visio drawings be imported as editable objects.

The NMS shall include a development server, separate from the operational NMS servers. The NMS shall allow for the upload of finalized changes from the development server to the operational servers. The NMS shall include two workstations for remote access to the development server and the operational NMS servers.

3.13 Email System

The NMS shall include two email systems (servers and software) to allow for the transmission of alarm information to the technicians. The Internet connection for outgoing email is via an MFN router located at the Tampa Maintenance site. The MFN router is currently connected directly to a mail server, and the mail server only allows outbound email communications (i.e., no equipment on the internal microwave network has any connectivity to the Internet through that server). All external connection requests from Internet sources are rejected. The NMS email systems shall match this configuration to ensure a one-way secure solution.

The email system shall be configured so any email alarms shall be sent with server/alarm identification/severity and be formatted such that it is optimized to be received by cell phone text message. The outgoing email shall be sent from an email address associated with the site name of the originating alarm point (e.g., <site name>@dot.state.fl.us).

4 EQUIPMENT REQUIREMENTS

All hardware furnished by Vendor shall be Commercial Off The Shelf (COTS).

4.1 NMS Servers

The NMS shall consist of a minimum of two operational servers and a development server. All three servers shall be configured the same. The servers shall be designed for mounting in two-post 19-inch equipment racks and include suitable support. The servers shall include redundant -48VDC power supplies. All storage volumes shall be redundant, hot-swappable, and front accessible. The storage volume shall be sized to maintain a minimum of 180 days of alarm history and support multiple copies of managed equipment configuration files plus and additional dedicated 1 TB of FTP and TFTP accessible storage space for exclusive use by the FDOT for technician data file storage (equipment manuals, as-built documentation, etc.). Each server shall have a minimum of three 10/100/1000Base-T Ethernet interfaces and a port for Lights-Out-Management (LOM) to allow for remote system-level access and remote login.

4.2 Email Server

The NMS shall include two email servers. Each server shall be configured the same. The servers shall be designed for mounting in two-post 19-inch equipment racks and include suitable support. The servers shall include redundant -48VDC power supplies. All storage volumes shall be redundant. Each server shall have a minimum of two 10/100/1000Base-T Ethernet interfaces (one for public Internet facing connection and one for private FDOT network connection).

4.3 Workstations

The NMS shall include two workstations intended for dedicated remote access. The workstations shall be commercially available off-the-shelf and be an all-in-one form factor (processing and storage contained within display). The display shall be a minimum of 23-inch with 1920x1080 resolution. The workstation shall be provided with a keyboard and mouse. The workstation processor shall be a minimum Intel 4th Generation Pentium i5 or

i7 series quad-core processor. The workstation shall be equipped with a minimum of 16 GB of RAM and a 1 TB hard drive. The workstation shall be installed with Windows 10 Professional operating system. The workstation shall be furnished with a minimum 1000VA UPS.

5 INSTALLATION REQUIREMENTS

5.1 NMS Servers

The NMS operational servers shall be installed at the Tallahassee FHP and McArthur tower sites, and the NMS development server shall be installed at the Tallahassee FHP site. The servers shall be installed in rack locations as specified by the FDOT. The Vendor shall ensure that proper support and clearance is provided for the equipment. If it is necessary to extend the front of the NMS server forward in the rack to ensure adequate clearance in the back, the Vendor shall furnish and install the necessary rack stand-off brackets. The Vendor shall ground the equipment to the rack. FDOT will connect the site's DC power system to the servers. The Vendor shall interface the servers to the site's local area network switch through Vendor furnished Surge Protection Devices (SPDs). The SPDs shall be Crouse-Hinds MTL Surge ZB24540, or approved equivalent.

5.2 NMS Workstations

The NMS workstations shall be installed at the Rhyne Building and the TERL. The FDOT will provide desk space for the installation of the workstation. The workstation UPS shall be installed on the floor as directed by the FDOT. The Vendor shall be responsible for powering up the workstation. The FDOT will connect the workstation to the FDOT network and install the VPN client software (if required). The Vendor shall install the NMS client and test its functionality.

6 CUTOVER REQUIREMENTS AND ACCEPTANCE TESTING

The Vendor shall install all equipment in its final location prior to system cutover. The Vendor shall provide the FDOT with a minimum of 10 days advance notice of system cutover. The Vendor shall furnish a detailed cutover plan to the FDOT for review and approval 14 days prior to cutover. The Vendor shall use the cutover procedures defined in this section to develop the cutover plan. The system will be cutover from the existing two server configuration (Pensacola / Tampa) to the proposed two server configuration (Tallahassee / McArthur).

The cutover shall be performed in two phases associated with the two server installations. For each phase, the Vendor shall verify ping response from each server to a sample of all equipment on the STN. The NMS shall begin monitoring a sample of equipment to verify that the alarm notifications are processed and emailed to the technicians. Equipment that supports multiple SNMP managers will have its secondary manager assigned to the new NMS server. For items that support only one manager, a sample of sites and equipment will be "re-homed" to the new NMS server. The Vendor shall verify that a sample of all equipment is being processed in the new NMS, including SCAN, SNMP, TL1, and ASCII. The Vendor will not be responsible for physically reconfiguring a device to work with the NMS. If a physical connection must be established, the FDOT will provide the manpower to perform the reconfiguration. However, the Vendor shall be on site (not remote) during the cutover and testing of the system.

The Vendor shall fully test the management of one device of each type with its own device driver. The FDOT will provide the personnel to activate the alarms and monitor the controls in the field. The Vendor shall be responsible for correcting deficiencies associated with the network management system.

6.1 Phase I: Tallahassee FHP Cutover and Acceptance Testing Requirements

The Tallahassee NMS server will monitor sites along I-10, I-95, I-4, and I-75 from SR-6 to Ocala DOT.

These sites are currently being monitored by the NetBoss servers at Pensacola and Tampa.

The Vendor shall coordinate with the FDOT and the FDOT Maintenance Contractor to turn off NetBoss processes on the Pensacola and Tampa servers in order to test the new NMS server.

After it has been demonstrated that the new NMS is properly monitoring the sample of equipment, the Vendor shall “re-home” the remaining equipment to the new NMS server.

6.2 Phase II: McArthur Cutover and Acceptance Testing Requirements

The McArthur server will monitor sites along I-75 from Wildwood to McArthur-Sunrise, Florida’s Turnpike Enterprise, Florida Keys’ sites and all fiber sites including and south of Orange County. These sites are currently being monitored by the NetBoss servers at Pensacola and Tampa.

The Vendor shall coordinate with the FDOT and the FDOT Maintenance Contractor to turn off NetBoss processes on the Pensacola and Tampa servers in order to test the new NMS server.

After it has been demonstrated that the new NMS is properly monitoring the sample of equipment, the Vendor shall “re-home” the remaining equipment to the new NMS server.

6.3 NMS Development Server

The Vendor shall demonstrate the “roll-over” of changes made from the development server to the operational servers. The Vendor shall provide the procedure for FDOT to perform roll-overs. The Vendor shall provide a test plan for FDOT approval that demonstrates changes including modification of existing scenes, addition of new scenes, addition of new scenes support new equipment and/or sites, modification of managed equipment device drivers and addition of new managed equipment device drivers.

6.4 Workstation

The Vendor shall demonstrate remote access and operation of client software to the NMS development server and each operational NMS server. The Vendor will not be responsible for network connectivity issues.

7 PERFORMANCE PERIOD

After successful completion of cutover and acceptance testing, the NMS system shall enter a 30-day performance test period. During the 30-day performance test period, the FDOT shall utilize the network management system for its intended purpose (production usage) to test all operational modes and equipment configurations, to ensure that the system functions properly and that all system "bugs" have been corrected. The use of the

system during this performance test period shall not be interpreted as being "accepted" by the FDOT.

Successful operation is defined as the absence of any major failure of equipment or software, or equipment or software function, which results in the disabling of a major equipment item, resulting in the inability of the overall system to perform as specified. Minor failures, such as operational problems and adjustments normally encountered during implementation of a new system, shall not constitute a failure in achieving successful operation.

Failures associated with lightning damage shall not be the responsibility of the Vendor. The Vendor shall present evidence of lightning damage to the FDOT before filing a claim. The FDOT shall review for approval any claim associated with damage due to lightning.

In the event of a major failure, the Vendor shall correct the issue and the 30-day performance test period will be restarted at Day 1. If a successful performance period cannot be accomplished within two attempts, or within 90 days of the completion of the cutover and acceptance testing, the FDOT reserves the right to deem the Vendor in default and enforce the provisions set forth in the contract.

8 TRAINING REQUIREMENTS

The Vendor shall provide two types of training: “System Administrator” and “Operator and Maintenance”.

The training shall be held in an appropriately equipped training facility within the State of Florida where the trainees will have hands on training with similar hardware. The personnel being trained shall be exposed to and shall be able to directly manipulate all of the software applications and operating systems as installed as part of this project. The personnel being trained shall have exposure to, but shall not be limited to, all aspects of network management system applications, computing hardware, and networking hardware.

The System Administrator training shall be provided for 5 people. The System Administrator training shall include training to maintain, configure, and operate the NMS including build graphics, build device drivers, edit graphics and device drivers, populate the database, and customize the system.

Operator and Maintenance Training shall be provided in three (3) groups of seven (7). The Operator and Maintenance training shall include viewing alarms, acknowledging and clearing alarms, placing alarms in maintenance mode, use of all monitoring software, using the reporting tools, and customizing the user experience.

9 WARRANTY AND MAINTENANCE & SUPPORT AGREEMENT REQUIREMENTS

9.1 Warranty

All equipment and services furnished by the Vendor as part of this project shall be warranted to be free from defects in material and workmanship, and shall conform to these Technical Specifications. In the event such defects in equipment or services become evident within the warranty period, the Vendor shall correct the defect by, at its option, (1) repairing any defective component of the equipment; (2) furnishing and installing necessary replacement parts; or (3) redoing the faulting services. The Vendor is responsible for all charges incurred in returning defective parts to the Vendor's, subcontractor's, or supplier's plants, and in shipping repaired or replacement parts to the FDOT. The Vendor shall provide labor to perform warranty services at no charge to the FDOT during the warranty period. The Vendor further warrants that during the warranty period, equipment furnished under this contract shall operate under normal use and serves as a complete system, which shall perform in accordance with these Technical Specifications. The warranty period shall be a period of at least 12 months from the date of final system acceptance as defined herein. Claims under any of the warranties herein are valid, if made within 30 days after termination of the warranty period.

9.2 Maintenance Agreement Requirements

After the expiration of the warranty period, the FDOT shall enter into a maintenance agreement with the Vendor to provide continued software support, upgrades, and enhancements for the network management software provided as part of this project (Monday through Friday, 8 AM to 5 PM EST). In addition, the FDOT shall enter into a maintenance agreement with the Vendor to provide continued hardware support for the servers.

The Vendor shall provide a document outlining standard software maintenance and support to the FDOT. The standard support shall include the following:

- Standard maintenance Monday-Friday, 8:00 am to 5:00 pm EST
- Future versions/upgrades of management software at no cost

- Guaranteed Response times for different levels of problems
    - Critical – Critical functions are not operating and Equipment is not being managed - One (1) hour initial call back, Twenty-four (24) hour resolution
    - Major – Non-Critical functions are not operating- Four (4) hour initial call back, Five (5) day resolution
    - Minor – Non-operational failures or areas that require improvement – Two (2) day initial call back, resolution with next software release

The Vendor shall provide Original Equipment Manufacturer (OEM) warranty on-site support for a minimum of five (5) years. The hardware support shall include the OEM's standard equipment warranty terms and conditions.

Because of security requirements of the STN, all upgrades to the system must be accomplished without access to the public Internet. The Vendor shall provide procedures for performing upgrades and updates as needed to the NMS, including the server operating systems without access to the Internet.

10 DOCUMENTATION REQUIREMENTS

10.1 Site Documentation

The Vendor shall provide a complete set of documentation for the equipment installed at each site. This documentation shall include all equipment manuals, software manuals, hardware and software licenses, administrative and maintenance procedures, documentation on the overall system configurations, and software, hardware, and network configurations.

10.2 System Documentation

The Vendor shall provide all equipment manuals, software manuals, and maintenance procedures for all equipment and software. In addition, the system configurations shall be documented for all hardware, software, and networking for the entire system.

The system configurations shall take the form of diagrams, lists, descriptions, parameters, and procedures organized and assembled under one cover. Hardware and software licenses shall also be included in the system documentation. The Vendor shall provide four sets of system documentation to the FDOT for review and approval and shall reflect the as-built conditions for the installed systems. All system passwords and software code keys shall also be included.

The Vendor shall provide the administrator level group/user ID and passwords to the FDOT.

10.3 Network Management Software Clients

The Vendor shall provide to the FDOT two copies of the network management software clients. The software client package shall contain all manuals, installation procedures, cheat sheets, and software as a complete deliverable.

If licenses are required for users on the system, the vendor shall include a minimum of 25 licenses.

10.4 Original Software Installation Images

All original software installation images shall be delivered to the FDOT and shall be included with all installation procedure documentation and software manuals. In

addition, all software licensing documentation, software code keys, and passwords shall be included as well.

10.5 Backups

The Vendor shall provide the initial backup of all of the network elements onto the Vendor proposed backup system. The Vendor will take at least one complete system backup of each server (NMS and e-mail) following final system acceptance, and provide the backup to FDOT on a separate storage medium (such as USB hard drives or DVD-ROM discs) for archival purposes. Additionally, the Vendor shall identify the backup procedures (complete, incremental, and differentials), provide for a backup schedule, and identify the restoration procedure for each system.

11 MANAGED EQUIPMENT LIST

The Vendor shall configure the NMS to manage the equipment listed in Table 1. The FDOT will provide the Vendor with the locations and IP addresses of each managed element.

The FDOT also has planned future equipment to be installed. This equipment is listed in Table 2.

Table 1 - Managed Equipment List

Device	Quantity	Management Protocol Support	Comments
Harris DVM6-45	120	SCAN	Managed via 99 separate SCAN regions.
Harris DVM-10/8T	2	SCAN	
Harris DVA	35	SCAN	
Harris DV12/16T	4	SCAN	
Harris Constellation	12	SCAN or SNMP	
Larus Starclock STS5800	14	TL1	
Nortel Passport 15000	14	SNMP	
Nortel ASN Router	85	SNMP	
Nortel BPS 2000 Switch	70	SNMP	

DPS Telecom NetGuardian 832A	85	SNMP	
Telco Systems Access 60 Channel Bank	56	SNMP	
Eastern Research (Sycamore) DACC DNX-11	14	SNMP	
Carrier Access Widebank 28 M13 mux	35	SNMP	
Adtran Opti 3 Fiber mux	6	SNMP or TL1	
Ciena Optical Metro 5200	20	SNMP or TL1	
Avaya Ethernet Routing Switch 8800	2	SNMP	
Avaya Ethernet Routing Switch 8600	9	SNMP	
Avaya Virtual Services Platform VSP-4450	3	SNMP	
4RF Aprisa XE 960MHz MW radio	4	SNMP	
4RF Aprisa FE 960MHz MW radio	4	SNMP	
4RF Aprisa SE 960MHz MW radio	4	SNMP	
Telco Systems T-Metro	3	SNMP	
MDS LEDR 900-TNE200/900	2	SNMP	
Telco Edgelink 100	6	SNMP or TL1	
Multitech MultiVoip MVP210 and MVP410	70	SNMP	
Nortel Baystack Hub	70	SNMP	
Patton Electronics IPLink 2603/T/48	1	SNMP	
Adtran TDU 120e	1	SNMP	
Valere Compact DC Power System BC2000 controller	4	SNMP	
Eltek FlatPack2	6	SNMP	
Generex Battery Monitors BACS Webmanager Budget II	30	SNMP	Additional units being added.
JPS SNV12 Voter	7	ASCII	
Larus TiemPo clock	2	TL1 or SNMP	
Perle IOLAN STS16	2	SNMP	

Technostrobe Obstruction Lighting System - Lantronix	6	SNMP	

Table 2 – Future Equipment List

Device	Management Protocol Support
Ciena Converged Packet-Optical Platform 6500 series	SNMP
Ciena Packet Networking 3900 Series	SNMP
Avaya IP Office 500 VoIP Platform	SNMP
Avaya Identity Engines roles-based Network Access Controller	SNMP
Avaya VSP-8000	SNMP
Avaya VSP-9000	SNMP
Cyberoam CR50iNG VPN Gateway	SNMP
TrippLite SmartPro VS UPS and SNMPWebCard	SNMP
Patton Electronics IPLink 2620/T/48	SNMP
Alcatel Lucent 7705 Service Aggregation Router	SNMP
Alcatel Lucent 7750 Service Router	SNMP
Alcatel Lucent 5620 Service Aware Management System (SAM)	SNMP
Alcatel Lucent OmniSwitch 6860	SNMP
Alcatel Lucent MPR9500	SNMP
Cisco ASR 9006	SNMP
Cisco Catalyst 2960X	SNMP
Cisco ASR 920	SNMP
Cisco Catalyst 2060-X	SNMP
RAD RiCi 16	SNMP
Dragonwave Harmony Microwave Radios	SNMP

Dragonwave Horizon Microwave Radios	SNMP
Aviat IRU-600	SNMP
NEC iPASOLINK 100/200/400/1000	SNMP
Microwave Networks Proteus MX	SNMP
Ericsson Mini-Link series	SNMP
Spectracom SecureSync	SNMP
Transition Networks Packetband TDM 16/32	SNMP