Volume 2 – Technical Proposal

Nebraska State Patrol
MSS Modernization Project
Volume 2 – Technical Proposal
RFP No. 6724 Z1

Submitted by:
Datamaxx Applied Technologies, Inc.
FED ID: 59-3081678
DUNS No.: 55-689-8229

2001 Drayton Drive
Tallahassee, Florida 32311
(850) 558-8000
January 26, 2023

Contact Person:
David Stephenson, Senior Account Executive
Telephone: (850) 558-8505
E-mail: david.stephenson@datamaxx.com

Table of Contents

2. VOLUME II – TECHNICAL PROPOSAL

A. Project Understanding

The bidder should provide narrative describing their understanding of the NSP MSS modernization project. An explanation of how the proposed solution addresses the issues and opportunities outlined in the RFP should be included.

Datamaxx Response: Datamaxx understands the scope and implementation of the system.

Datamaxx also understand the criticality of the implementation overall, including the project management and reporting requirements.

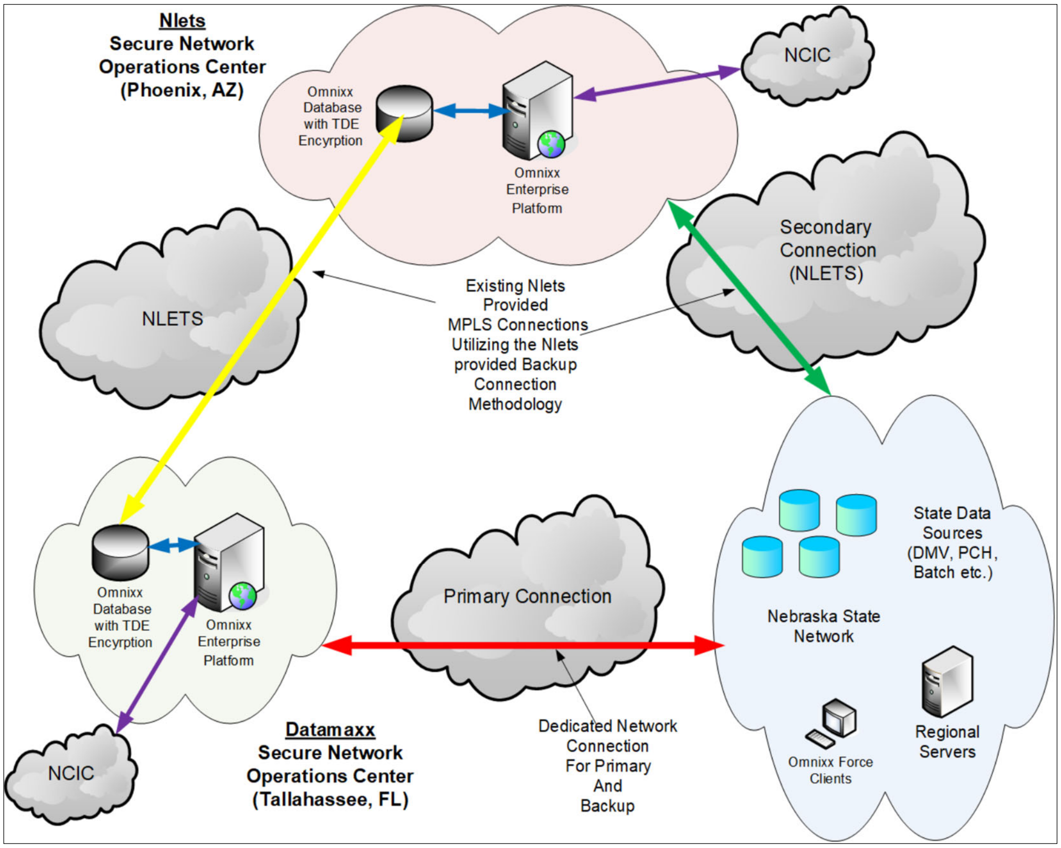
There are several stringent requirements in this specification, especially when it comes to the disaster recovery functionality. In creating this response Datamaxx considered very carefully the approach to the Disaster recovery, not only from the functional point of view but from the overall perspective of what would be the best for the State. These considerations had an impact on the overall architecture, as will be explained in this section.

Datamaxx has provided the system for many years and while conceptually the new system will appear identical to the users (while providing new functionality), the implementation will require careful thought and architecture.

The first decision point is "where the system resides", and we considered two potential options for the location of the system.

1. A commercial cloud provider, such as Microsoft Azure, and
2. The Datamaxx Secure network operations center (NOC)

In this proposal, the primary system will reside in the Datamaxx Network Operations Center (NOC) and the Disaster Recovery will be hosted at the Nlets NOVA hosting center in Phoenix, Arizona, as shown below.



Using the Datamaxx NOC as the primary and Nlets as the disaster recovery site provides several advantages, and the reasons for this decision are as follows:

- **The Datamaxx NOC already has hosted state systems that use NCIC and Nlets**. The primary, dedicated connection between the Datamaxx NOC and the Nebraska network will need to be established, but the communications circuits for NCIC and Nlets are already in place and the accompanying equipment (secure routers, encryption hardware, etc.) are installed in the NOC and available to Datamaxx personnel.

  This avoids the risk of having NCIC and Nlets circuits terminate and be managed inside a commercial hosting service. There is a concern that the commercial service staff may not be fully aware of the criticality of these interfaces and may not have the necessary knowledge of their operation, whereas the Datamaxx staff have immediate accessibility.

- **Both the State and Datamaxx already have communications circuits to Nlets.** Thus, the network paths are already in place when the Disaster Recovery system needs to be activated. This eliminates any risk from the backup network paths that must be in place at a commercial hosting service and may be rarely used and thus may not have complete attentions from the commercial staff, when the switch to the Disaster recovery site be needed.

Effectively, everything is managed at a single point of contact with Datamaxx personnel available 24 hours a day.

The switch, hot files and interfaces to NCIC and Nlets will reside in the Datamaxx Secure Network center. State data sources (e.g. DMV, Patrol Criminal History, etc.) will not be relocated or modified, as they are outside the purview of the State Patrol in all cases, except for PCH.

Also, it cannot be assumed that these data sources will make any changes to allow connectivity from domains outside of the control of the State. Such changes are out of the control of the State Patrol and would affect the schedule of this implementation and thus must not be considered.

Another consideration is that there are client systems, such as the batch processes for uploading inputs from other organization's and interfaces from remote systems, such as those used by city and county systems. These cannot be expected to make any modifications, except for normal configuration changes, such as an IP address. The external agencies that feed these processes are also outside of eth control of the State Patrol and thus cannot be relocated.

In order to address these issues, Datamaxx provides a hybrid model that places all components in the cloud, but allow the State data sources and clients to operate as they were before, with no changes, except for a potential configuration change for client interfaces.

In order to address these issues, Datamaxx provides a hybrid model that places all components in the cloud, but allow the State data sources and clients to operate as they were before, with no changes, except for a potential configuration change for client interfaces. The final determination of the network paths and connections will be determined during the project design and configuration.

Datamaxx has a strategy that has been implemented for the other systems that operate from the Datamaxx NOC but access state data sources that has been well proven.

The data sources are accessed by local services, should these data sources have restrictions on the network points from which they can be accessed. If an individual data source can be configured to accept communications from a remote system in the NOC via a secure connection, then the interface will be located in the NOC. If the data source requires access from a local point (e.g. the DMV system that is hosted by the State OCIO) then the interface will be installed locally in order to protect that access.

This approach allows a "mix-and-match' approach depending on the data source involved.

Importantly, the data sources are not impacted, and are unaware of the changes that may have been made to the location of the message switch itself. This uses the network infrastructure as described in this proposal. No changes to the data streams are required.

For the client implementations (*such as the batch processes*), these can be configured to access the NOC via a secure connection or via an intermediate service provided by Datamaxx. This will preserve the integrity of the operations and the external entities that feed the batch processes (*and receive and process responses*) will be unaffected.

This hybrid strategy has already been deployed in 2 other State systems, and has been operating for 22+ months now in a full production environment. This approach reduces risk as it has the flexibility to adapt to the existing implementations that are external to the current message switch, without requiring changes to them.

The strategy that is proposed will provide the State with the best balance of cost, reliability and maintainability.

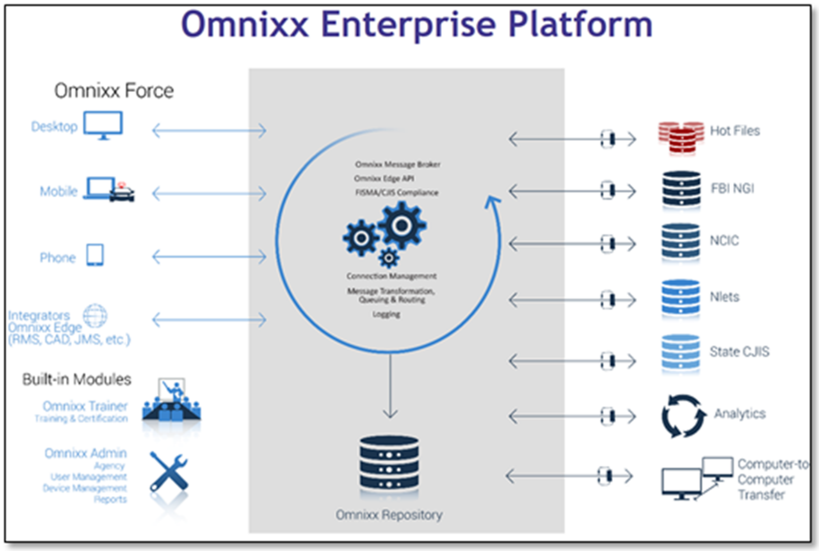
Datamaxx understand clearly the implementation, as similar implementations in the Datamaxx Cloud, including hot files, are operating and have been operating in production for several years.

B. Proposed System Design

The bidder should include a proposed design solution within the proposal. The design solution should be described in detail to demonstrate that the proposed design meets the requirements of the RFP. There is no minimum degree of detail required.

The bidder should identify the major subsystems or components (e.g., configuration items) that compose the proposed system architecture. The bidder should discuss how each major subsystem or component and interface to other systems (outlined in the requirements) will be implemented and tested, i.e., in developed hardware or software; by using COTS products; or to-be-developed hardware or software or combinations of same. The bidder should indicate what new product development (e.g., custom software, COTS extension or customization) and integration products (e.g., services layer, glue code), if any, are required.

Datamaxx Response: The proposed Datamaxx Omni*xx* Enterprise, which includes the Omnixx Enterprise Platform® and the Omni*xx* Force® suite of solutions, provides a solid foundation for deploying highly secure mission critical systems including message brokering, enterprise searching, enterprise reporting, information sharing and access, data collection and workflow, monitoring, and mobile capabilities – all from one server platform.

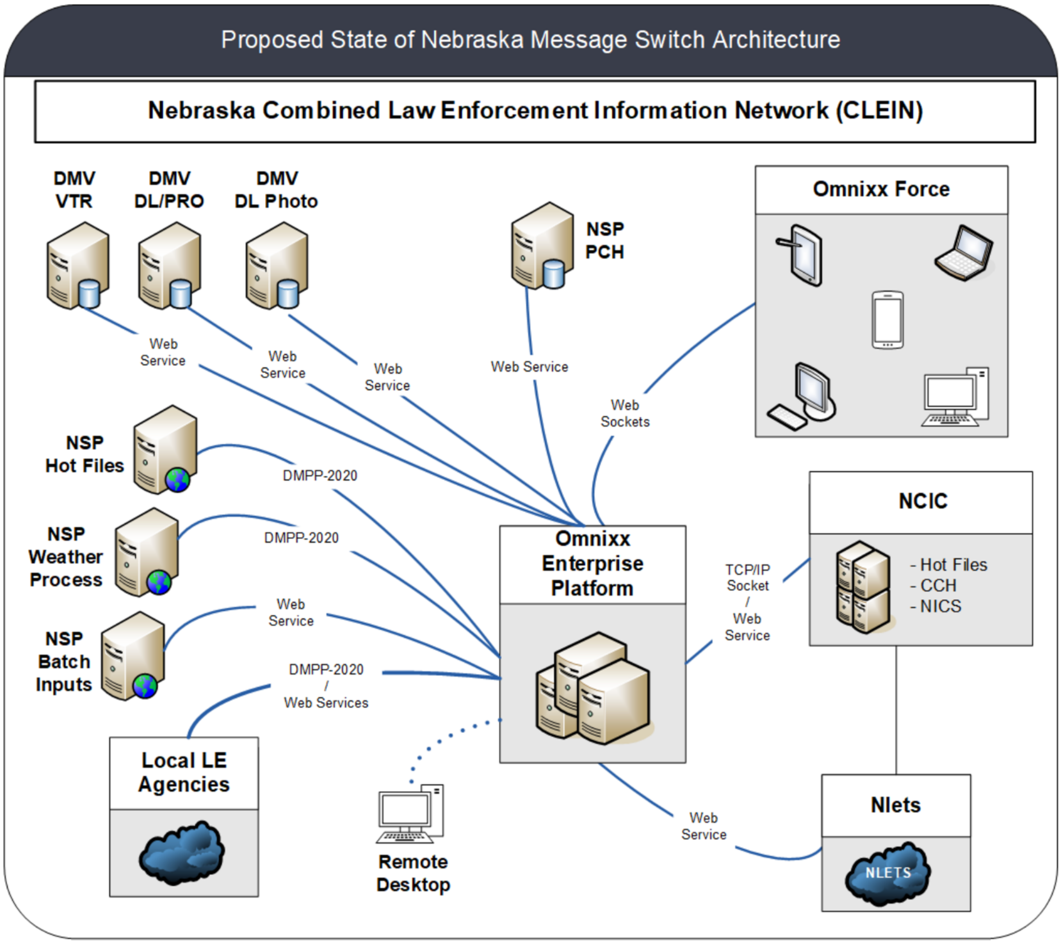


The core component is the proven Omni*xx* Enterprise Platform with Omni*xx* Message Broker and Omni*xx* Force End User Interface, which provides NSP with a proven, scalable distributed architecture second to none.

It provides all of the necessary services (Message Switch, connection management, queuing, routing, message transformation, logging, reporting, and repository for users, devices, business rules).

It provides support for all of the necessary protocols for connecting to the various National, State, and In-State Systems (e.g. TCP/IP, HTTPS, TLS, REST, SOAP, MSMQ, DMPP-2020, etc.) and provides an external adapter methodology that can be adapted for non-standard interfaces.

The recommended solution for NSP is to utilize the Omni*xx* Enterprise Platform to provide secure connectivity to Nebraska agencies, the National Crime Information Center (NCIC) and the National Law Enforcement Telecommunications System (Nlets) and additional information systems as shown in the following Proposed Architecture diagram.



The high-level scope for this project will include the following with regard to the features and functions of the Omni*xx* Enterprise Platform:

- Compliance and support of transactions, codes and requirements of NCIC, Nlets, NSP operating manual and published FBI updated Technical and Operational updates (TOUs).
- Maintenance feature to allow administrators capability to control and manage transaction forms and associated elements list.
- Support for the modern web browsers
- Support for high availability and disaster recovery
- Phased approach for regional system providing support for existing socket connections and enabling a smooth transition to web services.
- A web-based HTML 5 responsive web-based user interface (GUI) for front end user entry and receipt of message key data.
- Support for Advanced Authentication and SAML 2.0.
- Support for the CJIS Security Policy and encryption for data at-rest and in transit.
- Support for administrative functions including managing users, devices, ori, and configurations.
- Integrated reporting including statistics, user access, user access history, transaction and security logs.
- Support for state data source interfaces including DMV-VTR, DMV DL/PRO, DMV DL Photo, NSP PCH, NSP Hot Files, NSP Weather Process, NSP Batch Input, NSP Local LE Agencies, NCIC and Nlets.

The following pages provide a detailed summary of the proposed system capabilities.

High level features include:

- Supports Multiple Messaging Formats (e.g. XML and Dot/Slash Text formats)
- Broadcast Messaging
- Guaranteed Message Delivery
- Message Forwarding, Spawning and Carbon Copying
- Monitoring, Alerts & Notifications
- High performance, responsive zero-footprint client that runs on desktops, laptops, smart phones, and tablets
- Shared user repository via web services
- Integrates with LDAP, Active Directory, SAML 2.0 (as a Service Provider)
- Compression
- Powerful differencing and synchronizing engine
- Robust web-based user management/separation of duties
- Restrict application and transaction access to configurable roles
- SQL Server Reporting Services Integration
- SOAP and REST Support
- XML, JSON, JavaScript, HTML, XSLT, CSS
- Multiple Tier-1 Proxies – secure access in the DMZ
- Full Audit Logging with Searchable Logs – simple and complete queries; scheduled search jobs for large data sets and broad time ranges (e.g. multi-year) email the user when complete.

- Schedule-Based Alternate Routing – non-24 hour agency devices automatically alt route to 24 hour devices on nights and weekends
- FIPS 140-2 CJIS compliant encryption.

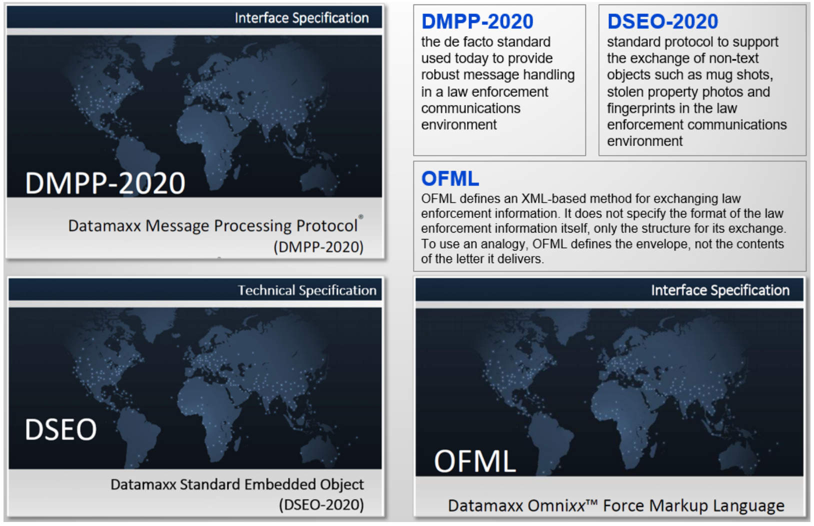
The Omni*xx* Enterprise Platform is a proven and robust platform providing many regional, state, and federal locations a reliable system including the Federal Bureau of Investigation, Department of Justice, Washington State Patrol, Louisiana State Police, Georgia Bureau of Investigation, Nebraska State Patrol, Montana DOJ, North Carolina DOJ, South Carolina Law Enforcement Division, Maryland DPS, South Dakota DPS, Mississippi DPS, Iowa DPS, Puerto Rico DOJ, Guam DOJ, and many regional locations in California, Georgia, and Florida. Many locations have been using the Omni*xx* Enterprise Platform for over 10 years.

The Omni*xx* Enterprise Platform also provides best in class support for XML formatted message exchange to Nlets, NCIC, as well as other systems that employ GJXDM (Global Justice XML Data Model), and NIEM (National Information Exchange Model).

Datamaxx invented and published several technology standards that have been embraced by the law enforcement community and all major law enforcement vendors.

These standards will provide:

1) **DMPP-2020** – the <u>Datamaxx Messaging Processing Protocol</u> provides a standard approach for communications and guaranteed message delivery. DMPP-2020 is now a standard, used in over 30 States.
2) **OFML** – <u>Omni*xx* Force Markup Language</u> - defines a robust and consistent XML-based method for exchanging law enforcement information.
3) **DSEO** – <u>Datamaxx Standard Embedded Object</u> – standard protocol to provide symmetric support of non-text objects such as mug shots, stolen property photos, fingerprints, driver's license photos, etc.


Interface Specification
DMPP-2020
Datamaxx Message Processing Protocol®
(DMPP-2020)
Technical Specification
DSEO
Datamaxx Standard Embedded Object
(DSEO-2020)
Interface Specification
OFML
Datamaxx Omnixx™ Force Markup Language

DMPP-2020
the de facto standard used today to provide robust message handling in a law enforcement communications environment

DSEO-2020
standard protocol to support the exchange of non-text objects such as mug shots, stolen property photos and fingerprints in the law enforcement communications environment

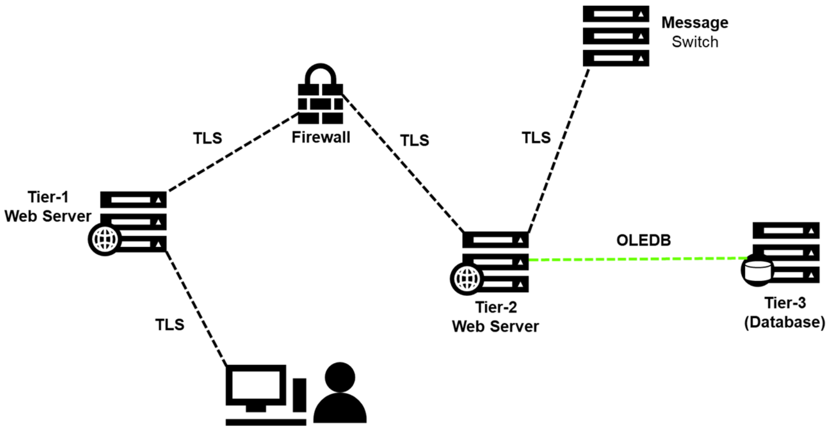
OFML
OFML defines an XML-based method for exchanging law enforcement information. It does not specify the format of the law enforcement information itself, only the structure for its exchange. To use an analogy, OFML defines the envelope, not the contents of the letter it delivers.

These provide a proven solid foundation for deploying highly secure mission critical law enforcement systems, and provides a reliable standard for NSP to adopt for future growth and 3rd party migration and supports existing interfaces as the same time.

The Omni*xx* Enterprise Platform was built from the ground up leveraging the best in Microsoft platforms, technologies, and development tools. It is a robust platform leveraging Microsoft technologies such as .Net, SQL Server, and Windows OS technologies providing a flexible and familiar environment that integrates natively with Windows. One example of deep integration with Windows is that the Omnixx Enterprise Platform utilizes the core Windows kernel HTTPS driver which provides high performance web services from the Windows core OS. This driver is highly optimized and scalable and is the same driver used by Internet Information Services (IIS) to serve up high performance web sites by Windows.

Another unique feature offered by the Omnixx Platform is it exposes Web Services for items stored in repository (e.g. User Profiles, Device Configurations, Groups, Roles, ORIs, Archive Log, etc.) and to send and receive messages. These powerful features mean that any application needing to access to the repository information and/or send and receive transactions, it can do so in a secure and standardized way (XML over TLS 1.2) utilizing industry standard web services. No other MSS vendor offers this flexibility.

The Omnixx Enterprise Platform is "n-tiered" and can be configured to have multiple tiers distributed across multiple physical platforms, if desired. There is a "gateway" tier, an "application" tier, and a "database" tier that can be co-located or placed on separate physical or virtual machines depending upon the requirements for how it is to be deployed within the network. This provides many advantages for securing access to the data sources as well as for scalability, redundancy, and disaster recovery.



The architecture is "firewall friendly" in that access between servers use standard Internet technologies such as "Simple Object Access Protocol (SOAP)" and REST. This permits components such as the repository database to be located within a secured network a protected by firewalls, with no requirement to open access to any other function except those required by the Transport Layer Security Protocol (TLS).

This is an important level of indirection, as it allows end user access to the user facing components (such as the Web Server and communications components) but prevents any user access to protect items such as direct host system or database access. This architecture also provides distributed and delegated administrative capabilities via a web browser.

The system console web application is used to manage user profiles, devices, configurations, reports, etc. It provides fine-grained control of the features by using certifications or roles to control access to them. For example, an administrative user can be configured to access only those user accounts within his or her agency, providing a way to delegate user maintenance in a restricted fashion. This fine-grained control provides a unique feature that is configurable to provide access to functions within the system.

The Omni*xx* Enterprise Platform incorporates all communications, message switching and routing, with access to all necessary data sources. The communications component will serve as the hub for NSP users to access law enforcement related networks and databases.

It provides standard interfaces that facilitate the seamless integration of multiple types of devices. It will add data content processing using open standards, including "XML", while maintaining compatibility with existing data streams.

It is inherently capable of handling any form of Binary data (e.g. images, documents), without being restricted to fixed standards, such as the NCIC Image format specification. It will also allow for "URL" based exchange of data, from any authorized Web based repository, using Web Services and XML.

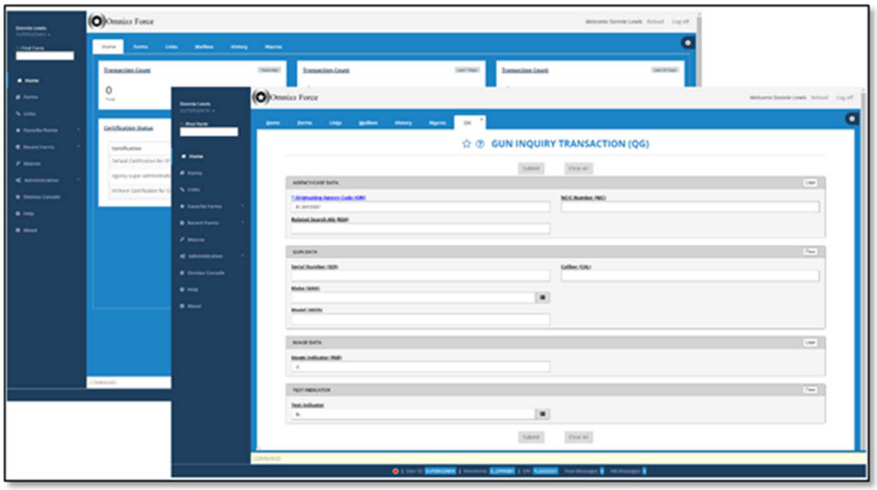
Datamaxx has been designing and developing Law Enforcement interfaces for over 2 decades, and completely understands the intricacies of each protocol and interface.

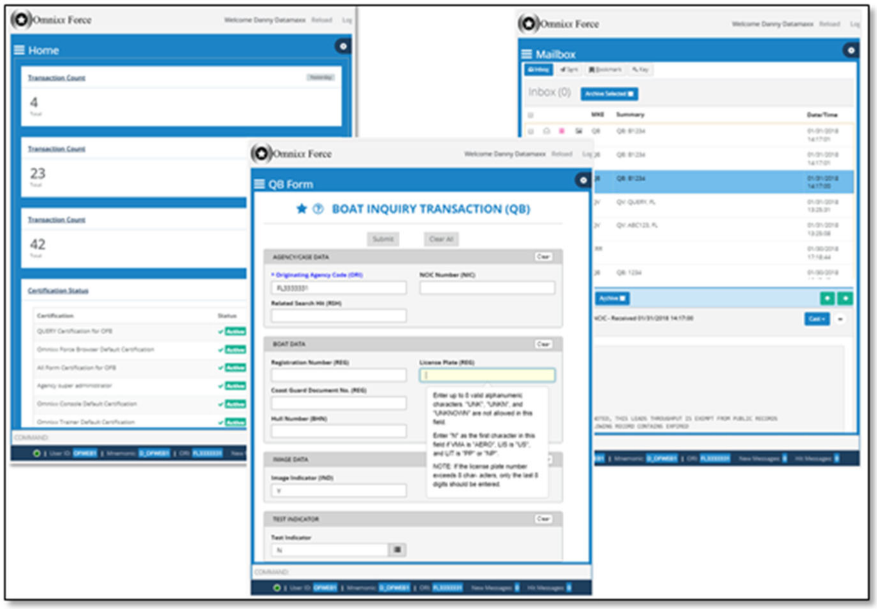
Using the various protocols, the Omni*xx* Enterprise Platform provides a seamless transition to new technologies, providing a platform for future growth, and at the same time provides support for legacy interfaces and protocols, where applicable.

This is especially important to regional systems whereas 3rd party systems can continue to operate using their current documented interface control strategies, and the platform will provide uninterrupted support. Datamaxx has proven experience transitioning to the new platform while support legacy interfaces.

The Omni*xx* Enterprise Platform® also provides the Omnixx Force® HTML5 end-user interface, which is a high performance, responsive zero-footprint client that runs on desktops, laptops, smart phones, and tablets. It provides an easy to use, modern interface with easy to use fill-in forms and command line entry, and a variety of user options for message display, saving favorites, and workspaces for commonly used forms.

The screenshots below depict the interface on a desktop, tablet, and smart phone device. Responsive design is incorporated enabling the interface to adapt to the screen size of the device it is being presented on. In addition, the interface is optimized for mobile users to provide commonly used queries (Person, Vehicle, Article, Boat, and Gun) and provides advanced features for desktop users such as workspaces for multiple forms and mailbox undocking for multi-monitor environments commonly used by dispatchers. Also, command line, configurable keystrokes, favorites, most recently used forms, night mode, and many other properties are saved for each user giving each user the ability to customize the interface for their use.

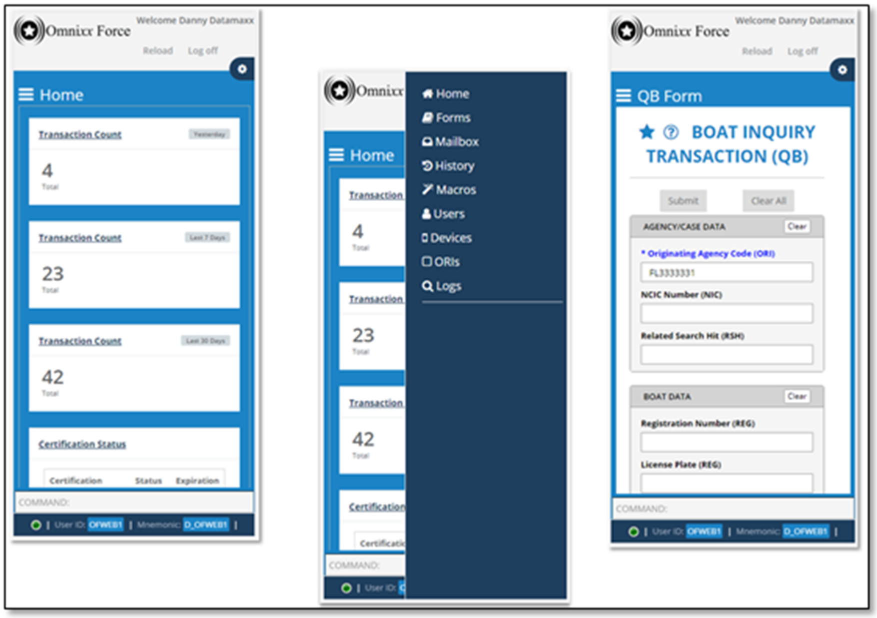




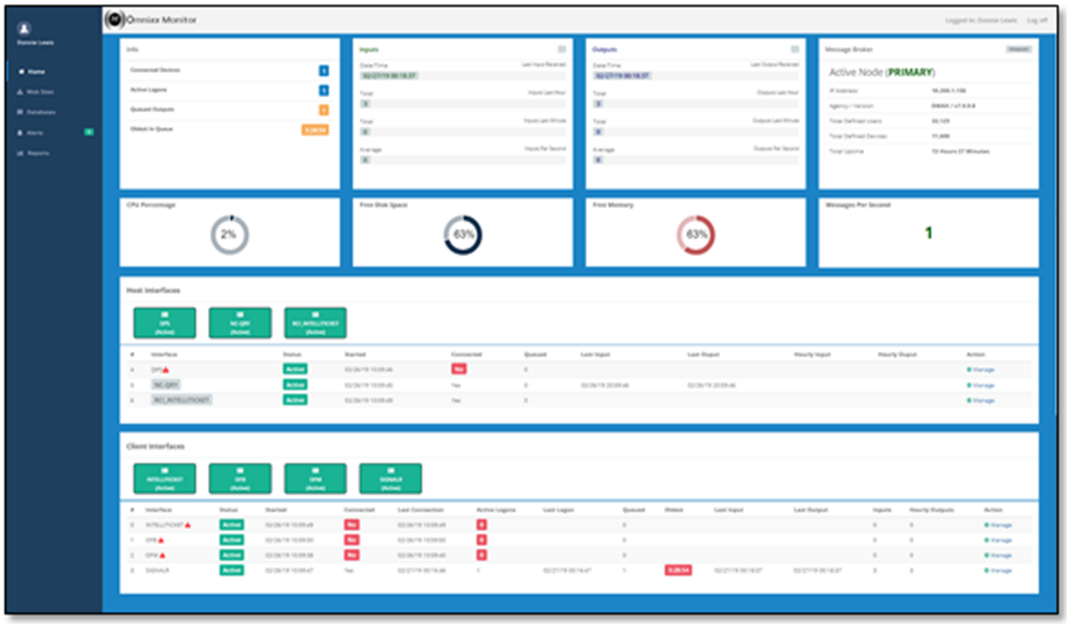
Enter up to 8 valid alphanumeric characters. "UNK", "UNKN", and "UNKNOWN" are not allowed in this field.

Enter "N" as the first character in this field if VMA is "AERO", LIS is "US", and LIT is "PP" or "NP".

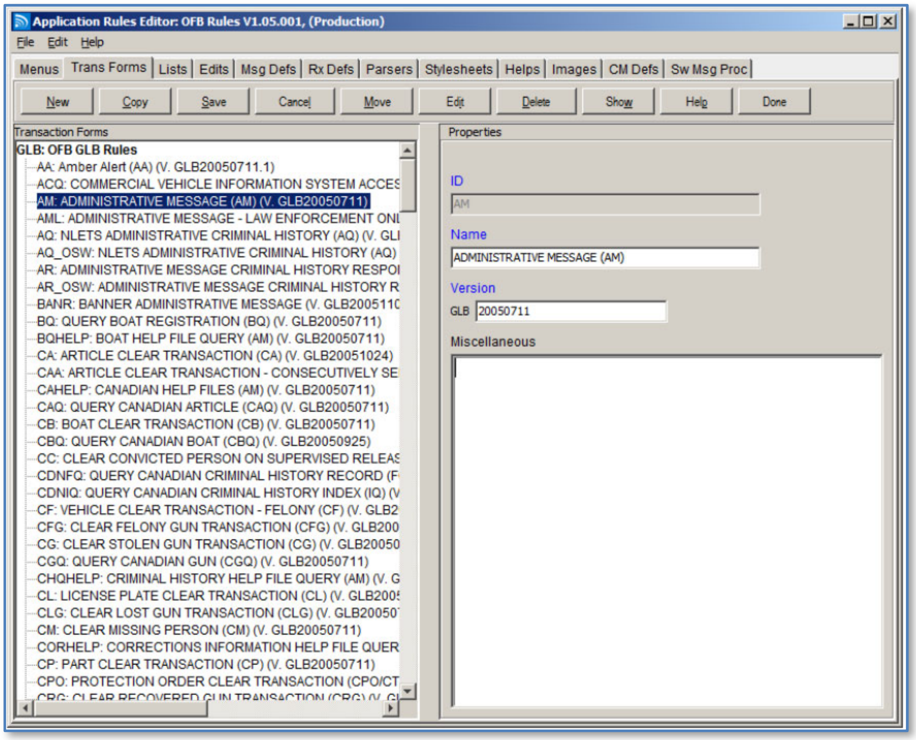
NOTE: If the license plate number exceeds 8 char- acters, only the last 8 digits should be entered.



For Omni*xx* Enterprise performance monitoring, interface status, queue status and management, etc., the platform includes Omni*xx* Monitor, an operational dashboard that provides a visual display of the system, including real-time statistics, CPU, disk, memory health, messages per second, database and website available, queue status, interface status and message statistics. Critical events that exceed a threshold (such as high CPU or memory use, or disk space low) will log entries into the Windows Event log, which can trigger notifications to system administrators.



The Omni*xx* Enterprise Platform also provides the tools to make changes to existing message keys and the addition of new message keys by authorized administrators.



Transaction Forms

GLB: OFB GLB Rules
- AA: Amber Alert (AA) (V. GLB20050711.1)
- ACQ: COMMERCIAL VEHICLE INFORMATION SYSTEM ACCES
- AM: ADMINISTRATIVE MESSAGE (AM) (V. GLB20050711)
- AML: ADMINISTRATIVE MESSAGE - LAW ENFORCEMENT ONI
- AQ: NLETS ADMINISTRATIVE CRIMINAL HISTORY (AQ) (V. GLI
- AQ_OSW: NLETS ADMINISTRATIVE CRIMINAL HISTORY (AQ)
- AR: ADMINISTRATIVE MESSAGE CRIMINAL HISTORY RESPOI
- AR_OSW: ADMINISTRATIVE MESSAGE CRIMINAL HISTORY R
- BANR: BANNER ADMINISTRATIVE MESSAGE (V. GLB2005110
- BQ: QUERY BOAT REGISTRATION (BQ) (V. GLB20050711)
- BQHELP: BOAT HELP FILE QUERY (AM) (V. GLB20050711)
- CA: ARTICLE CLEAR TRANSACTION (CA) (V. GLB20051024)
- CAA: ARTICLE CLEAR TRANSACTION - CONSECUTIVELY SE
- CAHELP: CANADIAN HELP FILES (AM) (V. GLB20050711)
- CAQ: QUERY CANADIAN ARTICLE (CAQ) (V. GLB20050711)
- CB: BOAT CLEAR TRANSACTION (CB) (V. GLB20050711)
- CBQ: QUERY CANADIAN BOAT (CBQ) (V. GLB20050925)
- CC: CLEAR CONVICTED PERSON ON SUPERVISED RELEAS
- CDNFQ: QUERY CANADIAN CRIMINAL HISTORY RECORD (F
- CDNIQ: QUERY CANADIAN CRIMINAL HISTORY INDEX (IQ) (V
- CF: VEHICLE CLEAR TRANSACTION - FELONY (CF) (V. GLB2
- CFG: CLEAR FELONY GUN TRANSACTION (CFG) (V. GLB200
- CG: CLEAR STOLEN GUN TRANSACTION (CG) (V. GLB20050
- CGQ: QUERY CANADIAN GUN (CGQ) (V. GLB20050711)
- CHQHELP: CRIMINAL HISTORY HELP FILE QUERY (AM) (V. G
- CL: LICENSE PLATE CLEAR TRANSACTION (CL) (V. GLB2005
- CLG: CLEAR LOST GUN TRANSACTION (CLG) (V. GLB20050
- CM: CLEAR MISSING PERSON (CM) (V. GLB20050711)
- CORHELP: CORRECTIONS INFORMATION HELP FILE QUER
- CP: PART CLEAR TRANSACTION (CP) (V. GLB20050711)
- CPO: PROTECTION ORDER CLEAR TRANSACTION (CPO/CT
- CRG: CLEAR RECOVERED GUN TRANSACTION (CRG) (V. GL

Properties

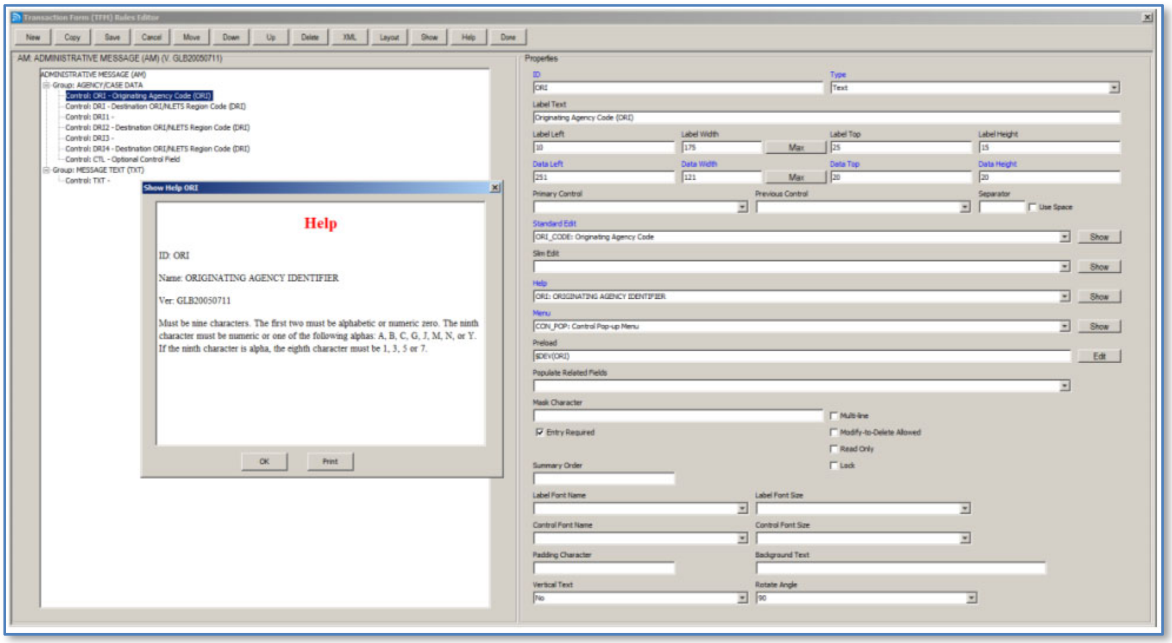
ID: AM

Name: ADMINISTRATIVE MESSAGE (AM)

Version: GLB 20050711

Miscellaneous

Transaction Forms and associated components (e.g. code tables, field help, field edits or validations, message processing scripts, stylesheets, etc.) and displays of message keys are defined by "business rules" and are managed using the Omni*xx* Application Rules Editor (ARE) which provides a graphical user interface to manage the XML documents.



AM: ADMINISTRATIVE MESSAGE (AM) (V. GLB20050711)

ADMINISTRATIVE MESSAGE (AM)
- Group: AGENCY/CASE DATA
  - Control: ORI - Originating Agency Code (ORI)
  - Control: DRI - Destination ORI/NLETS Region Code (DRI)
  - Control: DRI1 -
  - Control: DRI2 - Destination ORI/NLETS Region Code (DRI)
  - Control: DRI3 -
  - Control: DRI4 - Destination ORI/NLETS Region Code (DRI)
  - Control: CTL - Optional Control Field
- Group: MESSAGE TEXT (TXT)
  - Control: TXT -

Help

ID: ORI

Name: ORIGINATING AGENCY IDENTIFIER

Ver: GLB20050711

Must be nine characters. The first two must be alphabetic or numeric zero. The ninth character must be numeric or one of the following alphas: A, B, C, G, J, M, N, or Y. If the ninth character is alpha, the eighth character must be 1, 3, 5 or 7.

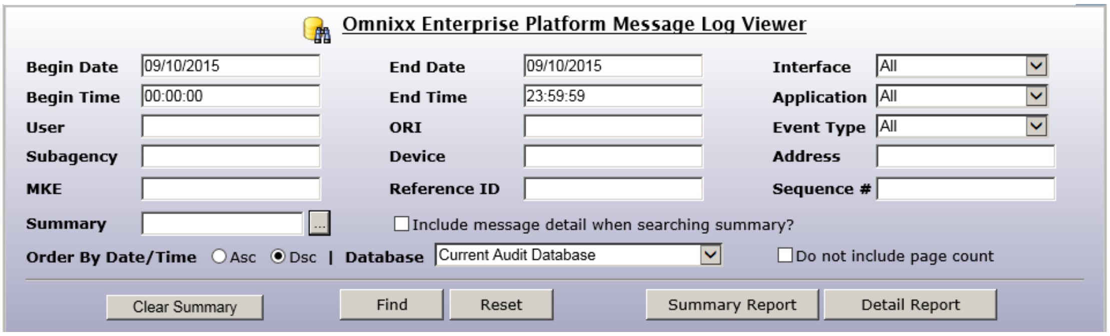
Properties

ID: ORI
Type: Text
Label Text: Originating Agency Code (ORI)
Label Left: 10
Label Width: 175
Label Top: 25
Label Height: 15
Data Left: 251
Data Width: 121
Data Top: 20
Data Height: 20
Primary Control:
Previous Control:
Separator: □ Use Space
Standard Edit: ORI_CODE: Originating Agency Code
Slm Edit:
Help: ORI: ORIGINATING AGENCY IDENTIFIER
Menu: CON_POP: Control Pop-up Menu
Preload: $DEV(ORI)
Populate Related Fields:
Mask Character:
□ Multi-line
☑ Entry Required
□ Modify-to-Delete Allowed
□ Read Only
□ Lock
Summary Order:
Label Font Name:
Label Font Size:
Control Font Name:
Control Font Size:
Padding Character:
Background Text:
Vertical Text: No
Rotate Angle: 90

The Omni*xx* Enterprise Message Log Viewer provides the ability to search logged messages by any combination of the search fields. These include source and destination credentials, ORI, specific fields and free text.

The screen shot below depicts the search fields available in the OEP Log Viewer. Multiple field combinations are supported as well as multiple items within a search field by separating them with a comma. For example, entering "QW,QB,QA" in the MKE search field will return records where the MKE equal QW and QB and QA. The same technique applies to the other search fields allow multiple values in each field, and multiple fields simultaneously.

The Date and Time search fields can be used to further restrict the date range of the search and free text searches can be entered into the Summary field to include searching the message summary field, and they payload of the message text by selecting the "Include message detail when searching message summary" checkbox. Results may also be ordered by selecting the Asc or Dsc radio options for ascending or descending order.



Omnixx Enterprise Platform Message Log Viewer

Begin Date	09/10/2015	End Date	09/10/2015	Interface	All
Begin Time	00:00:00	End Time	23:59:59	Application	All
User		ORI		Event Type	All
Subagency		Device		Address	
MKE		Reference ID		Sequence #	

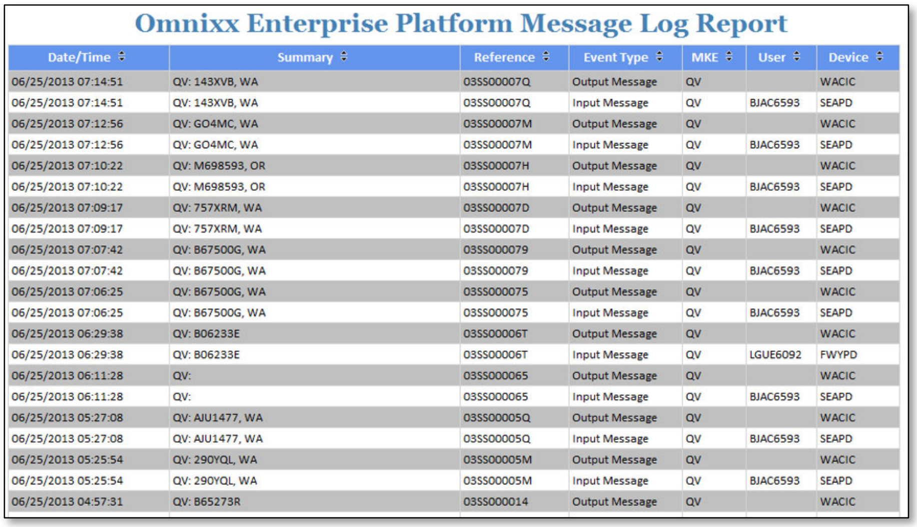
Summary □ Include message detail when searching summary?

Order By Date/Time ○ Asc ● Dsc | Database Current Audit Database □ Do not include page count

Omni*xx* Enterprise Message Log Viewer

The OEP Log Viewer supports complex search criteria using multiple combinations of Boolean operators including the AND & OR operators. Selecting the "…" button () next to the Summary field will display an interface enabling the operator to construct search criteria including AND & OR operators in multiple combinations.

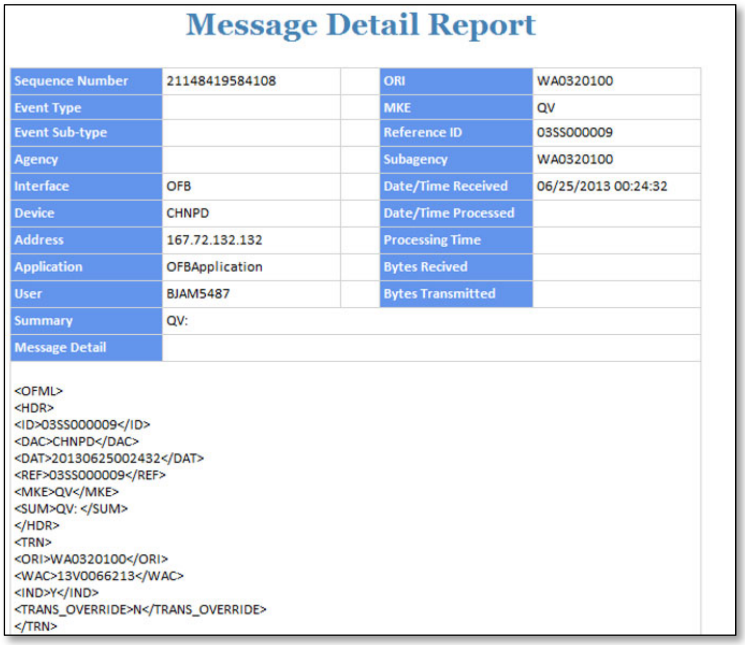
The Message Log Summary Report is accessed by clicking the "Summary Report" button.



Omnixx Enterprise Platform Message Log Report

Date/Time ⇕	Summary ⇕	Reference ⇕	Event Type ⇕	MKE ⇕	User ⇕	Device ⇕
06/25/2013 07:14:51	QV: 143XVB, WA	03SS00007Q	Output Message	QV		WACIC
06/25/2013 07:14:51	QV: 143XVB, WA	03SS00007Q	Input Message	QV	BJAC6593	SEAPD
06/25/2013 07:12:56	QV: GO4MC, WA	03SS00007M	Output Message	QV		WACIC
06/25/2013 07:12:56	QV: GO4MC, WA	03SS00007M	Input Message	QV	BJAC6593	SEAPD
06/25/2013 07:10:22	QV: M698593, OR	03SS00007H	Output Message	QV		WACIC
06/25/2013 07:10:22	QV: M698593, OR	03SS00007H	Input Message	QV	BJAC6593	SEAPD
06/25/2013 07:09:17	QV: 757XRM, WA	03SS00007D	Output Message	QV		WACIC
06/25/2013 07:09:17	QV: 757XRM, WA	03SS00007D	Input Message	QV	BJAC6593	SEAPD
06/25/2013 07:07:42	QV: B67500G, WA	03SS000079	Output Message	QV		WACIC
06/25/2013 07:07:42	QV: B67500G, WA	03SS000079	Input Message	QV	BJAC6593	SEAPD
06/25/2013 07:06:25	QV: B67500G, WA	03SS000075	Output Message	QV		WACIC
06/25/2013 07:06:25	QV: B67500G, WA	03SS000075	Input Message	QV	BJAC6593	SEAPD
06/25/2013 06:29:38	QV: B06233E	03SS00006T	Output Message	QV		WACIC
06/25/2013 06:29:38	QV: B06233E	03SS00006T	Input Message	QV	LGUE6092	FWYPD
06/25/2013 06:11:28	QV:	03SS000065	Output Message	QV		WACIC
06/25/2013 06:11:28	QV:	03SS000065	Input Message	QV	BJAC6593	SEAPD
06/25/2013 05:27:08	QV: AJU1477, WA	03SS00005Q	Output Message	QV		WACIC
06/25/2013 05:27:08	QV: AJU1477, WA	03SS00005Q	Input Message	QV	BJAC6593	SEAPD
06/25/2013 05:25:54	QV: 290YQL, WA	03SS00005M	Output Message	QV		WACIC
06/25/2013 05:25:54	QV: 290YQL, WA	03SS00005M	Input Message	QV	BJAC6593	SEAPD
06/25/2013 04:57:31	QV: B65273R	03SS000014	Output Message	QV		WACIC

The Message Log Detail Report is accessed by clicking the "Detail Report" button.



Message Detail Report

Sequence Number	21148419584108	ORI	WA0320100
Event Type		MKE	QV
Event Sub-type		Reference ID	03SS000009
Agency		Subagency	WA0320100
Interface	OFB	Date/Time Received	06/25/2013 00:24:32
Device	CHNPD	Date/Time Processed	
Address	167.72.132.132	Processing Time	
Application	OFBApplication	Bytes Recived	
User	BJAM5487	Bytes Transmitted	
Summary	QV:		
Message Detail			

```
<OFML>
<HDR>
<ID>03SS000009</ID>
<DAC>CHNPD</DAC>
<DAT>20130625002432</DAT>
<REF>03SS000009</REF>
<MKE>QV</MKE>
<SUM>QV: </SUM>
</HDR>
<TRN>
<ORI>WA0320100</ORI>
<WAC>13V0066213</WAC>
<IND>Y</IND>
<TRANS_OVERRIDE>N</TRANS_OVERRIDE>
</TRN>
```

The Omnixx Enterprise Platform provides standard reports that can be accessed by authorized administrators.

C. Proposed Project Management Plan

The bidder should submit a high-level project management plan which clearly identifies the work to be completed during the message switch implementation. This plan must include project tasks, deliverables, milestones, and associated dependencies. It shall also address risk management, deficiency management, and project change management processes.

Datamaxx Response: Please see *Appendix A* for the high-level project management plan.

D. Proposed Schedule

The bidder must submit a high-level schedule summary minimally representing the major milestones and contract deliverables associated with the Implementation Plan.

Datamaxx Response: Please see *Appendix B* for the detailed draft schedule.

E. Security Response

Bidders should provide a narrative of their overall approach to security. Security Proposal must demonstrate both a full comprehension of the security requirements throughout this RFP and associate requirements and plan attachment(s) and the intention to comply with these requirements. The Security Response must indicate how the bidder will comply with all personnel, physical, and technical requirements of the solicitation.

The bidder should describe its management structure and procedures for protecting NSP and state data, information, materials, equipment, and facilities to which prime and subcontractor personnel may have access. The bidder must describe the bidder's security organization, showing lines of communication to corporate management and explaining why this organization is appropriate for the project.

The bidder should describe the pre-screening procedures to be used prior to submitting potential employee candidates for facility and/or information access approvals and subsequent NSP background screening

Datamaxx Response: The Datamaxx Secure Cloud meets all security requirements as required under the FBI CJIS Security Policy as well as the Nlets Security Policy. Datamaxx undergoes an Nlets audit on a biannual basis. This audit covers various layers of security, including implementation best practices in terms of system design and configuration as well as social engineering, personnel vetting and all around facility security with regard to physical access.

Every Datamaxx employee undergoes and must pass a national fingerprint based background check. Additionally, our personnel are required to secure a certificate for Security Awareness Training. This training and certification extends to NCIC Certified Operator training as well for certain staff. All of which are done on a biannual basis.

The Datamaxx Secure Cloud is located in the Datamaxx headquarters in Tallahassee, Florida. This facility employs proximity badge readers for access to all exterior doors as well as certain interior doors, based on a particular area. Visitors and/or contractors are not allowed unescorted access to any area of the building.

F. Implementation Plan Response

Attachment A to this RFP contains the MSS Implementation Plan. The bidder must describe its understanding of the NSP’s requirements as expressed in the MSS Implementation Plan and its approach to satisfying those requirements. The bidder must address methodology and tools, assumptions, risks, applicable standards, deliverables, and deliverable content. The response to the MSS Implementation Plan should minimally include:

i. *Approach for the Development of Each Plan Deliverable* – The bidder must provide a textual description of their approach to conducting the activities and developing the deliverables associated with the Implementation Plan. For each task, the bidder must provide proposed activities, deliverables, descriptions of deliverable content, and methods and tools to be used, if the bidder recommends any additional deliverables, they should also be discussed here.

Datamaxx Response: The Datamaxx Implementation Plan is in line with NSP Implementation Plan found in Attachment A. In this regard the plan will have a primary end goal achieved via iterative deliverables and milestones.

Datamaxx will assign a dedicated Project Manager that will develop and manage a schedule using Microsoft Project. The schedule will track all deliverables, activities, resources and predecessors. Additionally, any dependencies, review periods, test cycles, remediation cycles, etc. This schedule will be an IMS and a Work Breakdown structure will be used as required for any sub task/project initiatives.

The communications plan will include a direct line between the Datamaxx Project Manager and the NSP Project Manager. Both Project Managers will be responsible for bringing in and rolling out of the project the relative subject matter experts and/or resources associated with a particular area of the project. All meetings will result in written meeting minutes with monthly status reports being distributed across the key personnel and stakeholders. All document distributed as a result of the project will be in electronic format, specifically email.

All requirements will be documented in a Requirements Traceability Matrix, wherein all parties agree on the requirements that will be implemented in the solution and will be subject to acceptance testing. This is line with the state’s requirement for an SRR and ultimately an SDR.

Any changes in the scope of the project that either introduce or omit a feature, function and/or requirement will be captured in a Change Request (CR). The CR will be developed by the respective Project Manager. All parties will agree to the CR by signing the document. Should it be necessary to capture any cost adjustment as the result of the CR a contract modification or purchase order would be issued by the state.

The majority of deliverables are part of a COTS solution. With that in mind, Datamaxx will provide test script results. This includes a Factory Test routine. Following such, the remaining testing that will occur will account for all nuances relative to a state's particular configuration and/or custom components. All testing will close out following an acceptance test period that brings the COTS, custom configurations and any custom components together as comprehensive solution.

ii. *Detailed Schedule* – A detailed Gantt-chart resource (staff) loaded Schedule in Gantt-chart form. The Integrated Master Schedule (IMS) must include, at a minimum, all activities required by the MSS Implementation Plan, including Management and Technical Reviews. The Schedule should identify any schedule margin/reserve. The Schedule must provide sufficient detail to demonstrate confidence that the proposed schedule is complete and realistic. There is no minimum degree of detail required.

Datamaxx Response: Please see *Appendix B* for the detailed draft schedule.

G. Operations Plan Response

Attachment B to this RFP contains the MSS Operations Plan. The bidder should describe its understanding of the NSP's requirements as expressed in the MSS Operations Plan and its approach to satisfying those requirements. The bidder must address methodology and tools, assumptions, risks, applicable standards, deliverables, and deliverable content. The bidder should provide a textual description of their approach accomplishing the work in the Operations Plan. For each task, the bidder should provide proposed activities, deliverables, descriptions of deliverable content, and methods and tools to be used. If the bidder recommends any additional items, they should also be discussed here. Minimally, the bidders response should address the following topics as introduced in the Operations Plan:

i. *System Interfaces. The bidder should identify applicable interface standards and discuss any limitations in its implementation of those standards, interface capacities (average and peak hour), as well as any assumptions, risks, or constraints.*

Datamaxx Response: The system interfaces use industry standard communications protocols and techniques. Note that the actual performance and potential throughput is dictated by the data source, and is not a function of the interface. Thus the capacities are presented as the potential that can be achieved from the perspective of the Message Switch.

A general assumption is that the data sources are available at all times, which is outside the control of the Message switch, unless noted. Error handling is provided where applicable, that will notify a user that the data source is not available.

Note that the NCIC CCH and NCIC NICS interfaces will convert to Web Services and NIEM when they will become available from NCIC. OFML is an XML implementation designed specifically for efficient data exchanges. DMPP-2020

The following is the table of interfaces.

Standard	Interface	Data Format	Peak Capacity	Constraints
Web Service, http	NSP PCH	XML for PCH	5 Msgs/Sec	
Web Service, https	DMV VTR	OFML	10 Msgs/Sec	SSL Certificates that expire must be maintained
Web Service, http	DMV DL/PRO	String for OCIO	10 Msgs/Sec	
Web Service, https	DMV DL Photo	XML/SOAP	5 Msgs/Sec	SSL Certificates that expire must be maintained
Web Service, http	NLETS	NLETS NIEM/GJXDM	8 Msgs/Sec	
Web Service, https	NCIC Hot Files	NCIC NIEM	10 Msgs/Sec	SSL Certificates that expire must be maintained
TCP Sockets	NCIC CCH	NCIC String	10 Msgs/Sec	Will convert to Https/NIEM. SSL Certificates that expire must be maintained
TCP Socket	NCIC NICS	NCIC String	5 Msgs/Sec	Will convert to Https/NIEM. SSL Certificates that expire must be maintained
DMPP-2020	NSP Hot Files	OFML	8 Msgs/Sec	Integrated with the Message Switch
DMPP-2020	NSP Batch Inputs	OFML	8 Msgs/Sec	Data inputs are provided by external systems
Web Sockets	Omnixx Force Clients	OFML	10 Msgs/Sec	
DMPP-2020	Remote systems	OFML	10 Msgs/Sec	Data inputs are provided by external systems
DMPP-2020	NSP Weather Process	OFML	2 Msgs/Sec	

The aggregate throughput capability of all interfaces on the Message Switch is upwards of 40 Msgs/second, averaged over several minutes. Normal operation on the current system is approximately 5 – 7 Msgs/second, depending on time of day and user activity.

ii. *Report Generation. The bidder should describe how authorized personnel will access and inspect the MSS. The bidder should describe the logging mechanism and how these are available to authorized personnel. Logs should inform of who accessed and who hanged what information.*

Datamaxx Response: **Report Generation**

Omnixx Force
&
Microsoft
SQL Server
Reporting Services

The Omni*xx* Enterprise Platform integrates with Microsoft SQL Server Reporting Services (SSRS), which provides a set of tools and services to create, deploy, export, schedule, and manage reports.

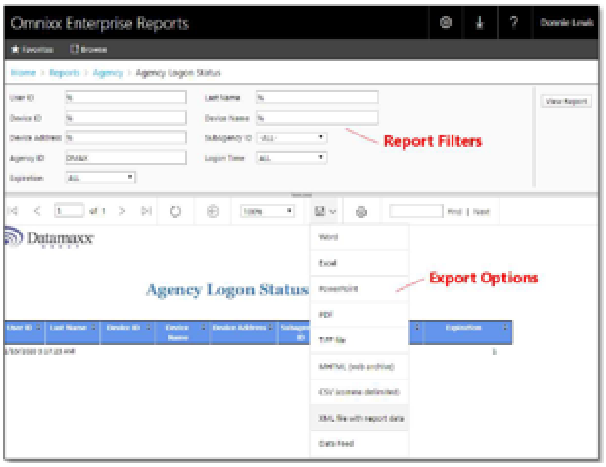
The Omni*xx* Enterprise Platform provides 36 standard reports as part of the solution (listed below) and there are several of tools available for creating custom reports for SSRS, including the SQL Server Report Builder and Visual Studio Code.

Datamaxx provides an entity relationship diagram as well as predefined data sets and views enabling custom reports to be added by anyone familiar with SQL Server Reports.

Reports are accessed from the Reports tab, and the list of available reports that are available to a user are controlled by a users' role, controlled by administrators, and provide the flexibility to deliver the right information to the right user.

The reports provide a variety of filters for ad-hoc reporting as well as the ability to schedule reports for delivery.

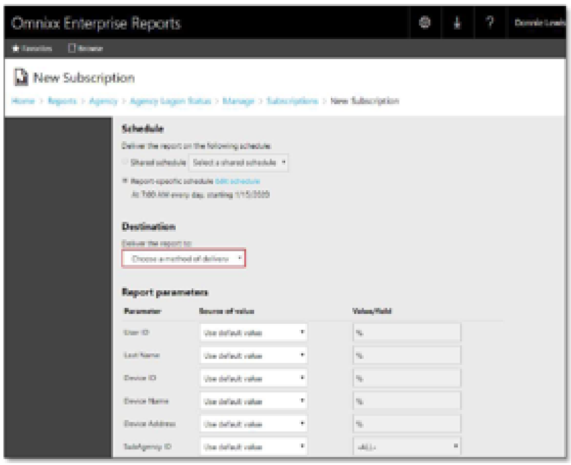
This provides fine-grained control over who can access a report and which reports an administrator authorizes the user to access.



User ID: %
Last Name: %
Device ID: %
Device Name: %
Device Address: %
Subagency ID: -ALL-
Agency ID: DMAX
Logon Time: ALL
Expiration: ALL

Agency Logon Status

User ID	Last Name	Device ID	Device Name	Device Address	Subagency ID		Expiration
1/3/2020 3:17:23 AM							1


Omnixx Enterprise Reports
Donnie Lewis
Favorites
Browse
Home > Reports > Agency > Agency Logon Status > Manage > Subscriptions > New Subscription
Edit schedule

New Subscription

Schedule

Deliver the report on the following schedule:

○ Shared schedule Select a shared schedule

● Report-specific schedule

At 7:00 AM every day, starting 1/15/2020

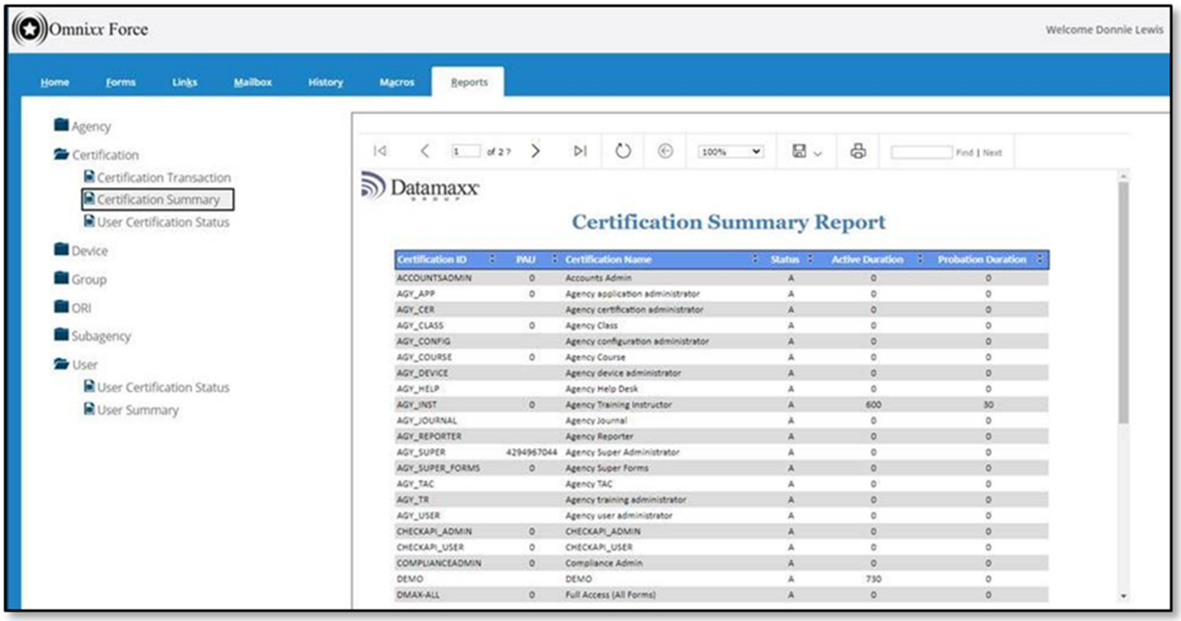
Destination

Deliver the report to:

Choose a method of delivery

Report parameters

Parameter	Source of value	Value/Field
User ID	Use default value	%
Last Name	Use default value	%
Device ID	Use default value	%
Device Name	Use default value	%
Device Address	Use default value	%
SubAgency ID	Use default value	-ALL-



Certification Summary Report

Certification ID	PAU	Certification Name	Status	Active Duration	Probation Duration
ACCOUNTSADMIN	0	Accounts Admin	A	0	0
AGY_APP	0	Agency application administrator	A	0	0
AGY_CER		Agency certification administrator	A	0	0
AGY_CLASS	0	Agency Class	A	0	0
AGY_CONFIG		Agency configuration administrator	A	0	0
AGY_COURSE	0	Agency Course	A	0	0
AGY_DEVICE		Agency device administrator	A	0	0
AGY_HELP		Agency Help Desk	A	0	0
AGY_INST	0	Agency Training Instructor	A	600	30
AGY_JOURNAL		Agency Journal	A	0	0
AGY_REPORTER		Agency Reporter	A	0	0
AGY_SUPER	4294967044	Agency Super Administrator	A	0	0
AGY_SUPER_FORMS	0	Agency Super Forms	A	0	0
AGY_TAC		Agency TAC	A	0	0
AGY_TR		Agency training administrator	A	0	0
AGY_USER		Agency user administrator	A	0	0
CHECKAPI_ADMIN	0	CHECKAPI_ADMIN	A	0	0
CHECKAPI_USER	0	CHECKAPI_USER	A	0	0
COMPLIANCEADMIN	0	Compliance Admin	A	0	0
DEMO		DEMO	A	730	0
DMAX-ALL	0	Full Access (All Forms)	A	0	0

Report Name	Description
Agency Maintenance Report	Provides details related to record maintenance for agency record(s).
Agency Use	This report summarizes the number of each MKE sent by each user, client device and/or ORI.
Certification Maintenance Report	Provides details related to record maintenance for certification record(s).
Certification Summary	Provides a summary of Certification records.
Certification Transaction	Provides a list of which transactions are authorized by each certification.
Client-Switch Interface Summary	Provides a summary of Client Switch Interface records.
Device Detail	Provides detail information for a specific Device record.
Device Maintenance Report	Provides details related to record maintenance for device record(s).
Device Summary	Provides a summary of Device records.
Group Membership	Provides a list of members for Group records.

Report Name	Description
Group Membership	Provides a list of members for Transaction Group records.
Group Summary	Provides a summary of Group records.
Hourly Distribution	This report summarizes the number of inputs, output and total bytes, and input, output and total messages sent and received over each interface by hour of day.
Interface Maintenance	This report summarizes when each interface was started or stopped.
Logon History Report	Provides a list on the history of user logons.
Logon Status Report	Provides a list on the current status of user logons.
Message Log Summary & Detail Reports	These provide summary and detail reports for the search results based upon the criteria entered for the search.
MKE By Device	This report summarizes the number of each MKE sent by each client device.
MKE By ORI	This report summarizes the number of each MKE sent by each ORI.
MKE By Switch-Host Interface	This report summarizes the number of each MKE sent to host interfaces such as NCIC, Nlets and DMV.
MKE By User	This report summarizes the number of each MKE sent by each user.
Omni*xx* Host Switch Summary	Provides a summary of Host Switch records.
Omni*xx* Switch Summary	Provides a summary of Omni*xx* Switch records.
ORI Summary	Provides a summary of ORI records.
Subagency Detail	Provides detail information for a specific Subagency record.
Subagency Maintenance Report	Provides details related to record maintenance for Subagency record(s).
Subagency Summary	Provides a summary of Subagency records.
Switch Host Interface Summary	Provides a summary of Host Interface records.
Transaction Group Summary	Provides a summary of Transaction Group records.
User Certification Maintenance Report	Provides details related to record maintenance for user certification record(s).
User Certification Status	Provides a list on the status of user certifications.
User Certification Status	Provides a list on the status of user certifications.
User Detail	Provides detail information for a specific User record.
User Maintenance Report	Provides details related to record maintenance for user record(s).
User Summary	Provides a summary of User records.

iii. *Support Services. The bidder should describe the approach to identifying, responding to, resolving and tracking problems. The bidder should identify which support services are to be performed on-site and which will be remote. The bidder should describe how configuration management will be provided.*

Datamaxx Response: The Datamaxx Technical Support team of professionals provides 24X7X365 support to our client base. Support is provided via a dedicated toll free number as well as via email for non-urgent calls for service. Datamaxx uses the Salesforce application to log and track support cases. In the event a client reported issue has not been resolved during the initial call for assistance, the case enters an escalation process. The initial step is to assign the issue to an appropriate category. Datamaxx will respond to and correct errors, defects, and malfunctions, in accordance with the following schedule.

CATEGORY	SEVERITY
1	A defect causing crashes of the system, the irrevocable loss or corruption of data, or the loss of a mission critical system or software functionality. No documented work-around is practicable.
2	A defect causing crashes of the system, the irrevocable loss or corruption of data, or the loss of a mission critical system or software functionality. A documented work-around is practicable.
3	A defect causing the recoverable loss or corruption of data, or the loss of system or software functionality that is not mission-critical.
4	A defect that does not materially affect the operation of the system, such as minor imperfections to the user interface or items that function properly but do not meet client requirements.
5	There is no defect; however, the Customer may request a change to the subject item through the Enhancement Request Process.

Depending upon the cloud environment the state chooses support services can be provided in either a remote or onsite capacity. For example, should the Datamaxx Secure Cloud be utilized then all support services would be provided onsite, by the respective Datamaxx personnel. Should the state pursue a third party cloud (MS Azure), all support services will be provided in a remote capacity.

Despite being remote and/or onsite the approach to identifying, responding to, resolving and tracking problems is identical.

iv. *Customer Support. The bidder should describe the proposed Customer Support services. The bidder should identify what is automated or has automation support, what kind of automation support is proposed, what support priorities are and what the Support Service Level Agreements (SLAs) are.*

Datamaxx Response: As indicated above, the Datamaxx Technical Support professionals receive calls for service either via email for non-urgent matters or through a toll free number. A case number is assigned from the salesforce application to all emails received.

Responses are sent back to the email indicated the case number for all future communications on the matter. All incoming calls will receive a case number at the time the case is opened. The Omni*xx* system will allow users and/or TACS to manage user related issues, such as password resets, etc.

In addition to traditional support wherein a user makes a request for service, the Datamaxx Secure Cloud implementations are all deployed with monitoring tools that offer automated support functions. These include such things as measuring the health and wellness of the system, measure response against each interface, etc. Should any monitored event result in abnormal response, Datamaxx technicians receive notifications immediately so they can investigate and resolve the issue.

The Service Level Agreement provides for the following: System Management: Operating System, SQL Server, Patch Management, Anti-Virus; COTS Software Management – applying upgrades, hot fixes, patches, etc. Monthly reports will be distributed that summarize all calls for service and the respective status. Should an issue not be resolved during the initial call for service, and escalation process will deployed. Prior to the escalation process, a category will be determined for the case based on the following table.

CATEGORY	SEVERITY
1	A defect causing crashes of the system, the irrevocable loss or corruption of data, or the loss of a mission critical system or software functionality. No documented work-around is practicable.
2	A defect causing crashes of the system, the irrevocable loss or corruption of data, or the loss of a mission critical system or software functionality. A documented work-around is practicable.
3	A defect causing the recoverable loss or corruption of data, or the loss of system or software functionality that is not mission-critical.
4	A defect that does not materially affect the operation of the system, such as minor imperfections to the user interface or items that function properly but do not meet client requirements.
5	There is no defect; however, the Customer may request a change to the subject item through the Enhancement Request Process.

DATAMAXX will make an initial response to a Category 1 call within a maximum time-period of one hour after receipt. Datamaxx will use extraordinary efforts to provide a fix, work around, or patch to Category 1 bugs within four (4) hours after the bug has been replicated and confirmed by DATAMAXX. Category 1 calls will be handled on a 24x7x365 basis.

DATAMAXX will make an initial response to a Category 2 call within a maximum time-period of one hour after receipt. DATAMAXX will provide a fix, work around, or patch to Category 2 bugs within twenty-four (24) hours after the bug has been replicated and confirmed by DATAMAXX. Category 2 calls will be handled on a 24x7x365 basis.

DATAMAXX will make an initial response to a Category 3 call (phone or email) within a maximum time-period of four hours after receipt. DATAMAXX will make reasonable efforts to identify a resolution to Category 3 calls within thirty (30) days and to incorporate Category 3 fixes in the next upcoming release of the product.

DATAMAXX will make an initial response to a Category 4 call (phone or email) within a maximum time period of four hours after receipt. Category 4 calls will be handled on a case-by-case basis.

DATAMAXX will make an initial response to a Category 5 call (phone or email) within a maximum time period of twenty-four hours after receipt. Category 5 calls will be handled on a case-by-case basis.

DATAMAXX will make an initial response to a Category 6 call (phone or email) within a maximum time period of thirty six hours after receipt. Category 6 calls will be handled on a case-by-case basis.

In the event that a resolution cannot be established for a failure during the troubleshooting process, DATAMAXX will provide a workaround for any critical error in an effort to ensure minimal downtime for the affected agency. This workaround shall be considered “temporary” until a permanent resolution can be distributed.

v. *Training. The bidder should describe the proposed approach to training and to ensure that all applicable users and bidder staff are sufficiently trained and stay current.*

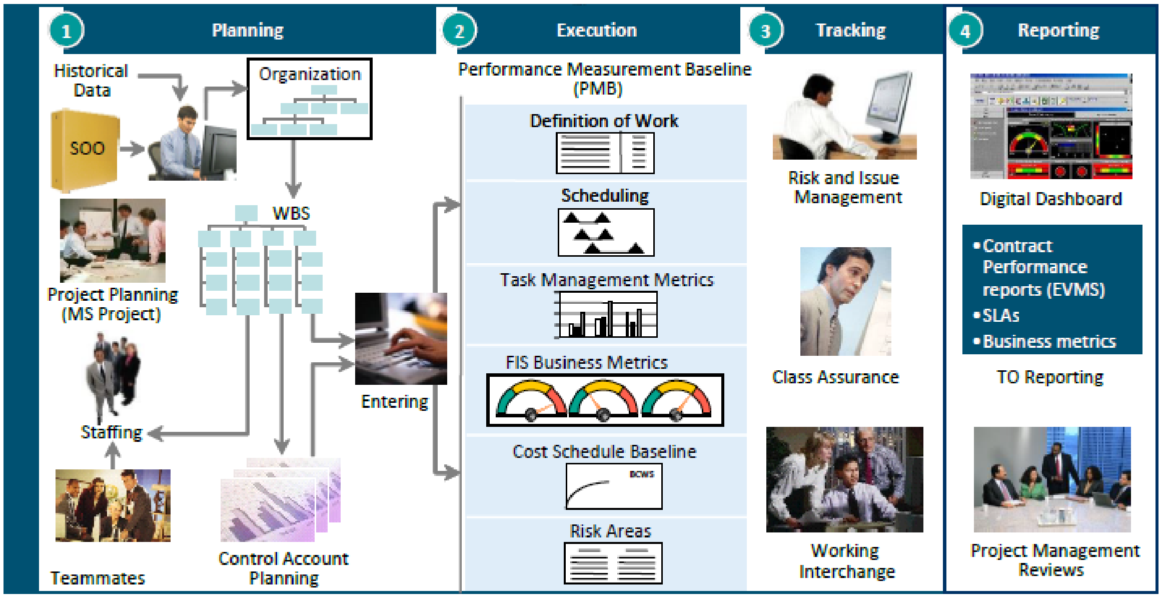
Datamaxx Response: Datamaxx offers a variety of training solutions that are delivered in a variety of configurations: e.g. web-based training; live in-person training; and pre-recorded training sessions. Training curriculum is designed for a variety of user types, including Train-the-Trainer; System Administrator Training; and End-User Training. Additionally, as part of the Datamaxx Secure Cloud services, Datamaxx customers can go to our web page to access the “Datamaxx Academy.” This academy offers monthly “Take 30” training webinars which cover numerous topics. Datamaxx customers can schedule “Take 30” web-classes at their leisure and with no additional cost.

vi. *Program Organization. The bidder should describe the proposed Program Management Office (PMO). The bidder should discuss how the proposed PMO (including subcontractors and vendors) is organized (an organizational chart should be included); how it fits into the* *bidder's overall corporate structure (an organization chart should be included); how the proposed PMO will interface with the NSP; and what the responsibilities are for key persons. The bidder should identify and discuss the principal interfaces and reporting mechanisms internal to and external to the PMO as well as elements of the bidder's support organization.*

Datamaxx Response: Datamaxx utilizes a modified "Strong Matrix Organization" structure as defined by the Project Management Body of Knowledge (PMBOK). This was derived from the Project Management Institute (PMI) designed to deliver projects on time, on budget, and with the desired results. This is coupled with deep experience integrating PMI with multiple life cycle framework and CMMI methods to insure successful delivery.

The Program Management approach begins with a robust Project Management Plan (PMP). The PMP incorporates proven best practices and procedures that are measurable, attainable, focused on quality, and cost savings. It provides the essential foundation to reduce program risk, provide critical visibility to stakeholders, generate control tools for managers, and produce steady, meaningful reporting results to the client. In addition, the PMP incorporates the lessons learned from past achievements and previous challenges, and provides best practices that continue to comprise a core part of our overall methodology. Our Project Manager follows the PMP, it serves as an operating manual helping to drive high quality, standardized, repeatable processes across tasks; enforce compliance with client guidelines, policies, and regulations; and reduce costs and establish successful partnership.

Our comprehensive management approach (see figure below) depicts the quality process for all program products and services and that we have maximum management and control of task milestones, schedules, cost, budget, risks, and deliverables. The six main operating principles of our management approach are: 1) we will work within the contract to always accomplish the mission; 2) customer satisfaction is paramount; 3) we will establish clear lines of accountability, authority, and communication; 4) risk management is essential and will be established at the programmatic, technical, and organizational level; and 5) process improvement is core to all processes.



Project Management Approach: Integrates all project aspects including technical, schedule cost, quality, personnel, risk, and communication management.

vii. *Management and Technical Reporting and Reviews. The bidder should identify proposed reviews, their purpose, frequency, participates, and any associated deliverables. The bidder should acknowledge the reviews required in the Operations Plan. All reports should be enumerated, their contents described, the frequency of reporting described, and the recipients (organizations) of the reports specified.*

Datamaxx Response: Datamaxx Project Manager will hold weekly meetings to discuss current project status including accomplishments, week ahead, potential risk, etc. The participants of the weekly meetings will include the Datamaxx key personnel relative to the current portion of the project as well as respective state personnel. These weekly meetings will end in the production and publication of a written set of minutes capturing the salient points of the meeting. These meetings will be held in a conference call environment allowing for participation regardless of location.

In addition to the weekly meetings, a series of Operational Program Management Reviews (OPMRs) will begin 60 days following acceptance and continue on a semi-annual basis. These meetings will cover the overall system performance including not only technical functionality, but also service level objectives, etc. Datamaxx will work cooperatively with the state to develop an agenda that includes but is not limited to the following:

1. Performance against Service Level Agreements (SLAs).
2. Financial and schedule status.
3. Planned activities.
4. Action item status.
5. Problem report status.
6. Configuration management and quality assurance reporting.

7. Issues and risks.
8. Other service level shortfalls and plans for corrective action.

These meetings will end with the publication of meeting minutes.

viii. *Facility Personnel. The bidder should describe the proposed staffing roster for the Primary Site and the COOP Site. The bidder should show how staffing would be redeployed in case the COOP Site needs to take over. All staffing roles should be identified, with an indication of the responsibilities and reporting requirements for each role. The bidder should indicate security measures that will be in place in respect to the bidder's proposed facility personnel.*

Datamaxx Response: The Datamaxx Secure Cloud will have the following roles assigned to a cloud implementation. All facility personnel have undergone a nationwide fingerprint based background check; achieved certification for both CJIS Security Awareness and NCIC Operator. Access to all cloud related implementations is based on a multi factor configuration that includes proximity badge readers, user and password login, as well as a PIN.

Facility personnel would not necessarily be deployed to the COOP site unless required. However, the COOP site has all infrastructure personnel readily available performing all system and infrastructure support and services. Datamaxx facility personnel will be remotely managing the application side of the solution.

Role	Responsibility	Reporting Requirements
Cloud Support Team	Oversee day to day operations. Answer, resolve and log calls for service, etc.	Supervisor, Technical Support
Field Engineer/System Administrator	Apply Omni*xx* updates, testing releases, escalated support issues, configurations	Manager, Field Engineering & Support
Cloud Administrator	System updates: Windows, SQL, Anti-Virus. Oversees all auditing and security routines.	Director, Cloud & IT Services

ix. *System Security. The bidder should describe the approach to establishing the managing system security over time. The bidder should explain and provide for ongoing compliance with NSP's security requirements.*

Datamaxx Response: The Datamaxx Secure Cloud undergoes constant review to insure that all best practices in managing overall system security are employed. Datamaxx conducts self-assessments on a quarterly basis, including ethical hacking scenarios. All security patches are kept current with release publications and during the regular Nlets audits, all security requirements are reviewed for compliance. Datamaxx will review the NSP security requirements on a quarterly basis to confirm compliance. Should it be necessary to review and/or discuss specific NSP security requirements, such discussions will be conducted during the OPMRs.

x. *System Maintenance. The bidder should show how the system is maintained over time. Maintenance is applicable to all software, hardware, services, inputs and interfaces that are required to operate the MSS. Maintenance includes regression testing and issue resolution after a change. The bidder should describe the approach to periodic maintenance reviews, the required hardware refreshes, system software updates and feature upgrades. The bidder should describe the approach to minimize downtime during scheduled and unscheduled maintenance.*

Datamaxx Response: The Datamaxx Secure Cloud adheres to a policy and procedures manual that outlines the manner in which all aspects of the cloud are maintained, including software, hardware, services, inputs and interfaces, etc. As previously stated, all third party applications, such as MS Windows Server, SQL and Norton Anti-Virus are subject to the manufacturer's release schedule. The Datamaxx release schedule is as follows: Major releases are available on an annual basis with service packs typically issued quarterly and/or hot fixes released as needed. Minimizing downtime during maintenance, whether scheduled or unscheduled is achieved by deploying a system that allows for a clustered environment as well as any pre-staging events that can occur prior to the maintenance window. All releases are placed into the respective test system first, qualified that no issues are introduced; any issue resolutions and/or enhancements are correct and then at a scheduled time are promoted to production.

xi. *Response Time Management. The bidder should describe the approach to monitoring and managing system response performance.*

Datamaxx Response: The Datamaxx Secure Cloud has several levels of monitoring that occur in order to manage overall system performance. With regard to response times, there is a particular application that Datamaxx deploys wherein a message is sent to each interface, and for any response times that exceed 1 minute, alerts are sent out to the respective team.

xii. *Correction of Deficiencies. The bidder should describe in detail how deficiencies are identified, categorized and triaged for resolution. The bidder should explain how the NSP is informed of the status of a deficiency log and which personnel is involved how in decision-making, depending on the priority of deficiencies.*

Datamaxx Response: Datamaxx team members, representing various groups within the organization meet twice per week to review deficiencies and/or enhancements in order to categorize and ultimately publish a release to address the issue. In the case of an urgent matter, a meeting is immediately convened so a hot fix and/or workaround can be established to address the issue. If the system is still in a project state, the Datamaxx Project Manager will communicate to the NSP Project Manager on details surrounding the issue. If the system is in a fully operational state, issues will funnel through the

Datamaxx Technical Support team, who will spearhead the matter internally using the same process as outlined above.

xiii. *Configuration Management. The bidder should describe the approach to configuration management across three separate environments per site. The bidder should describe the approach to automated deployment between environments as well as ensuring that the Primary Site and the COOP site are kept in synch. The bidder should describe how the NSP will be kept informed and what decision-making may be needed to maintain effective configuration management.*

Datamaxx Response: The Datamaxx approach to configuration management is based on four key elements: Identification, Baseline, Version Control and Auditing. Once the systems are promoted to a production state, an initial baseline will be established and all systems will be in synch with regard to version control.

Following initial promotion to production all systems will enter a maintenance period in which the configuration management approach will apply. Items/issues are identified through various means, including communication with clients; enhancements dictated by the market; etc. When a release becomes available, whether it is a major release or a hot fix, it is assigned a unique version number. All releases are first deployed in the test environment. Once the test system has been qualified to insure the release provided the expected result and didn't introduce any new concerns, an updated schedule for the remaining environments will be developed. Following the update of all environments an audit will occur to insure that all systems are again at a specific baseline and ultimately in synch with one another.

xiv. *COOP. The bidder should describe the COOP services proposed within the provisions of the Operations Plan.*

Datamaxx Response: Datamaxx will provide a COOP plan following contract award. While the state can declare a disaster, the contractor must do so within 2 hours of an event causing disruption of services, otherwise the disruption is considered unplanned. The provisions of the COOP plan will include the following:

1. The contractor responsibility for restoration of the solution.

2. The contractor shall be required to maintain regular and consistent communication with the state about the outage and steps taken to restore the solution.

3. The contractor shall be required to make a declaration of a disaster and invoke the Disaster Recovery Plan immediately.

4. The contractor shall restore the system data to a point no greater than 24 hours prior to the declaration of the disaster by the state or the contractor.

5. The state shall be able to log on to the disaster recovery site upon declaration of the disaster by the state or the contractor.

To ensure the COOP services are readily available when needed, routine testing of invoking these services will be performed. A schedule to perform such will be cooperatively determined by the contractor and the state.

H. Technical Requirements Response

Attachment C to this RFP contains the MSS Requirements Specifications, including the technical requirements. Response instructions are included within the attachment. Responses are required for each specification entry in Attachment C. an omitted response will be assumed to be same as a response of "not available."

Datamaxx Response: Datamaxx provides responses to the MSS Requirements in *Attachment C* under separate cover.