

RMS Attachment 3 - System Requirements Niche Technology

Note: This RMS Attachment 3, System Requirements provides the response provided as part of the Contractor's technical proposal for the New York State Police Records Management System project used as the benchmark to establish this Aggregate Agreement. The Contractor, Niche Technology Inc, and the Products offered under this Aggregate Agreement are required to adhere to the functionality contained in this response. An Authorized User should review the functionality described by the Contractor in this Attachment and should use this information as a baseline for the Statement of Work. Authorized Users should also determine if any changes are necessary to meet the specific project requirements when working with the Contractor to develop the Authorized User Agreement. Please see Attachment D, How to Use the Aggregate Agreement 18-02, for additional information when working with the Contractor to develop the Authorized User Agreement.

Contractor's Name: Niche Technology Inc.

Requirement Type: System Requirements

Instructions:

- The following requirements are mandatory (M) requirements. If a Contractor is unable to provide a feature identified as mandatory the proposal will not be further considered.
- For each requirement contained within this document a response is required even if the response is indicating the functionality is not offered
- For requirement T1,T2,T3 check the appropriate box:
 - **Offered** – this requirement is currently available
 - **Not Offered** – the feature is neither currently available nor can it be configured.
- Where indicated, responses to certain requirements shall include a comprehensive narrative to explain the solution proposed by the Contractor. If additional space is needed Contractor shall clearly label their response with the requirement identifier.
- NYS reserves the right to allow the Contractor to correct obvious errors of omission.

Assumptions/Context

1. All systems proposed by the Contractor shall comply with RMS Attachment 3, T11, and shall be in a currently supported state at the time of implementation.
2. All solutions proposed by the Contractor shall comply with NYS Information Technology Services Information Security Policy and Standards. For more information refer to the following link:
<https://www.its.ny.gov/eiso/policies/security>
3. All solutions proposed by the Contractor shall comply with CJIS Security Policy. For more information refer to the following link: <http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center>

Rqmt No.	Req Status	Requirement Type: Technology General Mandatory Requirements	Contractor Responses	
			Offered	Not Offered
T1	M	The proposed solution shall support a high availability configuration of hardware and software	<input checked="" type="checkbox"/>	<input type="checkbox"/>
T2	M	<p>The New York State Police conducts critical law enforcement operations 24 hours a day, seven days a week. The NYSP is supported by a NYS Call Center that will receive and vet all issues prior to logging with the Contractor for response.</p> <p>NYS requires the following for any RMS solution:</p> <ol style="list-style-type: none"> 1. Contractor support must be available 24 hours a day, 7 days a week, 365 days a year. 2. A maximum 30 minute initial response time* is necessary for any application downtime or major system outage impacting a large number of users where no workaround exists. <p>By indicating that this is offered, the Contractor certifies that these requirements shall be met.</p> <p><i>* Response Time is understood to mean an undertaking of action in the form of troubleshooting the issue.</i></p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
T3	M	The proposed solution shall support a permanent RMS training environment in the NYS Data Center that is available 24/7/365 using the same version of the Contractor's solution currently in production with NYS	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Niche Technology response – Mandatory Technical Requirements

Niche Technology is already supporting these requirements for large police RMS installations worldwide.

Requirement: Application Performance				
Req. No.	Req. Status	Requirement Description		
T4	M	<p>The Contractor shall provide the performance characteristics that shall be measurable and enforceable based on a Contractor specified reference architecture, hosted by NYS throughout the term of the contract of its proposed solution including, but not limited to, the following:</p> <ul style="list-style-type: none"> • Response time for EACH function; • Impact to business operations during report generation / search requests; • Due to the critical nature of the RMS and 24 x 7 x 365 use, scheduled application downtime must be completed with the least amount of impact to business operations. All scheduled application downtime will be reviewed and approved by NYS and will follow the NYS ITS change control process. <p>The Contractor's response shall include a description of how each performance characteristic will be measured throughout the term of the contract and how, prior to implementation, the Contractor would complete performance testing in a NYS hosted reference architecture to validate for NYS that the proposed solution meets the stated performance requirements. In addition, the Contractor's response shall include a description of the average time for scheduled application downtime and impact to business operations.</p>		
<p>Provide a comprehensive description of how the proposed solution satisfies the requirement including technical specifications, capabilities, features, considerations, constraints, and limitations. Reference additional pages, if necessary. Indicate if the solution is offered or not offered →</p>			<p>Offered <input checked="" type="checkbox"/></p>	<p>Not Offered <input type="checkbox"/></p>
<p>Niche Technology response: see our response material immediately following this table.</p>				

Niche Technology response – Application Performance

Overview

Thorough system monitoring is essential for reliable operation. NicheRMS is compatible with a standard Windows Performance and Alerts service, such as Perfmon.

Windows Perfmon integration is part of SQL Server and Windows and Niche provides Perfmon integration for the Niche Data Server (NDS). This allows all aspects of system operation to be recorded and analyzed through a single tool. The monitoring applies to the application server layer and the database server layer, and to all aspects of each component, such as processor time, memory use, network-related metrics, storage performance, and layer-specific counters such as those produced by SQL Server and NDS.

Use of a standard performance-monitoring solution allows customers to integrate NicheRMS monitoring into their system administration processes.

Support for requirements

The Contractor shall provide the performance characteristics that shall be measurable and enforceable based on a Contractor specified reference architecture, hosted by NYS throughout the term of the contract of its proposed solution including, but not limited to, the following:

Response time for EACH function;

NicheRMS is compatible with a standard Windows Performance and Alerts service, such as Perfmon. Windows Perfmon integration is part of SQL Server and Windows and Niche provides Perfmon integration for the Niche Data Server (NDS). This allows all aspects of system operation to be recorded and analyzed through a single tool. The monitoring applies to the application server and database server layers, and to all aspects of each component, such as processor time, memory use, network-related metrics, storage performance, and layer-specific counters such as those produced by SQL Server and NDS.

We provide application-specific counters that are automatically installed with the NicheRMS application (NDS) servers. Customers and designated partners can use this data to track application-level numbers of user connections, transactional volume, and average response times, including specialized counters that track the NDS-level and database-level contributions to the overall response time.

The NDS application server publishes performance counters for consumption by Microsoft's Perfmon tool and Performance Logs and Alerts service. Examples include:

- Number of users logged in
- Transactions per second
- Average total response time (defined below)

Average total response time is the average time that a single user or interface-initiated transaction takes to execute, including both NDS and database server processing time. This is elapsed time, not CPU time, and measures users' experience (except for network delay).

Most user actions require more than a single transaction, and transaction times vary significantly depending on what is being done, but the average total response time provides a very good instantaneous measure of user experience.

Within this context, the following are the response times for the major types of NicheRMS operations:

- Time from keying characters on keyboard to appearance on screen – instantaneous
- Time for writing to database (e.g., saving a full or partial record) - < 2 seconds in 99% of cases
- Time for creating new record on database - < 2 seconds in 99% of cases
- Time for doing a simple search on records to reveal matches (e.g., person search on surname or combination of several demographic details) - < 2 seconds in 99% of cases
- Time for retrieving a record from the database - < 2 seconds in 99% of cases

It is not possible to predict the response time for complex ad-hoc searches and reporting operations, as the required time varies widely. Some investigative searches and statistical reports can be very complex, and take a correspondingly long time to execute, but provide substantial value to the user.

For more on performance monitoring, please see our supplementary material below.

Impact to business operations during report generation / search requests;

In everyday use, users can generate standard reports and carry out standard searches and queries without affecting system performance, as these types of activities do not have a significant impact on system load.

User profiles for employees in standard officer and other police employee roles can be set to prevent a user from generating a query that will return more than a set maximum of results.

For users who need to generate large or complex reports, or interfaces that extract large quantities of data, many customers choose to replicate operational data to a reporting server. The reporting server is a replicated copy of the primary database with its own database server and storage that is used to run complex searches, large reports and data extracts (through the application layer or directly against the database). Load placed on the reporting server does not impact interactive system users (unless they choose to run searches on the reporting server).

Due to the critical nature of the RMS and 24 x 7 x 365 use, scheduled application downtime must be completed with the least amount of impact to business operations. All scheduled application downtime will be reviewed and approved by NYS and will follow the NYS ITS change control process.

There is no routine downtime required for NicheRMS maintenance. However, downtime is required for software upgrades. The downtime can be minimized through proper planning and preparation, but cannot be eliminated. For longer periods planned downtime, it is possible to provide read-only access to the system while the upgrade is taking place. This significantly mitigates officer safety issues by providing officers with most of the information that they would have had access to under normal circumstances, although officer efficiency is still affected.

The downtime required for upgrades and updates depends on the size and extent of the update. NicheRMS upgrades are not provided suddenly or at random. Niche provides knowledge transfer during the initial implementation project, and the working assumption is that the customer will have staff available who are familiar with NicheRMS and its standard system administration tasks, either directly or via contract with a third party IT provider. When there are new releases, Niche personnel provide the customer's IT staff with detailed instructions and any scripts or specialty utilities required. Niche also provides release and installation assistance via telephone and email, on a 24/7/365 basis.

The size and extent of the update also affect processes to be followed. Niche provides detailed instructions and, where necessary, scripts to be run against the database. Examples of upgrade processes include:

- NicheRMS end user application update: Managed centrally using Niche-provided tools.
- NicheRMS database schema update: Scripts provided by Niche database team to the customer database team.
- NicheRMS server application update: Standard process provided by Niche.
- Application configuration updates: Performed by application administrators.

Note we typically recommend that the update be implemented in a test system before being used to update the production system.

Details of the upgrade process and typical timelines also depend on how many changes the customer has asked to have "turned on" in the upgrade build. Agencies often ask for additional functionality inside the product from when they first go-live. The actual upgrade software installation takes little time at all. A major agency with thousands of officers that has to run a database schema update may have the RMS down for a few hours while the schema update script is run.

Agencies schedule upgrade installations through their Niche Project Manager to ensure that adequate technical resources are available in the unlikely event something goes wrong in the process. Niche technical staff can then quickly attend to any issues that occur.

The Contractor's response shall include a description of how each performance characteristic will be measured throughout the term of the contract and how, prior to implementation, the Contractor would complete performance testing in a NYS hosted reference architecture to validate for NYS that the

proposed solution meets the stated performance requirements. In addition, the Contractor's response shall include a description of the average time for scheduled application downtime and impact to business operations.

The system is always installed and fully tested in the customer environment, both before and after implementation. This is a standard part of our project methodology.

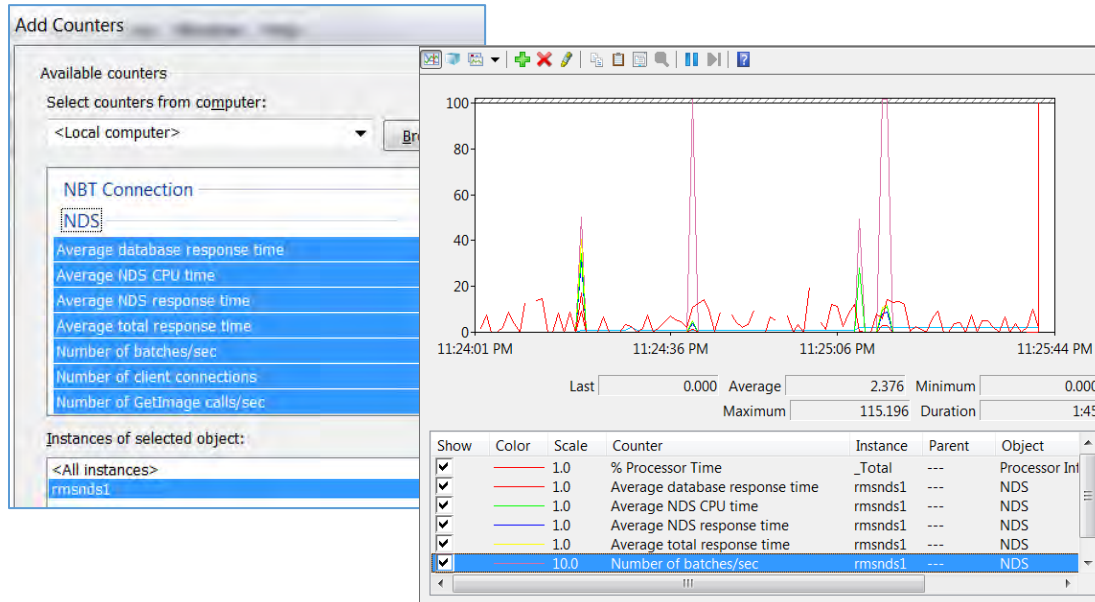
In addition, Niche provides periodic analysis of system operation as part of its support service. It is very important to do this prior to and after hardware or software changes/upgrades. This analysis provides a performance baseline prior to the hardware or software change and an objective evaluation of the impact of the change after it is complete. This is always carried out in the customer environment.

Please see our detailed performance monitoring information below for more details. For information on scheduled downtime, please see our response to the bullet point previous to this one.

Supplementary material: Application performance monitoring

Thorough system monitoring is essential for reliable operation. NicheRMS is compatible with a standard Windows Performance and Alerts service, such as Perfmon. Use of a standard performance-monitoring solution allows customers to easily integrate NicheRMS monitoring into their system administration processes.

Windows Perfmon integration is part of SQL Server and Windows and Niche provides Perfmon integration for the Niche Data Server (NDS), allowing all aspects of system operation to be recorded and analyzed through a single tool. The monitoring applies to the application server layer and the database server layer, and to all aspects of each component, such as processor time, memory use, network-related metrics, storage performance, and layer-specific counters such as those produced by SQL Server and NDS.



Niche provides application-specific counters that are automatically installed along with the NicheRMS application (NDS) servers. Customers and their designated partners can use this data to track the application-level number of user connections, transactional volume, and the average response time, including specialized counters that track the NDS-level and database-level contributions to the overall response time.

The NDS application server publishes performance counters for consumption by Microsoft's Perfmon tool and Performance Logs and Alerts service. Examples include:

- Number of users logged in

- Transactions per second
- Average total response time (defined below)

Average total response time is the average time that a single user or interface-initiated transaction takes to execute, including both NDS and database server processing time. This is elapsed time, not CPU time, and measures users' experience (except for network delay). Most user actions require more than a single transaction, and transaction times vary significantly depending on what is being done, but the average total response time provides a very good instantaneous measure of user experience.

Microsoft Windows and SQL Server also provide a large number of Perfmon counters, allowing all aspects of system operation to be monitored simultaneously, including CPU load, disk I/O, network traffic, memory use, SQL Server buffer use, SQL Server cache use, etc.

In addition to providing an instantaneous graphical representation of system performance, the Windows Performance Logs and Alerts service can be configured to record any set of counters (in the background) and can generate alarms when specified counters range outside desirable values. Niche provides an extensive list of counters that should be monitored in a production environment, including detailed information regarding healthy and typical ranges for key performance counters on the application and database servers.

Niche provides documentation and other forms of guidance regarding the above monitoring; it covers both the application layer and database layer, and addresses NicheRMS-specific counters and those published by Windows and SQL Server. For example, we provide a Windows Performance Monitoring manual that specifies healthy ranges of values for average total response time, application server CPU use, database server CPU use, SQL Server page life expectancy, transaction log I/O read latency, and so on. Niche has arrived at these values through extensive experience in the monitoring, as well as in the tuning of large NicheRMS implementations, and they are subject to ongoing assessment and revision.

Connection volume for end user NDS instances; typical business day (M-F 0800-1600)

Approx. # of connections	Notes
< 400	<ul style="list-style-type: none"> • Sufficient capacity to absorb additional users without memory pressure and stability effects • Most load balanced NDS installations can afford to lose at least one NDS without affecting overall system stability
400 - 600	<ul style="list-style-type: none"> • Plan to deploy additional NDS instances • Losing a server could result in the remaining NDS instances experiencing instability effects due to an increase in user connections/memory consumption
600 <	<ul style="list-style-type: none"> • Short term action required to make additional NDS instances available • Increased risk of instability effects due to lack of memory available to NDS.exe

Niche provides additional tools and guidance for detailed analysis of the system:

- Application layer capture/analysis of user operations, including aggregate analysis by operation type.
- Capture and analysis of long-running database queries, including aggregate analysis by operation type.
- Database-level wait stats analysis and block/lock analysis.
- Guidance regarding capture of application state using procdump, windbg, and related debugging tools, and how to configure the tools to capture unusual application behavior.

We advise customers to run the data collection aspects of most monitoring tools continuously, so that unusual events are captured as they happen instead of waiting for recurrence. Regular analysis of monitoring data can point out trends in system performance that can be corrected before they affect users.

In addition, there needs to be monitoring of secondary services across the data centers. This includes monitoring of AlwaysOn replica/mirrored database health, replication health, SAN/storage array-level performance, VMware-level hypervisor performance, *etc.* These metrics can be monitored through Microsoft-provided tools or management views, or you may use third-party tools to monitor these infrastructure components if you prefer. The key is to ensure that these system components are, in fact, being monitored according to best practices and that the resulting data is being assessed.

Statistical reporting of system performance

Perfmon logging and diagnostic log analysis can be used to track system performance over time. This information can form the base of any service reporting process. The report generation process can be automated and integrated with other police agency reporting processes. It is also possible to develop a simple interface application that uses the mechanisms that feed the Perfmon counters directly and extract the data into third-party reporting products. Other means of integrating with customer reporting are also possible.

Periodic analysis/health monitoring by Niche

Niche provides periodic analysis of system operation as part of its support service. It is important to do this before and after hardware or software changes/upgrades. This analysis provides a performance baseline prior to a hardware or software change and an objective evaluation of the impact of the change after it is complete.

Niche in-depth performance analysis

While Perfmon provides useful aggregate system performance monitoring, it does not provide details of which transactions perform well, how performance changes over long time periods, *etc.* The NDS audit logs and diagnostic logs record the time used by various system components in servicing each client request. Niche provides post-processing analysis tools to classify request types and graph performance trends over time. These tools allow low-level NDS transactions to be analyzed and can report trends. The diagnostic log analysis can also report information about network delays between the servers and the client workstations.

This type of analysis serves two purposes: it provides information about the volume of system use and how system response is changing over time and it provides information that is used as a starting point in identifying and optimizing expensive transactions (execution time x execution frequency) and long-running transactions (possibly not expensive due to low execution frequency, but problematic for the small number of users that run them). This type of reporting is used for proactive analysis (*e.g.* establishing a performance baseline prior to a software change) and when there are performance problems requiring analysis.

Niche also provides blocking/locking and wait stats monitoring scripts that record detailed information for solving more complicated database performance issues. In addition, SQL Server traces are used to locate long-running queries to help diagnose performance problems. As with the analysis of NDS-level operations, Niche provides tools that can group expensive database-level operations into high-level categories, allowing for the clear prioritization of tasks within analysis and optimization exercises.

Transaction response times

The following are the response times for the major types of NicheRMS operations:

- Time from keying characters on keyboard to appearance on screen – instantaneous
- Time for writing to database (*e.g.*, saving a full or partial record) - < 2 seconds in 99% of cases
- Time for creating new record on database - < 2 seconds in 99% of cases

- Time for doing a simple search on records to reveal matches (e.g., person search on surname or combination of several demographic details) - < 2 seconds in 99% of cases
- Time for retrieving a record from the database - < 2 seconds in 99% of cases

It is not possible to predict the response time for complex ad-hoc searches and reporting operations, as the required time varies widely. Some investigative searches and statistical reports can be very complex, and take a correspondingly long time to execute, but provide substantial value to the user.

Unscheduled system downtime

Downtime due to hardware and network failure can be kept under 0.25% / 60 minutes by proper design and testing of redundant features in the installation, as described within this response. Niche works with customer IT staff to design a solution that works with NicheRMS and fits into the current IT infrastructure, both during the initial implementation and all subsequent site refresh exercises.

Similarly, unplanned downtime can be minimized through the appropriate configuration of the system, proactive review of monitoring data and the use of automated alerts.

However, it is not possible to guarantee 0.25% / 60 minutes for system failures due to customer operator error, including implementing configuration changes to the environment or NicheRMS software without proper understanding and testing. It is also not possible to achieve a 0.25% / 60 minute target for actual defects in the RMS software, simply because of the time it takes to diagnose and fix a real problem.

Niche takes uptime requirements seriously – our customers have repeatedly affirmed that NicheRMS is one of their most reliable systems. For example, historic uptime stats from Merseyside Police showed system availability at 99.88% during normal system operation outside of scheduled downtime. That sample did in fact cover one period of downtime whereby the customer DB server had run out of memory due to misconfiguration. In that case, and many similar cases, the short-term solution was relatively simple (server restart) and the customer subsequently worked with Niche to enforce appropriate configuration of the system. However, the purely customer-side handling of the issue took 35 minutes to execute.

Further, Niche works diligently to avoid problems and to fix them as quickly as possible when they occur. In addition to the software design, monitoring, and troubleshooting techniques illustrated elsewhere in this response, Niche directly notifies customers of known critical issues, providing guidance on how to receive software fixes for the issue (if the issue is within NicheRMS) and how to otherwise avoid or workaround the issue, if such information exists.

Scheduled system downtime required for maintenance and upgrades

There is no routine downtime required for NicheRMS maintenance. However, downtime is required for software upgrades. Downtime can be minimized through proper planning and preparation, but cannot be eliminated.

For upgrades and updates, the amount of time depends on the size and extent of the update. It is necessary to schedule a longer downtime for major system upgrades and server estate refreshes. NicheRMS software upgrades can typically be performed very quickly. However, the size of a large-installation database means that database schema changes can take longer than one hour, particularly when the customer has gone significant periods of time (years) without performing a significant version update.

This type of downtime can be scheduled and steps can be taken to ameliorate operational difficulties. For example, if a major database schema update will take too long, a read-only instance of the system can be set up ahead of time to allow users to query – but not update – data during the downtime. Niche also has significant experience with fine tuning the database update process so that time-consuming tasks can be performed either while the system is online, or in parallel with other tasks during the upgrade.

NicheRMS upgrades are not provided suddenly or at random. Niche provides knowledge transfer during the initial implementation project, and the working assumption is that the customer will have staff available who are familiar with the NicheRMS system and with standard system administration tasks, either directly or via contract with a third party IT provider. When there are new releases, Niche personnel provide the customer's IT staff with detailed instructions and any scripts or specialty utilities required. Niche also provides release and installation assistance via telephone and email, on a 24/7/365 basis.

The processes to be followed also depend on the size and extent of the update, and Niche provides detailed instructions and, where necessary, scripts to be run against the database. Upgrade processes:

- NicheRMS end user application update: Managed centrally using Niche-provided tools.
- NicheRMS database schema update: Scripts provided by Niche database team to the customer database team.
- NicheRMS server application update: Standard process provided by Niche.
- Application configuration updates: Performed by application administrators.

Note we typically recommend that the update be implemented in a test system before being used to update the production system. Agencies schedule upgrade installations through their Project Manager to ensure that adequate technical resources are available in the unlikely event something goes wrong in the process. Niche technical staff can then quickly attend to any issues that occur.

Disaster recovery

NicheRMS supports a remote disaster recovery (DR) site:

- The DR site can be maintained as a “warm standby” site using SQL Server log shipping or asynchronous database mirroring. Use of asynchronous processes for maintaining the DR site data means that failover to the DR site should be manually triggered. This is normally acceptable as failover to DR is either deliberate (e.g., to allow hardware or network maintenance at the primary site) or results from a catastrophic (and rare) event.
- The DR site can potentially be maintained using synchronous database mirroring, which could allow instantaneous automatic failover. However, this configuration requires some NicheRMS development and requires substantial evaluation and testing because it can have a significant performance impact.
- The DR site can be maintained as a “cold standby” site using SAN mirroring. Failover could be automatic using tools external to NicheRMS, but is more likely to be manual.
- Network resiliency is the responsibility of the police agency.

Requirement: Application Scalability				
Req. No.	Req. Status	Requirement Description		
T5	M	Break out of scalability requirements The Contractor shall identify the mechanisms supported by their offering that will enable NYS to support the expected transaction volumes and identify how they can be extended to support the expected expansion of the user base of the RMS. Mechanisms and approaches identified must be consistent with the hardware and software requirements of NYS (as defined in RMS Attachment 3, Requirement T11.		
Provide a comprehensive description of how the proposed solution satisfies the requirement including technical specifications, capabilities, features, considerations, constraints, and limitations. Reference additional pages, if necessary. Indicate if the solution is offered or not offered →			Offered <input checked="" type="checkbox"/>	Not Offered <input type="checkbox"/>
Niche Technology response: see our response material immediately following this table.				

Niche Technology response – Application Scalability

Overview

NicheRMS is designed to be scalable from very small systems (e.g., a demonstration or small training system on a single laptop) to a very large system capable of supporting the NYSP. The ability to support large transaction volumes is a major feature of our system’s design: our first major installation was for a multi-tenant system supporting more than 40 agencies and 8,000+ sworn officers.

Support for requirements

The Contractor shall identify the mechanisms supported by their offering that will enable NYS to support the expected transaction volumes and identify how they can be extended to support the expected expansion of the user base of the RMS. Mechanisms and approaches identified must be consistent with the hardware and software requirements of NYS (as defined in RMS Attachment 3, Requirement T11.

The components of our recommended hardware and software environment have been thoroughly proven in NicheRMS installations, including installations with over 10,000 officers that have been running for more than a decade.

Different parts of the NicheRMS architecture can be scaled in different ways:

- Use of commodity hardware means that the application can be migrated onto newer or higher performance hardware over time as demands grow and equipment is refreshed.
- NDS application servers are load balanced and can be easily scaled by adding more servers. These are inexpensive commodity servers (or virtual servers) that can easily be added as required.
- Database server can be scaled out by offloading reporting and audit log functionality.
- The database server we recommend can be scaled up by allocating more CPU cores to the RDBMS and more memory to increase performance. This approach may be of use if the phased implementation is over a long period of time, e.g., if you start with a small go-live followed by other larger go-lives. However, if the implementation period is very long, it may make more sense to purchase a smaller, less

expensive database server initially and plan to replace it with a higher capacity one as the need arises. This approach also takes advantage of the continuously improving server technology. The old server could then be redeployed for other purposes.

- Database storage can be expanded easily by adding more disks and expanding the SQL Server storage volume, adding a second storage volume, *etc.*

It is a good idea to design the NicheRMS architecture for its final state when the system is being set up initially. However, it is not necessary to implement the full architecture for an initial limited go-live. Options for partial implementations include:

- Fewer NDS application servers
- No separate reporting and audit log database servers
- Lower capacity database server
- Lower capacity and/or lower performance SAN or other storage array
- Less (or no) redundancy at the primary site
- No, or lower capacity, remote disaster recovery site

Supplementary material: Application scalability

Options supporting scalability

Some parts of the system, like the NDS application servers, can easily be scaled simply by adding more servers. NDS servers are basic commodity-grade computer servers, typically having 4 vCPUs and 8 GB of memory, and they require very little per-instance configuration before being added to the load balancing solution. That is, they are well suited to VM templating and other standard techniques for expansion of computational capacity.

The primary read-write database server is not horizontally/outwardly scalable, and as such, is sized to handle any anticipated CPU load. Any expansion of processing capacity for this server role would require adding more processing units (vCPUs, cores) into the hosting environment. Upward scalability on other dimensions, such as increased instance-level memory or I/O performance, is more common to implement as it does not require additional SQL Server licensing costs.

Database server instances hosting additional secondary read-only databases can provide horizontal scalability of read only operations, such as search, reporting, data extracts, and certain out of the box external system interfaces.

NicheRMS facilitates the horizontal scaling of read-only operations by providing an automated process to generate and maintain transactional publications and subscriptions for read-only databases, using the current application metadata and database schema to generate the correct replicated articles.

Planning for future performance and capacity

NicheRMS systems are sized according to size of the police agency (number of sworn officers), as this gives a reasonable estimate of the amount of work that will be done. Note that growth in database size does not usually have a serious impact on system load. It does, of course, require the storage subsystem to grow, but modern SAN systems allow expansion of storage and the database server allows the database to be extended on a single storage volume or onto multiple storage volumes.

Because NicheRMS is a COTS product whose code base is shared across all customers, new versions of the proposed application are deployed into test and production environments on an ongoing basis. This wide level

of testing and production use means that application adjustments are made continuously, and generally require very little tuning prior to a deployment or upgrade.

For licensing; if an increase in infrastructure requirements is not due to a related increase in sworn officer count, but simply due to an expansion in the use of system features, scaling up or out does not require any additional NicheRMS software licensing. However, it may require additional associated investment in the software and hardware infrastructure within the hosting solution that supports NicheRMS.

Options for storage and archiving

Production NicheRMS databases range in size from 25 GB to many terabytes.

- RAID 1+0 should be used for the best performance and redundancy.
- Required storage depends on the volume of scanned files, images, and imported data.
- Customers may choose to use RAID 5/6 for binary data such as images and report narratives, which do not have the same performance requirements as fielded data.

It is impossible to determine the required size of the storage you require without investigation of any data to be converted and how the system will be used. Of most importance is whether scanned documents and large images will be stored in the NicheRMS database or stored in an external DAMS, document management system, or both. Since scanned documents represent as much as 90% of the storage in some NicheRMS systems, the effect of scanned data, forms and images can be huge.

The data storage array that we propose can be expanded to 500TB of capacity, which will result in about 400TB of usable storage if it is partitioned properly between fast RAID 1+0 and more efficient RAID 5 or 6. More detailed analysis is required to determine how much capacity is actually required for the New York State project. Please note that growth in database size does not usually have a serious impact on system load.

Requirement: Security / Authentication				
Req. No.	Req. Status	Requirement Description		
T6	M	<p>Contractor shall describe how their offering conforms to requirements regarding security and user authentication of the NYS Directory services offerings and the NYS Information Technology Services Information Security Policy and Standards¹. The response shall include but not be limited to the following components:</p> <ol style="list-style-type: none"> 1. How their offering will integrate with NYS EIAM as Identity Provider for authentication and authorization. 2. Describe their approach to remote and mobile security consistent with NYS and CJIS security requirements². 3. Approach to compartmentalization of agency owned data based on individual law enforcement agency rules; 4. Approach to logging access and modifications to data including access from mobile devices and equipment in their cars; 5. Approach to the detection of inappropriate access of information <p>¹For information regarding NYS Information Technology Services Information Security Standards refer to the following link: https://www.its.ny.gov/eiso/policies/security</p> <p>²For more information regarding CJIS security policy refer to the following link: http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center</p> <p>For information regarding EIAM please see RMS Appendix 7 NY.gov ID Specification</p>		
<p>Provide a comprehensive description of how the proposed solution satisfies the requirement including technical specifications, capabilities, features, considerations, constraints, and limitations. Reference additional pages, if necessary. Indicate if the solution is offered or not offered →</p>			<p>Offered <input checked="" type="checkbox"/></p>	<p>Not Offered <input type="checkbox"/></p>
<p>Niche Technology response: see our response material immediately following this table.</p>				

Niche Technology response – Security/Authentication

Overview

Niche Technology provides a security model that meets all of the requirements listed above. We provide several ways in which access to individual database records and specific reports can be carefully controlled. Please see below for more information.

NicheRMS has a flexible access control system designed to prevent unauthorized access by:

- Identifying and authenticating users robustly, including using two-factor authentication.

- Preventing users from accessing data and performing operations that they are not allowed to access or perform.
- Preventing users from accessing data they do not need to access.
- Logging all activity.

What follows is an overview of how Niche controls access to data in the NicheRMS database. More detailed technical information can be provided on request.

Support for requirements

Contractor shall describe how their offering conforms to requirements regarding security and user authentication of the NYS Directory services offerings and the NYS Information Technology Services Information Security Policy and Standards¹. The response shall include but not be limited to the following components:

How their offering will integrate with NYS EIAM as Identity Provider for authentication and authorization.

The NicheRMS architecture abstracts the identification and authentication functions of the system so that a variety of identification and authentication technologies can be supported without affecting the rest of the system. The common authentication mechanisms supported are:

- 1) Username/password managed internally by NicheRMS. Password complexity, reuse and login failure lockouts are managed by NicheRMS.
- 2) Kerberos/Windows integrated authentication. This allows users authenticated to a Windows domain to log in to NicheRMS without further authentication by using their Windows credentials. Credentials are managed by Windows or by whatever system is used to log in to windows (e.g. multi-factor authentication).
- 3) Token-based (smart card or USB token), multi-factor PKI authentication. Certificates, revocation lists and passwords/PINs are managed by the PKI.

Windows integrated authentication is the most common solution to providing single sign on in NicheRMS installations since users must be authenticated to Windows to access NicheRMS as well as other police systems, so either Windows authentication is the authoritative authentication source in the police service or Windows sign on is integrated with an enterprise-wide identity and authentication service. In either case, NicheRMS leverages the Windows credentials to authenticate users.

If Windows authentication is not a viable way to integrate with NYS EIAM, Niche can add the ability to integrate directly with NYS EIAM. As only the identification and authentication functions the NicheRMS system will be affected, this can be done without having any deleterious effect on the rest of the NicheRMS system.

The best approach to adding direct NYS EIAM support to NicheRMS depends on the technical details of NYS EIAM integration facilities (e.g. availability of SAML, OAuth, LDAP or some other mechanism). Development of this integration will be performed by Niche Technology developers working at our main office and will require remote access to a test system, either directly via the Internet or through a VPN, and will require appropriate documentation and technical support by NYS IT personnel.

Describe their approach to remote and mobile security consistent with NYS and CJIS security requirements².

Most CJIS-mandated risk mitigation for remote and mobile devices consists of agency-managed policies and device controls such as the implementation of Mobile Device Management systems, encryption of mobile

computer storage, use of Advanced Authentication, etc. NicheRMS supports these requirements through a number of technical features, described below:

- 1) End-to-end application-level encryption. NicheRMS can be configured to encrypt all data between the client app and the NDS application servers. This is particularly useful when CJI data is being transmitted across a large wide-area (e.g. state-wide) network where access and administration is not fully under the control of the police agency. It also protects CJI in environments where the network or server infrastructure is not under police control, and provides adjunct security for the VPNs normally used for mobile CJI access.
- 2) Support for Advanced Authentication. NicheRMS mobile apps (on Windows systems) support PKI token-based two-factor authentication (as well as all other NicheRMS authentication options), and are either compatible with, or can be enhanced to support other Advanced Authentication technologies.
- 3) Mutual authentication when using PKI two-factor authentication. By authenticating the user to the server and the server to the user, mutual authentication reduces the risk of man-in-the-middle attacks when mobile and remote devices connect via complex, unknown and outsourced network infrastructures.
- 4) Pass-through authentication. To support third-party smartphone apps that implement their own Advanced Authentication, NicheRMS can be configured to trust specific third-party servers connected via isolated network interfaces. If the third-party app is using PKI-based Advanced Authentication, NicheRMS can be configured to send a cryptographic challenge to the mobile app to verify that the device has access to the PKI token belonging to the user attempting to connect to the system.
- 5) Encrypted local storage. NicheRMS client apps are compatible with the encryption of local disk storage. Additionally, locally cached data is encrypted at the application level to mitigate risk if the device is lost or stolen.
- 6) Unified audit logs. NicheRMS audit logs record all system activity, no matter whether it originates on a desktop workstation, a mobile computer, a mobile device (e.g., smartphone), a third-party mobile or Web app, CAD, or any other source. Audit records identify the end user, no matter what the source of the operation or the authentication method used.

Approach to compartmentalization of agency owned data based on individual law enforcement agency rules;

Ownership of data in NicheRMS is based on a hierarchical system of domains that define sets of data and data ownership.

- NicheRMS assigns every data record to a domain within the database.
- Domains are arranged hierarchically: each police agency typically has its own domain with optional sub-domains.
- Each user is given access to one or more domains. A user may be granted different roles in different domains, so users may have update access in their home domains, and view-only access in other domains.
- The domain determines who owns the data. Domain ownership information can be used to control access by users in other domains.

This will allow each agency within a multi-tenant system to control access to its own agency-owned data.

Approach to logging access and modifications to data including access from mobile devices and equipment in their cars;

As we have said, the same user authentication and authorization processes apply broadly across all mobile devices and equipment. No user or interface can access the system without a standard authenticating login. Once logged in, the system's RBAC user roles and Access Control list will allow the NYSP to exercise tight control over what each user is allowed to access, and which data operations they have access to.

In addition, all logins and user actions while logged in are captured by the Niche Auditing system, which we describe in our Supplementary material section below. The Auditing system automatically captures all user actions including all modifications to data, no matter what their location is, or what device they are using.

NicheRMS also supports data encryption:

- **Protection of data 'at rest':** NicheRMS is designed such that users and applications should never have direct access to the database, except for a very few carefully controlled situations. Firewalls and other network-level controls can ensure that the database servers are never exposed to the general police network. Access to the database can be limited to the secure server room network. Most backup tools permit database backups to be encrypted, which is useful if the backup media is physically moved out of the server room for offsite backups. Similarly, any data extracts, logs, etc. moved outside the server room should be encrypted.

It is more difficult to protect the database from the system administrators who have physical access to the server hardware and are responsible for the operation of the hardware and software. NicheRMS is designed to allow for separation of duties between database administrators, audit log administrators and NicheRMS application administrators.

- **Protection of data 'in transit':** Data in transit is much easier to protect than data at rest. Standard encryption technologies will provide adequate protection from eavesdropping, man-in-the-middle and injection attacks. NicheRMS currently supports end-to-end application-level encryption (NicheRMS app to NDS server) of the network data connection when Kerberos or TLS authentication is used. Encryption is similarly available to any third-party app or interface that uses the Niche NDSCONnect API.

NicheRMS uses 3DES encryption with cipher block chaining when using TLS authentication and the Windows default encryption (typically AES) when using Kerberos authentication. Note that encryption is not currently available for Niche internal username/password authentication. The NicheRMS Web service can use the encrypted HTTPS protocol for communication with external systems.

Approach to the detection of inappropriate access of information

NicheRMS includes a robust, mature security infrastructure. As we describe in our supplementary material below, all system security and access is managed by the Niche Data Server (NDS), which ensures that no user or external interface can access the system without logging in, and that once logged in, the user or interface can only access the data and operations allowed by the domains, roles and ACLs they have been granted.

In addition, all operations performed by users are recorded in audit logs, including error messages generated when users attempt to perform operations that are disallowed by their security role. These logged errors can be examined to determine if there is a systematic attempt to penetrate the system. The security system is designed to prevent unauthorized activity, so any violation that can be detected is disallowed.

The following are some of the actions the system can take (configuration dependent):

1. **Repeated login failures:** User ID is locked out temporarily and/or permanently, depending on configuration. Applies only to built-in username/password authentication.
2. **Attempts to access protected data:** Protected data is filtered at the database server or the NDS application server (depending on how access to that data is controlled). Users do not get any

indication of the existence of the hidden data unless they are logged in with an ID that specifically grants them access.

3. **Attempts to modify protected data:** Error messages are generated and logged.
4. **Attempts to perform operations that are disallowed:** Error messages are generated and logged.
5. **Attempts to retrieve large amounts of data:** The system disallows retrieval of very large quantities of data. This is meant primarily to control load on the system; it also makes any attempt to perform a bulk download of data more difficult and more easily identified.
6. **Sensitive records can be flagged.** A notification will be generated and sent to a specified user or group when someone searches for and retrieves the flagged record. This mechanism is used both by investigators who want to be informed when an individual has contact with police and by security staff who want to monitor for suspicious access to particular records.

Non-repudiation of information: NicheRMS includes a very granular, fielded auditing system. The audit logs provide a complete record of the actions performed by each logged in user or interface, providing non-repudiation. NicheRMS also allows digital signatures to be captured on a variety of data in the system, providing evidence that a particular user or external party “signed off” on the data.

Non-repudiation features are further enhanced if two-factor authentication is deployed. NicheRMS supports two-factor authentication both by direct use of PKI tokens (typically USB or smart card) that are compatible with the Windows Cryptographic API and by the use of Windows Kerberos (Active Directory) authentication, with or without the use of two-factor tokens. Built-in username/password authentication is supported as well, but it does not prove user identity as robustly as two-factor authentication. See our supplementary material below for more on the Niche Auditing system.

Supplementary material: NicheRMS security and authentication

Niche Technology provides a security model that meets all of the requirements listed above. We provide several ways in which access to individual database records and specific reports can be carefully controlled. Please see below for more information.

NicheRMS has a flexible access control system designed to prevent unauthorized access by:

- Identifying and authenticating users robustly, including using two-factor authentication.
- Preventing users from accessing data and performing operations that they are not allowed to access or perform.
- Preventing users from accessing data they do not need to access.
- Logging all activity.

What follows is an overview of how Niche controls access to data in the NicheRMS database. More detailed technical information can be provided on request.

User authentication (logins)

Users must log in to NicheRMS before they can access any data or functions. For verifying a user’s identity on initial login, NicheRMS supports the following authentication options:

- **Active directory (Kerberos or NTLM)** authentication using username/password or two-factor authentication: When configured for Kerberos authentication, NicheRMS uses Windows authentication facilities to provide a secure, mutually authenticated connection between the client (user) and the NicheRMS application server. In most cases, the system is configured so that users are not required to re-authenticate when starting NicheRMS—Windows login credentials are automatically used. Kerberos-authenticated sessions can be configured for end-to-end encryption.

- **TLS authentication:** TLS authentication uses a Public Key Infrastructure (PKI) and, typically, hardware tokens (USB/smart card) to provide robust two-factor authentication without the use of Windows domains, Active Directory, *etc.* TLS provides mutual authentication (the user is authenticated to the server and the server is authenticated to the user) and, optionally, end-to-end encryption of network traffic.

NicheRMS supports single sign on when using TLS authentication (PKI tokens or smart cards). Behavior depends on the token vendor and configuration of the token and PKI.

- **Built-in authentication:** NicheRMS also provides a built-in username/password mechanism that can be used in cases where no external security package has been implemented.
- **Other authentication systems:** Other authentication mechanisms are also possible, although all existing installations have found that the options above have been sufficient.

The result is that no one can access data without logging in. Authentication is enforced no matter what device is being used: LAN/WAN connected desktop workstation, mobile laptop or hand-held device. For added security, different authentication mechanisms can be enabled on different network interfaces and/or TCP/IP ports on the NDS application servers. For example, NicheRMS built-in username/ password authentication could be allowed within the secure server room network (*e.g.*, for use by some interfaces) but disallowed for any network connection from the rest of the organization.

Niche user authentication and single sign on

For systems where users log in using Windows or PKI-based credentials, once a user has logged into the system, they can access NicheRMS without providing additional authentication.

Single authentication across functional areas

NicheRMS provides a single, unified system that does not require separate logins to different business areas, *i.e.*, separate log-ins are not required to access separate Investigation, Intelligence, Jail or Court file preparation applications. Once users have logged in and been authenticated, standard NicheRMS roles and ACLs are used to limit user access to data and operations within NicheRMS.

User authorizations (access to data)

Once users have been authenticated, their access to data is management by the NicheRMS access control subsystem (Niche Access Control or NAC). This subsystem allows an agency to control access to any record or part of a record. It can be used to limit access to any single record or to any file linked to a record (*e.g.*, intelligence reports). This subsystem controls access to operations and data in the NicheRMS database based on a combination of:

1. Domains (which specify data ownership)
2. Role-Based Access Control (RBAC) (“right-to-know” access control), and
3. Access Control Lists (ACLs) (“need-to-know” access control).

These features can be used individually or in combination to manage data access to classes of records and documents, and to data within records. This includes ensuring that confidential information will only be available to the users who are specifically allowed access.

RBAC roles are useful for controlling access to entire categories of records, for example, records involving juveniles/young offenders. The system can also be configured so that certain data fields on records will only appear to users who are logged in with particular roles.

ACLs are useful for controlling access to individual instances of records so that access to a given record or report can be blocked from users whose roles might usually allow them access.

Role-based Access Control (RBAC) for standard role-based control

NicheRMS uses domains and roles to control access to categories of information:

- **Domains** define sets of data and data ownership. NicheRMS assigns every data record to a domain within the database. Domains are arranged hierarchically: each police agency typically has its own domain with optional sub-domains. Each user is given access to one or more domains. The domain determines who owns the data. Domain ownership information can be used to control access by users in other domains.
- **Roles** define what data users are allowed to view and modify within a particular domain and what operations they are allowed to perform. Roles are often defined and assigned based on job function, and used to implement “right-to-know” security, e.g., roles can correspond to work functions, like “general patrol” or “sergeant” or “investigator”.

Roles are defined using rules that determine the access to data and operations that will be allowed to users who have been assigned those roles. An agency’s roles are usually defined during project implementation, based on agency requirements. Initially, roles are defined by Niche personnel, but agency users who are logged in with an appropriate system administrator role can access and update role definitions. Roles can be updated when and as necessary, without changes to the software code, and without having to stop or restart the system.

Each user is assigned one or more roles within a domain, and can switch between allowed roles when necessary. Note that users can be assigned different roles in different domains, so an investigator may have a senior-level role in the Internal Affairs sub-domain and have only normal user access in the rest of the police database.

Access Control Lists (ACLs) for discretionary access control

ACLs provide discretionary access control for “need-to-know” authorization in addition to the role-based “right-to-know” authorization described above. ACLs provide flexible options for allowing or denying access to sensitive information to individuals or groups.

An ACL provides a set of rules that can be applied to any data object in the system (e.g., a particular person, a person description, a report). The rules grant or deny access to an object based on the user’s identity and his organizational membership. In practice, agency system administrators can set up an ACL that includes a list of specific personnel and/or units who are “members” of that ACL. When the ACL is applied to a record or report, it means that access to that item can be immediately restricted to the members of that ACL.

Like roles, ACLs can be created, modified or removed when and as necessary, without changes to the software code and without having to stop or restart the system.

Case confidentiality: the effect of security on availability of records and reports

When a user does not have view access because of RBAC or ACL rules, the record or report in question will disappear completely for that user—it does not appear in search results, cannot be displayed and will not appear in reports. If other records link to it, for example if there is a link from an Incident record to a Person record that the user is not allowed to see, the link does not appear for that user. This will allow the New York State Police to exercise tight control over case confidentiality.

The same security applies to tasks and notifications as to other records in the system: the system ensures that users will only see the data that they are allowed to see. For tasks and notifications:

- Tasks and notifications are typically only viewed by the people they are assigned to and by their supervisors. If necessary, security can be set up to hide tasks and notifications from all users except for those with specific permissions (e.g., for Use of Agency investigations).
- Workflows can be set up so that when a task is generated and assigned, the person assigned the task will automatically be given permission to access the records that are the subject of the task. These permissions can be revoked as soon as the task is marked complete, i.e., a user can be given access on a limited basis only.

For flags and warnings/cautions applied to Incidents and master index records, the person adding the flag can select an option to hide a flag so that users will only see it if they have a role or ACL membership that specifically allows access to hidden flags.

Different security can be applied to records and reports based on creation date/time and their status. For example:

- A user may have read/write access to a report when it is first created, but the report can become locked after a certain length of time (e.g., 24 hours) or once the task associated with it has a status of "complete".
- A user who creates an intelligence submission may not have access to it after he or she clicks the submit button.

Auditing in NicheRMS

NicheRMS provides a well-established and extensive auditing system that meets all of the requirements listed in this section. Every action performed through a user application or any external system interface is logged to an audit log file outside the database. The audit log file is protected by the server's file system, not by database or NDS security, facilitating separation of duties among system administrators and making it unlikely for a user to be able to hide a security breach. NicheRMS has a number of different audit trails and layers of accessibility that serve different purposes. They are described in the sections below.

Audit logs

Every action performed through an end-user app or any external system interface is logged to audit log files held outside the database. The audit logs contain a complete record of all operations performed, including:

- Login/logout (including ID of workstation from which login occurred)
- Password change (note the password itself is not recorded)
- Domain change
- Security role change (i.e., where a user has changed from one role to another)
- Searches run
- Records retrieved (identified by primary key)
- Optional: all information returned to a user or interfacing application
- Changes to data (create, modify, delete)
- Reports printed
- Configuration and security setting changes

Audit log files are protected by the server's file system, not by database or NDS security, facilitating separation of duties among system administrators. With proper configuration of Windows server security and robust procedures, this makes it difficult for administrators and others dealing with the audit logs to hide system misuse or a security breach.

The audit logs record everything that happens in the system as a series of time-ordered activity records. Once the audit log files have been loaded into the auditing database, NicheRMS provides an Audit Log Viewer that allows the activity records to be searched and organized by user, by session, by database entity affected, etc. to allow auditors to gain a proper understanding of system activity.

Audit log server

NicheRMS records audit logs as files on the NDS servers. The recommended practice for online audit log access is to use a Niche-supplied utility to load the audit logs into an audit log database, where they are accessed using the desktop client through the production NDS servers. The audit log database can be hosted by the reporting database server or it can be hosted on a dedicated audit log server. Audit log files can be digitally signed (optional) and should be archived on offline storage (e.g., DVDs).

Audit log retention

All logs can be archived and retained for as long as necessary and legally required. Note that when audit logs are loaded into the audit database, any details that are deemed uninteresting can be filtered out and not loaded, saving space in the audit database. However, the original audit files, which are typically compressed and archived to DVD or other inexpensive permanent storage, remain available in case a later investigation requires details that were filtered out during the loading process. Typical requirements are for one to five years of online audit data access, with permanent (or effectively permanent) archiving of the raw logs. Tasks can be set up to delete old audit records from the audit database periodically.

Viewing detailed audit logs

Users cannot see any audit data unless they are authorized to see it. However, like any other data in the system, reports can be configured generate audit log extracts, summaries, etc. When users search, examine and print log information, that process itself is audited.

It is possible to configure the security roles to give different auditing users access to different types of audit information. For example, some audit users might only be able to see login/logout and session information while others could see the full set of audit data. In our experience, however, most police agencies choose to grant all auditors full access to the logs to ensure that they have full information available to them when performing their investigations.

NicheRMS provides a standard set of auditing reports. Like all other system reports, additional reports can be configured as part of this project to meet your requirements. Reports can be exported in any format necessary, including to fielded formats like Microsoft Excel (if the reports are configured for this). Assuming the agency has the necessary software (e.g., Adobe Acrobat), reports can also be "printed" to PDF.

Searching and reporting on system activity

The NDS application servers automatically record full audit log data. As we have described above, this information includes all operations performed by all client applications, which include individual users, as well as all interfaces (both server and client based). Niche provides an audit log viewer that allows an agency to audit the system for troubleshooting, identifying users or areas of functionality where more training might be required (e.g., same errors appearing multiple times), or identifying unauthorized use (e.g., users looking up information unrelated to their current assignments).

Once the log files have loaded into the audit database, users with the appropriate security roles can search, explore, and report on the log information through the Audit Log Viewer (ALV) functionality in the NicheRMS Desktop app. See below for examples from the search tool provided by the ALV. For example, an auditor can search to find:

- Who logged in and when.
- What they searched for.
- What records they viewed, created or modified.
- What fields they edited, what they printed, and so on.
- When a particular data item changed, and who changed it.
- All searches carried out for a particular name.
- Batches that generated errors or that contain error messages returned by the server.

Record-level timestamping

When a record is created or modified in the system, it is timestamped and tagged with the identity of the user who created or modified it. All users can see this information and use it as a quick check to see when a record was created and when it was last modified, and by whom. Because this feature does not provide any history, other than creation and last modification, these timestamps are only of limited use from a security standpoint. However, they can be used to determine that a database record was created five years ago and has not been modified since, which indicates that the data is intact without further, more complex investigation. It can also be of use in day-to-day record keeping to check if, and when, a record was modified.

Operational logs

Operational logs are recorded in the database. Unlike the audit logs, the purpose of these logs is to support police operations and evidentiary requirements, not system security. The operational logs are meant to be viewed, printed, *etc.*, by normal users in the course of their day-to-day work. Note that all activities recorded in the operational logs are also represented in the audit logs, which provide the definitive record of all activity on the system. The operational logs in NicheRMS include:

- **Incident event logging:** A select set of events is recorded in the database for each Incident. The log of these events provides a history of the work that has been done on an investigation and can be used to understand the history and state of an investigation.
- **Task logging:** A log of task actions is recorded for each task in the system. This history can be used to determine when the task was created, who it was assigned to, when it was reassigned, completed, marked for rework, *etc.*
- **Custody logging:** A log of all activity and status changes for persons in custody.
- **Property and vehicle event logging:** Every action performed on a piece of property, including adding it to the system, checking it into stores, moving its location, *etc.*, right through to final disposal, is logged in the database. Each piece of property has a list of actions performed on it, which is used to meet continuity of evidence requirements.
- **Line-up creation:** A detailed log of photo line-up creation is maintained in the database. The purpose of this log is to provide evidence of how the line-up was assembled, including the search parameters for distracter images in a line-up containing a suspect, which distracters were selected, which were rejected, *etc.* The log is associated with the line-up and can be viewed and printed as required.
- **Witness viewing logging:** If photo line-ups are viewed online by witnesses, a detailed log of the witness's actions is recorded in the database, including when and how long a witness looked at each image, which images were rejected, which were marked as possible matches, *etc.* The purpose of this log is to provide evidence of how the witness viewing session was conducted and what the witness determined during the process. The log is part of the witness viewing session, which is associated with the photo line up being viewed and the witness.

Additional feature: Search hit and Notify if flags for investigation of unauthorized use

In addition to our auditing system and Audit Log Viewer, Niche provides a set of flags that can be set on any type of record in the database. The flags can be used to generate notifications when the flagged records are searched, viewed or modified in certain ways. This can be very useful for monitoring access to particularly sensitive information, such as the arrests of prominent persons. More information on flags is provided with our responses in RMS Attachment 1 – Functional Requirements.

Requirement: Interoperability				
Req. No.	Req. Status	Requirement Description		
T7	M	<p>The technical requirements for interoperability shall address issues of connectivity among systems, data and file exchange, and other communication related scenarios. The Contractor shall propose a solution that supports interoperability using open standards where available. The Contractor’s response to this requirement shall address, at a minimum, the following:</p> <ul style="list-style-type: none"> • Any limitations to interoperability in their solution; • Strategy for achieving interoperability with the Contractor’s proposed system; • Explanation of how the Contractor is looking ahead and supporting any research efforts to address interoperability challenges that are not presently realized amongst RMSs and components; • Detailed model or diagram of the proposed solution’s system architecture, noting whether each component or service utilizes an open standard or not. If it supports an open standard, list the supported open standards. If the component or service does not support an open standard, explain why it does not. If nothing is noted, NYS will assume that the system and services are NOT fully open and interoperable. For each component and service, identify if third party commercial software will be utilized and identify the particular product. 		
Provide a comprehensive description of how the proposed solution satisfies the requirement including technical specifications, capabilities, features, considerations, constraints, and limitations. Reference additional pages, if necessary. Indicate if the solution is offered or not offered →			Offered <input checked="" type="checkbox"/>	Not Offered <input type="checkbox"/>
Niche Technology response: see our response material immediately following this table.				

Niche Technology response – Interoperability

Overview

As a company, we concentrate on developing and supporting our core COTS product, NicheRMS. Every NicheRMS installation project requires interfaces and integrations with other systems, so an important part of this is to support customers and third-party developers who want to develop interfaces and extensions to NicheRMS. We do this by using common, open technologies, by providing APIs and integration hooks in the application and by providing technical assistance and test facilities. This has resulted in a product that is easy to integrate with and highly interoperable.

Support for requirements

The technical requirements for interoperability shall address issues of connectivity among systems, data and file exchange, and other communication related scenarios. The Contractor shall propose a

solution that supports interoperability using open standards where available. The Contractor's response to this requirement shall address, at a minimum, the following:

Any limitations to interoperability in their solution;

Every NicheRMS project requires interfaces and integrations with other systems, and we have a standard, proven approach for providing reliable interfaces in a cost-effective way. We approach system interfaces as follows:

- Niche provides some interfaces to widely-used systems. These have been developed as out-of-the-box NicheRMS interfaces that are available to customers as part of the standard software package, e.g., interfaces to CAD systems. We do not license out-of-the-box interfaces separately, although third parties may license their part of the interface.
- For interfaces to local systems that an agency may require, we provide the NicheRMS system API and web services toolkit at no cost. Such interfaces are agency-specific and may be developed by an implementation partner or the agency's in-house IT team.

Our system is developed to support interoperability with other systems based on the use of proven, mainstream tools and technologies. All of these technologies are used routinely in mission-critical environments around the world and are well supported, well tested and well understood by a broad range of software developers, security experts and IT staff in general.

For more on our approach to interfaces and integrations, please see the material provided in our Supplementary material section below.

Strategy for achieving interoperability with the Contractor's proposed system;

NicheRMS provides the following in support for interoperability and operational requirements:

- **Application layer:** uses NDSConnect (proprietary), an extensible Web service using HTTP or HTTPS, SMTP, others as required by external systems.
- **Session layer:** TLS (when using application-level encrypted sessions), any other VPN tunneling protocol that supports transparent TCP connections.
- **Network/transport layer:** TCP/IP for all user client and interface communication, TCP/UDP for communication between the NDS application servers.
- **Media layers:** Any media layer that supports the required network layer is acceptable.

For more details, see Key software technologies on page 37, below. For a deployment architecture diagram, see the Deployment architecture section on page 38.

Explanation of how the Contractor is looking ahead and supporting any research efforts to address interoperability challenges that are not presently realized amongst RMSs and components;

We have extensive experience working with agencies and third parties to develop and deploy interfaces to NicheRMS. To support this, we provide an interface toolkit that can be used by agency IT personnel or third-party suppliers to build and implement interfaces. It is delivered as a standard part of the NicheRMS system and we work with our customers to extend the system's interoperability as the challenges arise. Niche reviews and/or writes queries to extend NicheRMS interface functionality when necessary, and provides support via e-mail, phone and web conferences.

We support third-party developers who are creating interfaces to NicheRMS, and provide a web-accessible NicheRMS test system, configured like the agency's target system. This allows the developers to do their work from their development offices instead of relying on access to an agency-supplied NicheRMS test system.

In some cases, a hybrid approach is used, where we develop the NicheRMS facing side of an interface and agency IT staff or third party developers develop the target system facing side of the interface. Because each party deals primarily with the system that they understand, have access to, and may be able to modify if required, this approach can be very effective.

In addition, the NicheRMS database is a standard relational database that can be accessed by BI and crime analysis tools. This information is all available for reporting using the ILP/Analytics tools provided within NicheRMS, by exporting this data to third-party analytical packages. Our existing customers are using a wide range of third-party tools to provide analytical and reporting outputs from NicheRMS data: these include the i2, Business Objects, Cognos tools and Palantir.

Detailed model or diagram of the proposed solution’s system architecture, noting whether each component or service utilizes an open standard or not. If it supports an open standard, list the supported open standards. If the component or service does not support an open standard, explain why it does not. If nothing is noted, NYS will assume that the system and services are NOT fully open and interoperable. For each component and service, identify if third party commercial software will be utilized and identify the particular product.

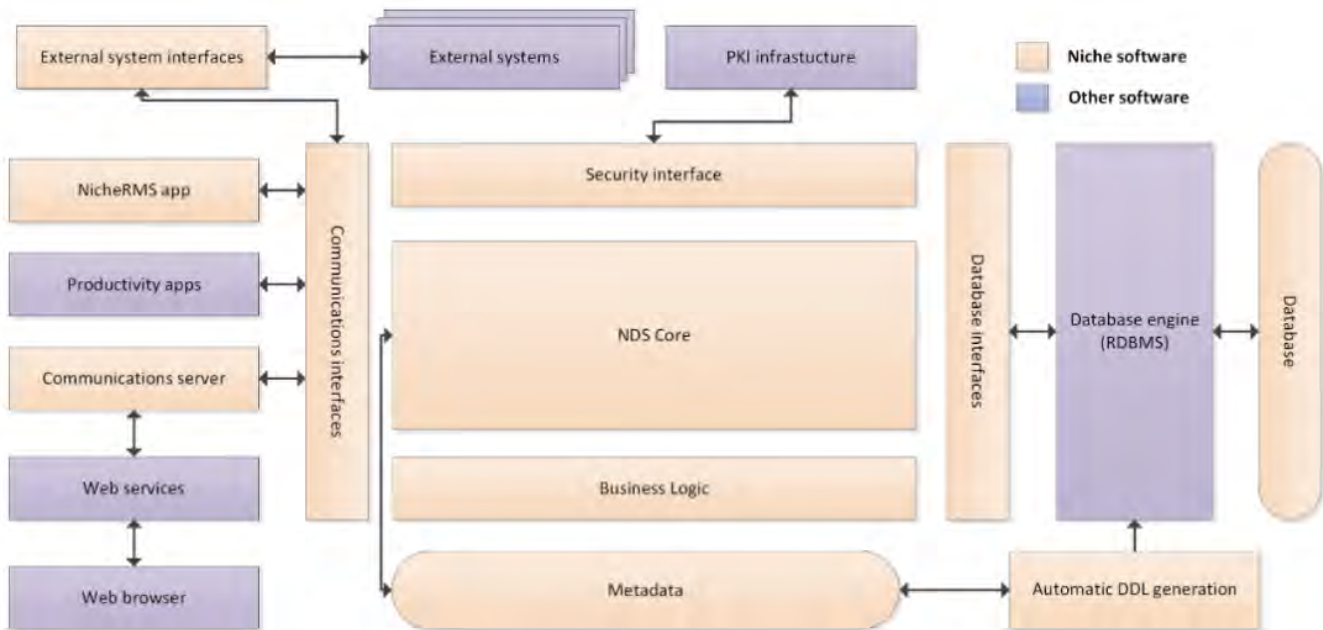
NicheRMS system architecture supports open standards. Interfaces to external systems can be completely managed using Niche-supplied APIs to communicate with the NDS application servers or through a Web service that communicates with the NDS application servers.

This is managed within the overall system architecture, which is a single n-tier application with a single relational database. While it is convenient to describe and discuss functional areas of the NicheRMS system as separate components or “modules”, it is actually a single software application with no internal horizontal interfaces. That is, the tiers for presentation, application and data storage communicate with each other via the network, but the modules/functional areas do not – they are part of a single application.

This is a key advantage because it means that once an item of data or report has been entered, it is instantly available to any other functional area that requires it, with no internal interfaces or duplication of data. For example, data and reports added to an Arrest are automatically available to Incident records via linking, and will be automatically included in Filing packages when it comes time for case preparation. The diagram below provides a simplified illustration of the logical parts of the NicheRMS solution and how they are connected.

Our approach ensures 100% internal data consistency with full transactional integrity. It does not require internal interfaces that add complexity and reduce reliability. A single security model is applied uniformly across the entire system, ensuring that there can be no inter-module inconsistencies leading to data breaches.

Also see *Supplementary material: Interoperability with Niche* (immediately below).



Supplementary material: Interoperability with Niche

Every NicheRMS project requires our system to communicate with other systems, often many other systems. We have a proven, standard approach for providing reliable interfaces and integrations in a secure, cost-effective way.

Niche's approach to interface development

Effective integration is critical for efficient agency-wide processes, such as minimizing repetitive data entry and maximizing ease of use, quality and efficiency.

We have extensive experience working with police agencies, partners and third-parties to develop and deploy interfaces to NicheRMS.

To assist with this, we provide the NicheRMS Interface Toolkit at no additional cost. It is designed to support development of interfaces to local systems that an agency may require. If an agency does not have its own in-house developers, we support third-party developers or other implementation partners in creating interfaces to NicheRMS. Niche reviews and/or writes queries to extend NicheRMS interface functionality when necessary, and provides support via e-mail, phone and web conferences.

As further support for partners who are creating interfaces to NicheRMS, we provide an Internet-accessible NicheRMS test system, configured like the agency's target system. This allows the developers to do their work from their development offices instead of relying on access to an agency-supplied NicheRMS test system.

In some cases, a hybrid approach is used, where we develop the NicheRMS facing side of an interface and customer IT staff or third party partners develop the target system facing side of the interface. Because each party deals primarily with the system that they understand, have access to, and may be able to modify if required, this approach can be very effective.

In addition, NicheRMS uses a standard relational database that can be replicated and accessed by BI and crime analysis tools. Our existing customers are using a wide range of third-party tools to provide analytical and reporting outputs from NicheRMS data. These include i2, Business Objects, Cognos tools and Palantir.

Interface options

NicheRMS has a highly functional and flexible interfacing capability that can be used to create interfaces with third-party systems and applications. There are several different ways in which systems can exchange data with NicheRMS in real or near real-time.

Interface classifications

The fundamental classifications are (always from the point of view of NicheRMS):

1. An outgoing “push” interface where NicheRMS sends its data to the other system. A push interface may be automatically triggered by changes to NicheRMS data or may be manually triggered by a user action. Example: an interface that sends a Filing package to a Prosecution system.
2. An outgoing “pull” interface, where the interfaced system requests data from NicheRMS, usually to satisfy a request from one of its users. Example: a CAD system interface used to provide CAD users with person or location details held by NicheRMS.
3. An incoming “pull” interface, where NicheRMS requests data from the interfaced system. Example: An interface that queries NLETS or other information exchange system.
4. An incoming “push” interface, where the interfaced system sends data to NicheRMS based on its own internal trigger mechanism. Example: A CAD interface that sends open and/or completed CAD events to NicheRMS.

Niche supports numerous varieties of all of these types of interfaces in production at many different customer sites.

Types of interfaces supported

Interfaces can be set up to perform any action that a user can, and are subject to the same role-based access control security. Specifically, interfaces can be in any of these forms:

- **A Web Service client** that accesses NicheRMS via Niche-supplied Web Service.
 - We provide a standard SOAP-based web service that includes a set of commonly used methods that are suitable for most interfaces. The web service is easily extensible by Niche, by the agency or by third-party developers, if necessary, to provide additional services.
 - The web service is pre-configured with standard search and data retrieval functions and can be extended (by Niche or a third-party) to provide access to all NicheRMS functionality.
 - This web service can be integrated with enterprise service bus components.
- **XML interfaces:** NicheRMS uses XML extensively for interfaces with other systems.
- **A Niche-supplied API** can be used to access the NDS application servers over a TCP/IP connection. This approach provides maximum flexibility and performance but results in more coupling between the interface and NicheRMS. This interface-building approach has been used by Niche, customer agencies, and third parties. API bindings for C/C++ and .NET are available.
- **.NET client plug-ins** that interact locally with the desktop/mobile client application and have full access to NicheRMS facilities as well. Some agencies have used client plug-in functionality to build interfaces that provide interactive simultaneous access to NicheRMS and other systems, include legacy systems as part of migration.
- **Direct backend database access to the separate reporting database** – this is used for some statistical reporting processes, ETL processes and other bulk data extracts. This access is always read-only and normally through database views that are configured to provide security (e.g., excluding data filtered out by ACLs) and reduce coupling to the underlying NicheRMS database. Direct backend

database access is performed against the separate reporting database to ensure interactive performance of the production NicheRMS application database is not affected.

Interface toolkit

Niche's Interface Toolkit provides the necessary DLLs, documentation and sample programs (in source code form) to build interfaces to the application layer (NDS) in any Windows language (using the "extern C" calling sequence) or in any .NET language (.NET-specific APIs) and to the client app using any .NET language. It also provides APIs for accessing the Niche metadata (data model).

We also support a configurable, extensible Web service that can be used to build interfaces from any platform. Niche supplies a supported set of Web service functions that correspond to the common search and data retrieval operations performed by the client app. Additional Web service functions can be added as required by Niche, the customer or a third party.

Whenever the interfacing facilities are extended or there are customer or third-party questions regarding interfacing, the Interface Toolkit is extended so that the new features and enhanced documentation is available to all interface developers.

Data publish interface

The Interface Toolkit includes the components required to build a robust *publish interface*. This is an interface that reacts to changes in the NicheRMS data and publishes the changes to the interfaced system. A typical application is to mirror information from NicheRMS to a central state or national repository for investigative or other purposes. The publish interface implements the following features:

- Database triggers that queue data for publishing or deletion when it changes in the NicheRMS database. The triggers are automatically generated based on a set of parameters that specify which data is to be tracked and how the data changes are to be aggregated for each interface. For example, a particular interface may consider a change to a person's address to be a change to the person, so the trigger would behave accordingly and queue the person record for publishing when the address changes.
- A queue and queue reader that combine multiple publish requests for the same record into a single request. The publish process is normally configured with a five-minute delay to allow time for multiple repeat requests to appear in the queue so that they can be combined.
- An extract process that takes the data in the database corresponding to the queued publish requests and converts it to the form required by the remote system.
- A comparison process that tracks published data (in the form of a hash of the published field values) so that data that has not changed is not re-published.
- The actual publish process that interacts with the remote system, typically through Web service calls.
- A slow crawl process that works its way through the NicheRMS database and attempts to publish every record. The comparison process discards any attempts to re-publish already-published information.
- The Niche data publish components in the Interface Toolkit are used by Niche developers to build a functioning data publisher capable of reacting to customer-specified changes in the NicheRMS database. Either Niche developers, or customer or third-party developers can complete the development of a fully-functioning publish interface by adding the necessary publish command generation, data transformation and communications features to the interface.

The slow crawl also un-publishes published information that is no longer available for publishing, assuming the target system supports removal of published information. This is very important as it allows data to be un-published even if no changes have occurred in the database. Some reasons that data might have to be un-

published include passing a non-disclosure date or changes to the NicheRMS security roles that make a record that was previously visible to the publishing process invisible, and therefore not for publication. The slow crawl can also be used to perform the initial publish for a new interface.

Developers who need to build a publish-style interface have the benefit of getting all of these features without doing additional work. The main development task is to define the transformation of the NicheRMS data into the form required by the target system and to transfer the data to that system.

Information exchange protocols

NicheRMS can support essentially any data exchange method or protocol. Most modern interfaces are Web service-based and use XML as the low-level data format. Niche prefers to use broadly adopted standards such as NIEM to help with interface and code reuse. However, other standards are also supported, such as NIST for interfacing with LiveScan systems.

Information exchange with other systems via file sharing is not significantly different than the interface development described above. The same tools, processes, development roles, etc. are used no matter what the actual data transport process is. An example of a NicheRMS interface that is often file-based is the CAD interface (CAD data to NicheRMS).

The content of the files is usually XML, NIST or some other key/value pair format, CSV or a fixed width column file format. Most NicheRMS interfaces contain a stage where the data is put in XML format. This allows XSLT and other transformation tools to be used to perform any data translations independent of the actual file format.

The actual file transfer usually takes place via a Windows (or other) file share, or via FTP. In some cases, there is a specific protocol with data and trigger files to establish two-way communication through file shares. LiveScan interfaces use this approach.

Requirement: Proposed Solution Architecture: Hardware and Software							
Req. No.	Req. Status	Requirement Description					
T8	M	<p>The Contractor shall provide a detailed description of its overall architectural solution in its proposal including, but not limited to, the following:</p> <ul style="list-style-type: none"> • Depiction of interfaces to external systems and communications topology, understanding that the New York State Information Technology Services (NYS ITS) will host the computing platforms; • Approach to supporting mobile computing capabilities (e.g., in an officer’s automobile) including off-line computing and automated re-synchronization when system is available; • Approach and objectives for keeping the software solution current with supporting software elements. This would include operating systems, database, programming languages, browsers, etc. Include objectives for how soon the proposed solution will be certified for use with updated technologies. 					
Provide a comprehensive description of how the proposed solution satisfies the requirement including technical specifications, capabilities, features, considerations, constraints, and limitations. Reference additional pages, if necessary. Indicate if the solution is offered or not offered →			<table border="1"> <tr> <td>Offered</td> <td>Not Offered</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </table>	Offered	Not Offered	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Offered	Not Offered						
<input checked="" type="checkbox"/>	<input type="checkbox"/>						
Niche Technology response: see our response material immediately following this table.							

Niche Technology response – Hardware and Software

Overview

NicheRMS is a single n-tier application with a single relational database. While it is convenient to describe and discuss functional areas of the NicheRMS system as separate components or “modules”, it is actually a single software application with no internal horizontal interfaces. That is, the tiers for presentation, application and data storage communicate with each other via the network, but the modules/functional areas do not – they are part of a single application. For a comprehensive overview of our overall architectural solution, please see the supplementary material provided below.

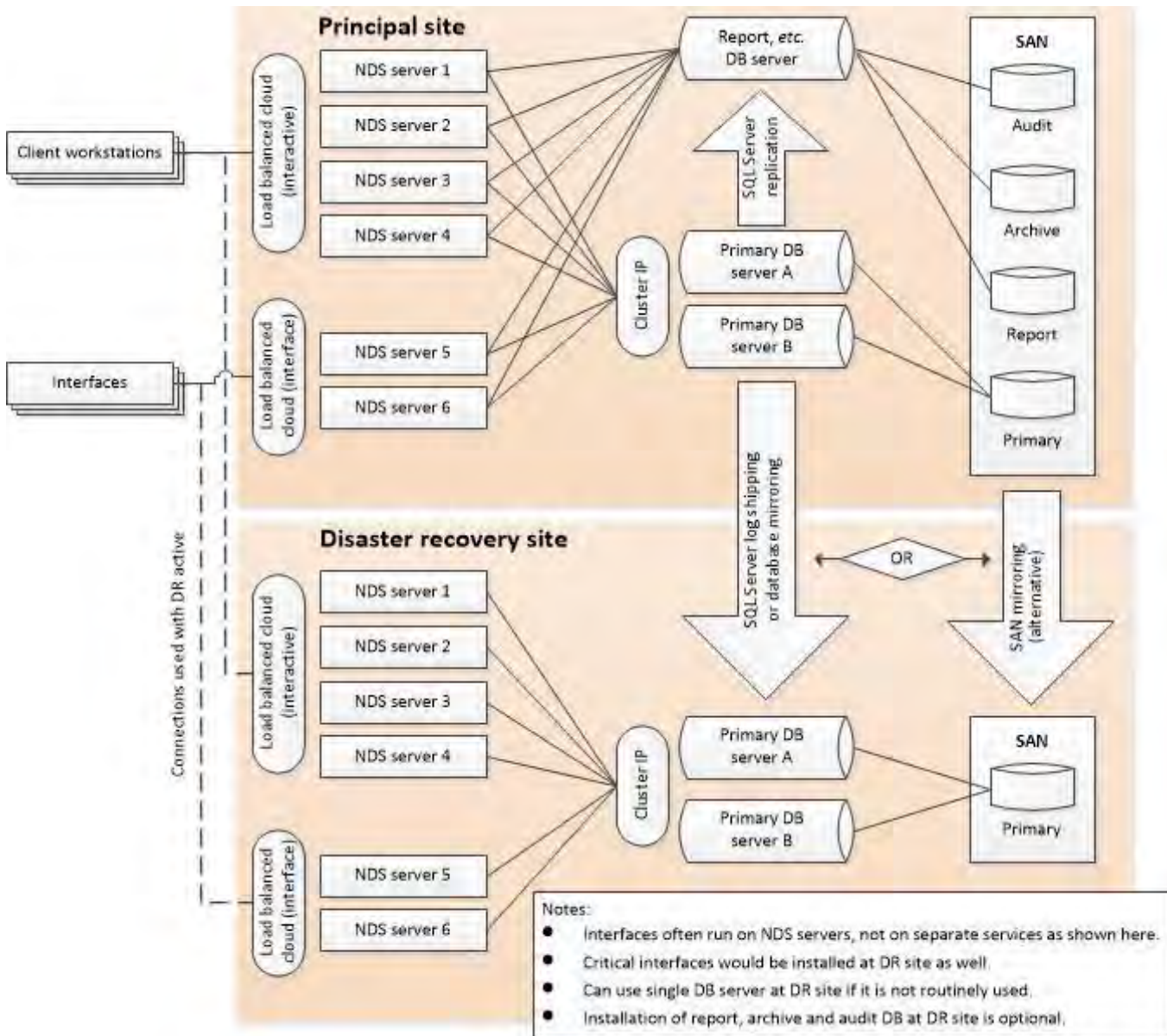
Support for requirements

The Contractor shall provide a detailed description of its overall architectural solution in its proposal including, but not limited to, the following:

Depiction of interfaces to external systems and communications topology, understanding that the New York State Information Technology Services (NYS ITS) will host the computing platforms;

Interfaces are managed within our standard system architecture, where interfacing is accomplished by using Niche-supplied APIs to communicate with the NDS application servers or through a Web service that communicates with the NDS application servers. There is generally no direct access to the backend database. This ensures that business rules and security are respected by all parts of the system.

Specialized Niche or third-party user interfaces and client applications can use the APIs or Web service to access the system. See below for a diagram. Also see our detailed system architecture overview provided in the Supplementary materials section below.



Approach to supporting mobile computing capabilities (e.g., in an officer’s automobile) including off-line computing and automated re-synchronization when system is available;

NicheRMS provides all police RMS functions within the same seamless, integrated system. We provide a native Windows application with a standard user interface (UI) that is consistent across all Windows devices.

Mobile use: The NicheRMS Universal app can be installed natively on a range of Windows OS devices (Windows 7, 8.1 and 10), including PCs, laptops, tablets, notebooks and touchscreen combination devices. Any modern commercial 3G/4G/LTE will provide ample bandwidth to support the NicheRMS app. This will allow all users access to the system whether they are in an office, a patrol vehicle or other mobile location.

Connectivity for mobile users

NicheRMS tolerates low bandwidth, high latency 3G/4G mobile networks. Any modern commercial 3G/4G/LTE network provides ample bandwidth to support the NicheRMS app.

NicheRMS is tolerant of mobile latency and latency jitter: Mobile networks have different characteristics than WAN networks. While bandwidth tends to be lower, the critical difference is latency: mobile networks have higher overall latency and exhibit latency jitter (*i.e.*, most of the time latency is moderate, but severe latency spikes occur during periods of low signal strength).

- The NicheRMS app communicates with the NicheRMS server through a relatively small number of highly compressed transactions. Between transactions, users interact with locally cached data, providing instant interactive response. This means that users are less affected by latency jitter than users on a Web app or using a Remote Desktop Protocols (RDP)/Citrix session.
- By contrast, a Web or RDP/Citrix session is much more “chatty” and requires more bandwidth overall, so the user experience is severely degraded by latency jitter and low bandwidth conditions.

NicheRMS is tolerant of disconnections: In addition to latency jitter, mobile sessions regularly experience a complete loss of connection for an extended period. NicheRMS resumes normal operation once the network connection is re-established, with no loss of work in progress, and no need for the officer to manually reconnect in order to resume their work.

Network bandwidth requirements depend on how the system is used. For basic use, 33kbps per active user (typically 10% of logged in users) has been found to be sufficient. Clerical staff require more bandwidth because they usually work faster than officers. Access to large images, scanned documents and Word forms dramatically increases required bandwidth.

The requirements for NicheRMS access from mobile computers in cars are the same as for other desktop or laptop workstations. The difference is that mobile work is usually less intensive (more time spent driving, slower typing due to worse ergonomics, no mobile clerical staff) and there is less need to access large scanned documents and forms.

It is difficult to determine how many large documents will be accessed by users without more information about how the New York State will use the system. However, some rough bandwidth estimates for scanned documents can be made:

- A scanned document requires 50KB to 100KB per page.
- If a 10-page document (say 750KB) is to be retrieved in three seconds, a bandwidth of approximately $750\text{KB} \times 10 \text{ bits/byte} / 3 \text{ seconds} = 2.5\text{Mbps}$ will be required (10 bits per byte is used due to overhead).
- If a user takes 5 minutes to read/process the 10-page document (and therefore will not retrieve another document for 5 minutes), then $5 \text{ minutes} \times 60 \text{ seconds/minute} / 3 \text{ seconds retrieval time} = 100$ users can share the same 2.5Mbps connection (assuming they don't all try to retrieve a document at the same time and can tolerate longer retrieval times if they happen to overlap another user's operation).

To illustrate how scanned documents and forms can dominate bandwidth requirements, and why bandwidth cannot be accurately determined until we understand your workflow, that same 2.5Mbps bandwidth could support over 750 “normal” users who access only RMS data without documents.

Offline use

Our standard NicheRMS app has an offline mode that allows officers to add reports while using a Windows OS device in situations where no network connection is possible, *i.e.*, the same app supports both online and offline work. Reports entered while offline are uploaded when officers return to a network-accessible location. Incoming data is validated as part of the import process.

Offline operation (by definition) does not provide central live database inquiry functions; however, standard data entry work is still possible. When the central database is available, data entry operations minimize data entry effort by reusing all possible information already held about persons, locations, vehicles, *etc.* This means the user is searching for existing entity records during data entry processes, reviewing the information on file, and then updating or entering information as required. By contrast, during offline operation, the user needs to enter all information (since they don't know whether the information is already in the system).

NicheRMS also provides a separate mobile forms application, the NicheRMS Offline app. It provides officers with offline data entry forms, which are then synchronized with the database. This application allows officers to add and fill in reports while in a disconnected mode when operating in locations where no network or internet connections are available. When the network becomes available, the officer can upload their completed forms to the NicheRMS database. The app can be run from any Windows-compatible PC or laptop, in any patrol car or field situation, and is subject to the same CJIS-compliant security as the rest of the RMS product.

Approach and objectives for keeping the software solution current with supporting software elements. This would include operating systems, database, programming languages, browsers, etc. Include objectives for how soon the proposed solution will be certified for use with updated technologies.

Access to a continuously-evolving product

Niche Technology's COTS model includes a renewal process aimed to prevent the system from ever falling into a legacy state. Our concept is of an evergreen product continually being refreshed and developed. This allows our customers to avoid the high cost and disruption of RMS replacement every few years. We do not recognize the concept of a finite life for our product, as some other COTS suppliers do. We seek to continuously improve our product to meet our customers' evolving needs.

As a product, NicheRMS is tremendously configurable and extensible: it provides an extensive set of configurable features that allow a custom fit for each customer in terms of language, UI terminology, reports, interfaces, field options, validation rules, user permissions, *etc.* When we provide upgrades and new features, we provide them in a way that customers can install without losing their custom configurations. This means that each of our customers can run the current version of NicheRMS and take advantage of new features and technologies (evergreening). At the same time, the product will continue to support agency-specific configurations and needs.

All our customers are running the current version of NicheRMS, including customers who first started using the system 18 years ago. As our first large customer, the OPP/OPTIC consortium are a primary example of how this approach can work very well for a large customer.

Customers can install upgrades without losing any existing features or function. No customer is required to install a new update if they don't want it, but this does not block them from installing other updates in future. New features are controlled using parameters—this means that a particular new feature can be turned on or off depending on whether or not you want to use it.

All Niche customers benefit from regular software enhancements, leading to system longevity. As part of our SLA, Niche typically aims for a major version release every 12 to 18 months. New releases include functional enhancements based on:

- Commitments made to new customers during the procurement process
- Features requested by existing customers
- Features required to support legal changes
- Features that take advantage of new technology

Smaller patches are issued on an as-needed basis, for example for bug fixes and updates required by changes to laws and regulations. Niche has a well-developed process for delivering and implementing patches and new

versions, including tools that automatically perform synchronized updates of installed NicheRMS apps on widely dispersed workstations, notebooks, etc.

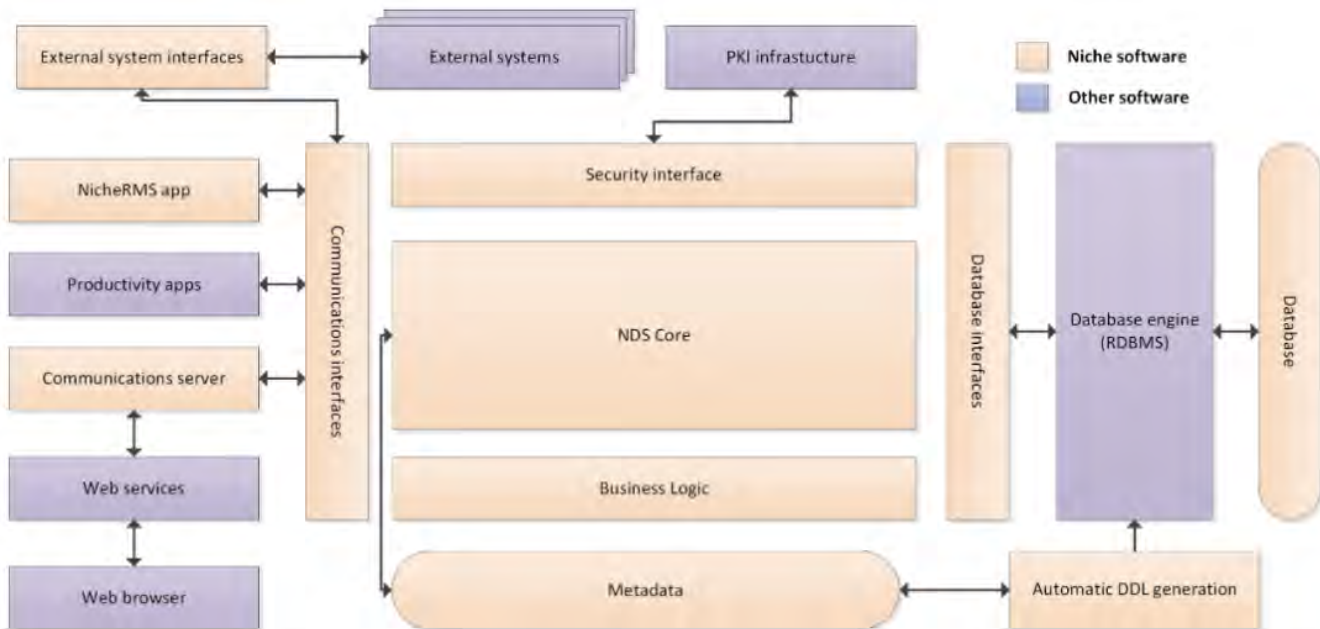
Regarding costs, all upgrades are made available to all Niche customers as part of our standard warranty and maintenance package, so there will be no additional costs for the software itself. If there are likely to be additional costs associated with an upgrade (e.g., new functionality that requires specific hardware, such as signature tablets or barcode readers), Niche informs the customer well in advance.

Supplementary material: NicheRMS System Architecture

NicheRMS is a single n-tier application with a single relational database. While it is convenient to describe and discuss functional areas of the NicheRMS system as separate components or “modules”, it is actually a single software application with no internal horizontal interfaces. That is, the tiers for presentation, application and data storage communicate with each other via the network, but the modules/functional areas do not – they are part of a single application.

This is a key advantage because it means that once an item of data or report has been entered, it is instantly available to any other functional area that requires it, with no internal interfaces or duplication of data. For example, data and reports added to an Arrest are automatically available to Incident records via linking, and will be automatically included in Filing packages when it comes time for case preparation. The diagram below provides a simplified illustration of the logical parts of the NicheRMS solution and how they are connected.

Our approach ensures 100% internal data consistency with full transactional integrity. It does not require internal interfaces that add complexity and reduce reliability. A single security model is applied uniformly across the entire system, ensuring that there can be no inter-module inconsistencies leading to data breaches.



Physical and logical organization of the data in NicheRMS

NicheRMS uses an object-oriented data model based on Yourdon-Coad methodology. Key features of the architecture include:

- The object-oriented *application data model* is described by the Niche Metadata Language (NML), which controls both client applications and the NDS application server.

- All application logic deals with the object-oriented application data model, which is automatically mapped into a database-level relational data model by NDS.
- Clients (NicheRMS Universal app, NicheRMS Desktop app, Interfaces, *etc.*) interact with NDS using *Niche Application SQL*. This language is similar to standard SQL, but differs in many significant ways (further documentation available on request).
- The NDS middleware submits database-level SQL queries to the backend relational database to retrieve and modify data required to satisfy both client and internal requests.
- NDS enforces business rules, data integrity checks and data security.

Key software technologies

Our flexible, high-performance architecture supports large-scale, mission-critical environments. It is based on the real world experience we gain by supporting our existing large police installations. The NicheRMS architecture uses industry standard technologies and tools:

- Operating systems supported:
 - Microsoft Windows 7, Windows 8.1 and Windows 10
 - Microsoft Windows Server 2008, 2008 R2, 2012 and 2012 R2
- Database server: MS SQL Server Enterprise Edition 2008/2008 R2, 2012, 2014 or 2016
- Hardware: Intel x86, x64 or equivalent
- Web server: Microsoft IIS
- Web service: Standard SOAP based Web service, developed in .NET
- Network communications: TCP/IP (IPv4 and IPv6)
- Productivity tool integration: Microsoft Office
- Security technologies: Entrust, Kerberos (Microsoft Active Directory integration), TLS, encryption supported by Microsoft Cryptographic API.
- Interface technologies – client: .NET assembly plug-ins, hyperlinks, DDE
- Backup tools: any tool that works with Microsoft SQL Server
- Interface technologies – server: API with “extern C”, C++ and .NET bindings (can be called from any Windows programming environment); SOAP Web service (can be used from essentially any environment).

As evidenced by the list above, NicheRMS uses only proven, mainstream tools and technologies. All these technologies are routinely used in mission-critical environments around the world and are well supported, well tested and well understood by a broad range of software developers, security experts and IT staff in general. This has resulted in a product that is easy to integrate with and highly interoperable.

Hosting options

NicheRMS can be hosted in a customer data center, either on physical servers or on virtual servers. NicheRMS systems are in production using both approaches, and also using a mixed approach (virtual servers for the NDS application servers, physical servers for the database). Relevant notes:

1. Most installations of NicheRMS worldwide are hosted on physical servers, located at police agencies' own sites.
2. Many Niche customers are now moving to virtualize the servers at their own sites. Niche has worked with a number of customers to virtualize the middleware (NDS) servers. When the system is to be run

on virtual servers, it is important to use the same virtual server specifications (number of cores, memory) as would be used for physical servers.

3. A number of Niche customers use servers that are fully hosted at sites other than the local police agency, for example the OPTIC group of 43 municipal agencies in Ontario, Canada, where the central servers for all agencies are hosted by the Government of Ontario in one data center.
4. NicheRMS is also hosted in commercial datacenters for the PSNI (Northern Ireland) and the East Midlands (UK) consortium.

Any of these approaches will work for New York State, and all have predictable costs. The decision on the model to use depends on IT staff technical expertise, availability of data center space, pricing from suppliers and financial constraints (e.g. operating vs. capital budgets).

Cloud-based technologies

NicheRMS can be used in an IaaS cloud-based setting. We have two US customers who are deploying in production to Azure using IaaS. Other customers have test systems running in Azure, and we have our own demo system running in an Azure cloud. We can provide more information on this on request. Note that in all cases, the system will be operated by the New York State or a third party. Niche does not operate or manage the system.

Infrastructure responsibilities

NicheRMS is in production use in multiple large installations. Ongoing monitoring of those installations has helped refine our hardware capacity calculations. We have provided you with a specification that we believe will meet your needs based on our in-house capacity testing and on our experience with police RMS installations similar in size to the New York State. For details see page 67.

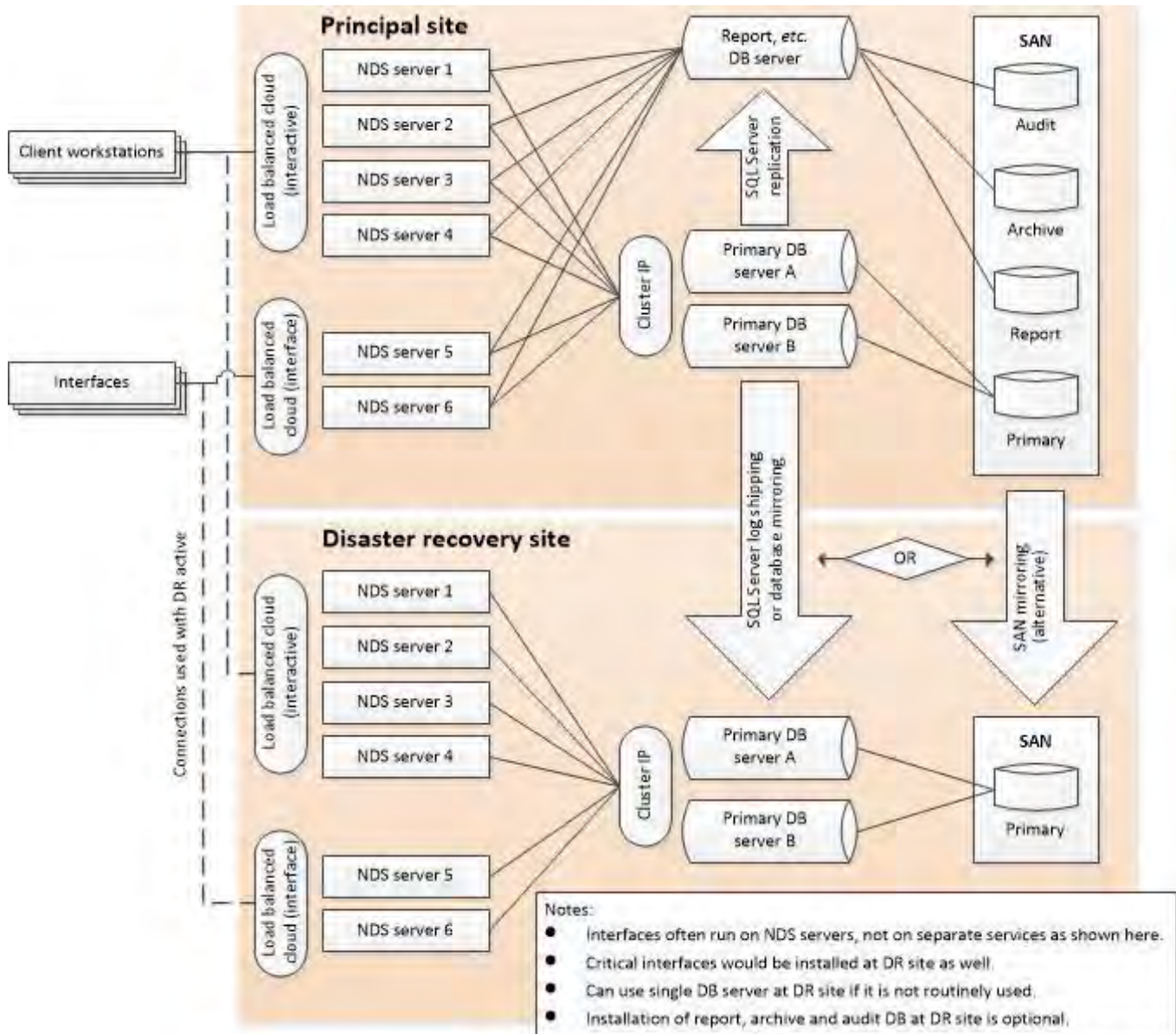
We recommend that you house and run the system in your own data center(s). New York State staff or contractors will install the hardware and load the software, and New York State staff will be responsible for operating and maintaining the system. NicheRMS uses commodity hardware and widely-used Microsoft operating systems and database servers. This makes it easy to find or train staff to operate and maintain the system. This is the model used by most NicheRMS customers.

Note there should not be substantial unexpected costs associated with increasing capacity if Niche's hardware and software recommendations are followed. If an incremental implementation approach is used, it may be possible to start with less than the recommended capacity, but the future need for additional capacity will not be unexpected.

Deployment architecture

NicheRMS is designed to be flexible. As we have said, the system is an integrated n-tier client/server system with proper separation of storage, business logic and presentation. The core application modules are a fully integrated system; they are not a suite of separate applications held together by interface "glue". The diagram below shows a typical NicheRMS deployment with a reporting server and a remote disaster recovery location.

Our system is specifically designed to support large police agencies, and contains the required configuration, management and monitoring features to support reliable operation in large installations. NicheRMS supports a variety of different server configurations, including virtual server (VMWare or Hyper-V) technology. As an early part of each Niche implementation project, we assist you to design your server infrastructure to support the required load, resilience and functionality, and to maximize fit in the existing police agency computing environment.



The system is partitioned as follows:

1. Data storage is managed by a relational database (Microsoft SQL Server).
2. Application logic, business rules and security are managed by Niche Data Server (NDS).
3. Graphical user interfaces are provided by client applications (e.g., NicheRMS Universal app). Client applications only communicate with the database via the NDS application server. There is no direct connection to the database.
4. Interfacing is accomplished by using Niche-supplied APIs to communicate with the NDS application servers or through a Web service that communicates with the NDS application servers. There is generally no direct access to the backend database. This ensures that business rules and security are respected by all parts of the system.
5. Specialized Niche or third-party user interfaces and client applications can use the APIs or Web service to access the system.

Standard NicheRMS system components

NicheRMS database

NicheRMS uses a Microsoft relational database server for data storage and retrieval. Microsoft SQL Server 2008 R2, 2012, 2014 and 2016 are the supported platforms for new NicheRMS projects. The database server can be installed in a failover cluster and/or with a remote disaster recovery site. Multiple databases (typically on separate servers) can be installed for reporting, archiving and audit log analysis. These additional servers help to reduce the load on the primary server, which is particularly important in large installations.

Direct access to the backend database is limited to data extracts and some complex analytical reports. Some Niche-supplied data import processes (e.g., import of address verification data) also operate directly on the backend database.

Niche Data Server (NDS)

The *Niche Data Server* (NDS) is the core of the system. NDS:

- manages all front-end communication with the client applications,
- enforces security and business rules,
- executes business logic, and
- communicates with the backend database.

All client applications (e.g., NicheRMS Universal app, specialty clients, custom front ends) must access the system through NDS, ensuring that security, logging and business logic are uniformly enforced. Similarly, external system interfaces must also access data through NDS, either via the SOAP-based NicheRMS Web service or directly using a Niche-supplied API. Because all client applications and interfaces use the same mechanism to access data through NDS, all the application services available to users through a client are also available to interfaces, Web service clients or any other interfaced application.

NDS processes requests from client applications and makes the necessary calls to the database to satisfy them. It then returns data, updates the database or performs other operations as required. Because NDS handles all requests from both client applications and interfaces, security and business rules are applied uniformly no matter what the source of the request. NDS produces audit logs that track all client and interface activity. Some client requests cause NDS to use external system interfaces to exchange data with other systems.

NDS is usually installed on a set of load-balanced servers, providing both load distribution and redundancy. Load balancing can be provided either by network appliances or Windows Network Load Balancing (NLB).

The entire system (clients, NDS and database) is defined, configured and controlled by the *metadata*, which contains the system data model augmented with information used to control the behavior of the different parts of the application. The metadata is also used to configure the system to suit the needs of different police agencies.

Location of business rules and logic

All business logic, data validation and security reside in the NDS application server, which is used by all user clients and interfaces. This ensures uniform enforcement of security and business rules across the system.

Some data validation is performed in client apps in addition to the server, e.g., picklist options, edit masks and date validation. This provides users with immediate feedback if they enter invalid data, without incurring the cost of a round trip to the server. However, the server still performs final validation to ensure that no client or interface can insert invalid data.

Business rules are loaded at run-time along with the user security roles, and can be changed at any time by authorized police IT personnel. System administrators can view and edit business rules from within NicheRMS, and Niche provides information on how to do this as part of the knowledge transfer that takes place during the implementation project. This allows the customer to quickly modify user role permissions and data validation rules and activate them immediately.

End-user clients/user interfaces

NicheRMS Universal app

The NicheRMS Universal app is the primary NicheRMS UI for mobile devices and desktop workstations. Its UI reconfigures itself based on the user device display size, touchscreen capability, physical keyboard or onscreen keyboard, *etc.*—this is part of Niche’s “train once, use anywhere” approach—users get a familiar look and feel whether they’re using NicheRMS from a mobile device or full desktop workstation.

NicheRMS Desktop app

The NicheRMS Desktop app is used in a desktop environment and provides administrative and management functions that are not required by general users, *e.g.*, auditing, administration of reports, business rules, charge definitions, incident types, *etc.*

Specialized apps

Niche also supplies specialized applications, such as a Bulk Document Loader for loading large numbers of scanned or faxed documents, or PDFs, into the NicheRMS database, and attaching them to database records. Other in-house developed and third-party apps can also be used to access the system.

Public access via the Internet

Citizen reporting and similar online reporting can be provided by commercially available third-party systems. Many of our customers are currently using the Coplogic DORS system with an interface to import citizen report data into NicheRMS. This interface can be adapted for each police customer and can accept data from Coplogic’s DORS or any similar system.

Virtualized access for Web browser access

In addition to the Windows OS devices that are used to run NicheRMS clients natively, the NicheRMS UI can be delivered to user workstations or mobile devices via Citrix, Microsoft RDP or other thin client technology (*e.g.*, HTML5 RDP). NicheRMS can be used on almost any device for which a Citrix receiver, Remote Desktop (RDP) or other virtual client technology is available. This includes iOS, Android devices, *etc.*

Third-party apps

Niche provides integration facilities that allow customer or third-party apps and interfaces to be developed. Like the Niche clients, these communicate with the system through the Niche NDS servers and are subject to all security and business rules.

Requirement: Proposed Solution Architecture: Reporting			
Req. No.	Req. Status	Requirement Description	
T9	M	The Contractor shall provide a detailed description of its overall architectural solution in its proposal including, but not limited to, the following: <ul style="list-style-type: none"> • Approach to reporting including, but not limited to, ad hoc, advanced report authoring, and export of data. • Approach to support accessibility for reporting, business intelligence, and data warehousing. 	
Provide a comprehensive description of how the proposed solution satisfies the requirement including technical specifications, capabilities, features, considerations, constraints, and limitations. Reference additional pages, if necessary. Indicate if the solution is offered or not offered →			Offered <input checked="" type="checkbox"/>
			Not Offered <input type="checkbox"/>
Niche Technology response: see our response material immediately following this table.			

Niche Technology response – Reporting

Overview

NicheRMS provides all data in a single integrated database, and all the data in the database is available for reporting. The system comes with a standard set of 350+ built-in reports. As part of the project, Niche configures existing reports for each customer, and adds new reports based on specific customer requirements.

The application provides extensive functionality for customers to create and manage their own reports within the system. In addition to standard options for creating and using reports, users can generate ad hoc reports using the search results from any detailed search. If there are particular searches that return results that need to be reported on regularly, these can be set up to run automatically and deliver the results to specified persons. Agencies can also run ad hoc queries directly against the database using SQL or third-party tools.

Support for requirements

The Contractor shall provide a detailed description of its overall architectural solution in its proposal including, but not limited to, the following:

Approach to reporting including, but not limited to, ad hoc, advanced report authoring, and export of data.

Niche’s output report definitions are loaded and stored in the NicheRMS database. NicheRMS comes with 350+ standard output reports that can be used as is or updated to meet customer requirements. These are reports that can be generated based on standard report parameters, for example to produce an Incident summary report from an Incident record, or a summary report of arrests in the previous 48 hours.

Users can also generate ad hoc reports by running a search (e.g., all master index Person records that meet a set of user-selected criteria) and generating a report based on the results. All reports can be generated and printed, or generated and saved to an electronic file suitable for export, such as an HTML file, XML or PDF.

Niche provides documentation and training that allows customer personnel to become self-sufficient in adding and maintaining output report templates. NYSP personnel can define custom output reports using the XSLT

format. Output report definitions are stored in the NicheRMS database, and define the set of data to be generated from the database. From an end-user point of view, these custom output reports are available from NicheRMS report menus and they behave exactly like standard output reports.

Existing reports (whether Niche-provided or custom) can be added, removed, modified or replaced without changing any underlying program code or restarting the system. Niche provides training, samples and technical support that will allow the agency to manage these processes. This allows customer agencies to extract whatever data they need from the database, formatted in any way necessary, and make the report available as a standard option for end users.

Approach to support accessibility for reporting, business intelligence, and data warehousing.

The NicheRMS database is a standard relational database that can be accessed by business intelligence and crime analysis tools. In addition to standard options for viewing and printing search results, NicheRMS data can be exported into other file formats for use with third-party analytical tools to generate charts and graphs from the assembled data. Our existing customers are using a wide range of third-party tools to provide analytical and reporting outputs from NicheRMS data: these include the i2, Watson, Business Objects, Cognos tools and Palantir.

In order to prevent the load created by BI/intelligence queries or related processes from affecting interactive performance, the installation can be set up to replicate data from the live NicheRMS database to a Reporting Server. This is a replicated version of the live NicheRMS against which BI and analysis tools are run. NicheRMS data can also be extracted from primary database or replicated reporting database, to a data warehouse and then queried using commercial BI and crime analysis tools.

Supplementary material: Reporting

NicheRMS provides a single, integrated, fully searchable database and a set of output reports that are directly useful for operational police reports and for crime analysis/ analytical support. Data entered into the NicheRMS database as part of everyday operations becomes part of a police force's integrated data repository with no additional user effort. Many reports can be generated directly from the NicheRMS database, as we show in our examples below.

NicheRMS comes with standard output reports that can be used as is or updated to meet the requirements of the NYSP. NicheRMS output reports:

- Generate sets of data that are directly useful for crime analysis / analytical support, with no further processing required.
- Are defined in XSLT, a standard reporting language, which export NicheRMS data into formatted output suitable for printing or export. Reports can be previewed electronically, printed or emailed.
- Can be configured to generate a variety of formats, but they normally produce HTML, which is displayed to the user in a Web browser window. The HTML can include hyperlinks that navigate back to data in the system, making these reports interactive.
- Are created and added prior to system go-live. However, your agency personnel can add, update and end-date these reports at any time before or after go-live. Niche provides documentation and training that allows customer personnel to become self-sufficient in adding and maintaining output report templates.

Report automation

NicheRMS includes a Report Runner utility that schedules standard reports to run at predetermined dates and times, *e.g.*, daily, weekly, *etc.* Reports produced by the Report Runner can be automatically emailed to a predefined email list. No programming is involved.

Sample output reports provided by Niche Technology

Niche provides a number of built-in output reports, and customers can define and add their own output reports in XSLT. Features to note:

- Users can generate reports interactively by selecting report options from a menu.
- NicheRMS includes a Report Runner utility that can be used to schedule standard reports to run at predetermined dates and times, *e.g.*, daily, weekly, *etc.* Reports produced by the Report Runner can be automatically emailed to a predefined email list.
- Reports can be generated and printed, or generated and saved to an electronic file such as an HTML file, XML or PDF.
- Reports may be directly useful as generated; they can also be exported to a file format suitable for import into a third-party analytical software package.

Operational Reports	Management Reports	Employee Management
<ul style="list-style-type: none"> • Alert summaries • Court summaries • Criminal record summary • Pending charge summary • Witness statement/will say • Arrest/Custody reports • Missing person report • Sudden death report • Victim report • Ident/fingerprint report • Witness viewing summary • Person photo/Photo lineup • Subject profile • Fraudulent document report • Use of Agency report • General incident report • Supplementary report 	<ul style="list-style-type: none"> • Incident summaries • Incident statistics • UCR incident statistics • Crime statistics • Hazardous person summary • Person summary • Hazardous addresses • Juvenile non-disclosure summary • Arrest summaries • Prisoner statistics • Fingerprint reports • First court appearance report • Property seizures • Property stolen/recovered 	<ul style="list-style-type: none"> • Employee ID card • Employee case load • Employee charge analysis • Unit/section case load • Unit/section charge analysis • Department case load • Department charge analysis

Link visualization

NicheRMS provides an integrated Link visualization report. It displays a graphical representation of the links between a selected record and the records to which it is linked. The resulting interactive view allows the user to specify what they want to see, and in what scale.

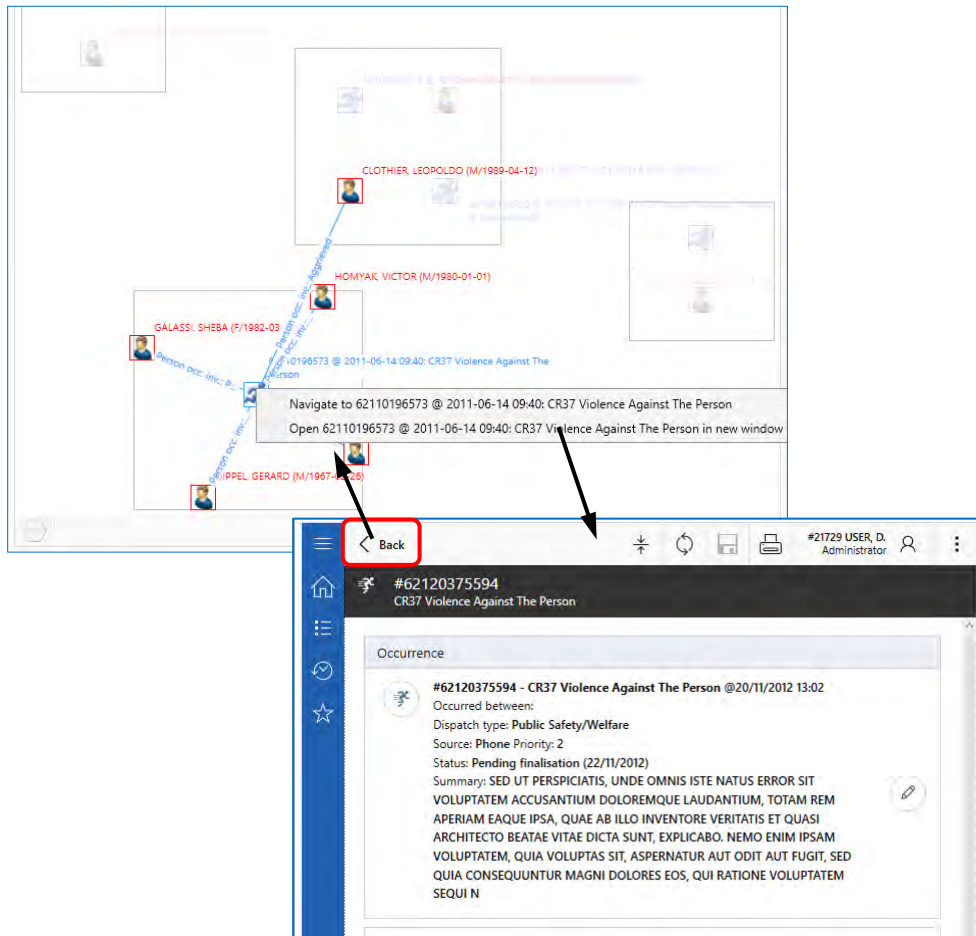
This feature is available directly from any Incident or other event-level record where an analyst wants to check connections between database records. It can also be generated from a list of search results. The user can specify what types of links to include, and the depth (*i.e.*, the maximum number of links from the initial record) to be displayed. The generated report also includes interactive options in for adjusting labels, nodes visibility, scale of the visualization, *etc.*

The image displays two overlapping windows from the NicheRMS application. The top window, titled "NicheRMS : Link visualization", features a left-hand navigation pane with various icons and a main area for configuring the link visualization. It includes options for printer selection, paper size, language, and depth (set to 2). There are also checkboxes for including different types of links (person, address, vehicle, property) and people, and a "Perform dead-end elimination" option. The bottom window, titled "NicheRMS : Report result", shows a network graph of entity records. Nodes are represented by small icons and are connected by lines. A legend on the right side of this window identifies the node types: Intelligence/stop check (red), Occurrence (blue), Person (green), Property (purple), General vehicles (orange), and Address (yellow). The graph shows a complex web of relationships between various records, with some nodes highlighted in red, indicating they are the current focus of the report.

The NicheRMS link visualization shows entity records as labelled nodes, with lines between them to show how the records are linked. Users can select any record in the diagram to see the identity of the record, direct links from that record to other records, and the link type of each direct link. In the next example below, the user started with a person, Leopoldo Clothier as the center for the link visualization. From here the user can see what other incidents this person has been linked to, as well as what has been linked to those incidents. The graphic nodes show the record type, which has been limited to incidents and persons for this report, and the lines between the nodes show the nature of the relationship. The user can select any node to view further details.

Selecting any record in the view causes the image to refocus on the selected record, though it does not reset the initial record. Right-clicking a record in the view opens a menu, allowing the user to open the selected record in this window or in a new window.

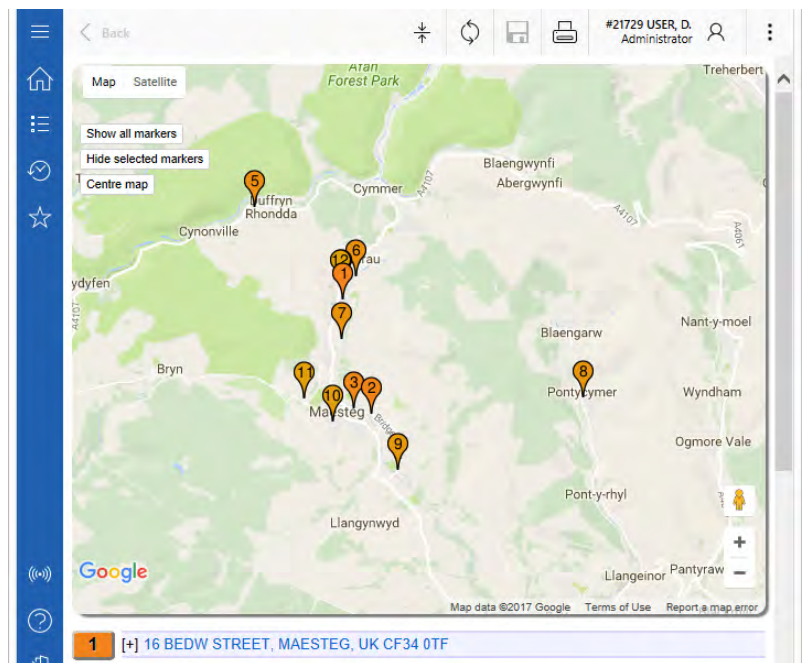
Users can select a record from the visualization and drill down to see details of reports, log entries and briefings on that record. In the example below, once the user has clicked the option to navigate to the selected incident, the user can click the **Back** button on the incident to return to the visualization.



Mapping from a set of search results

In addition to standard reports, NicheRMS provides mapping and link analysis tools that can be used directly from the list of search results. For simple analysis, such as pin mapping of incident locations, people, users can generate the necessary views of the information directly from a set of NicheRMS search results.

NicheRMS can access external address validation sources or load map data into the internal address validation engine, using an integration with the GIS/mapping software of your choice. On the right we show an example where a user has run a search for Motor Vehicle Collisions that match a particular profile (e.g. accidents resulting in injury or death). The user can use a menu option to immediately view the results on a heat map or pin map:

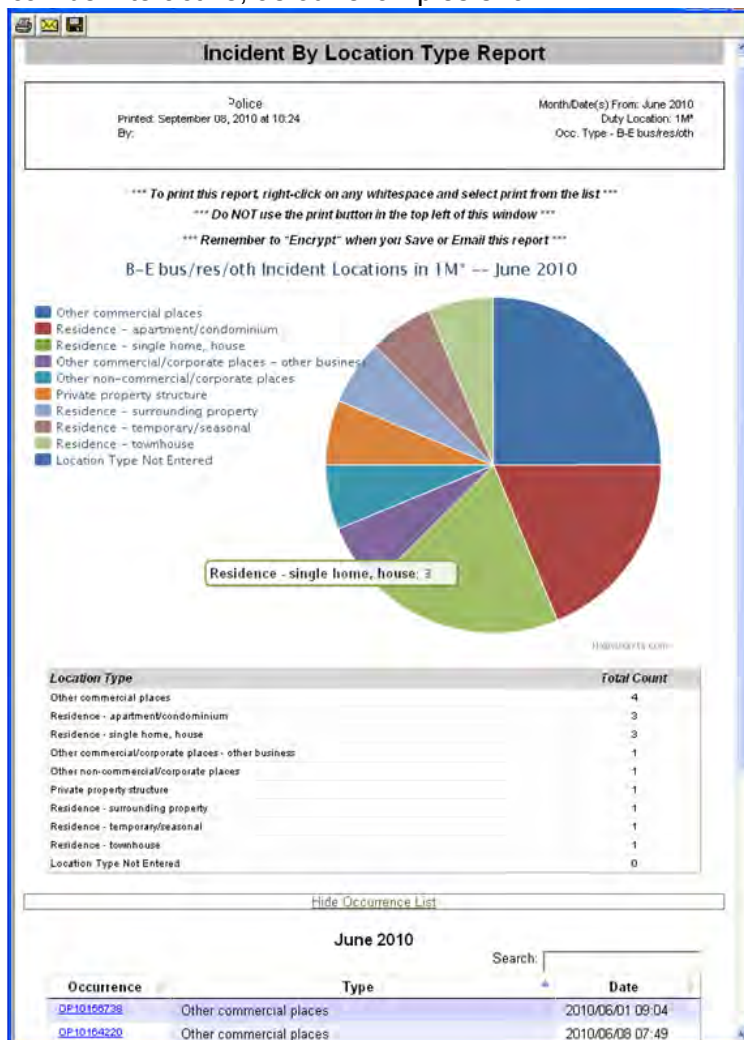


Custom output reports

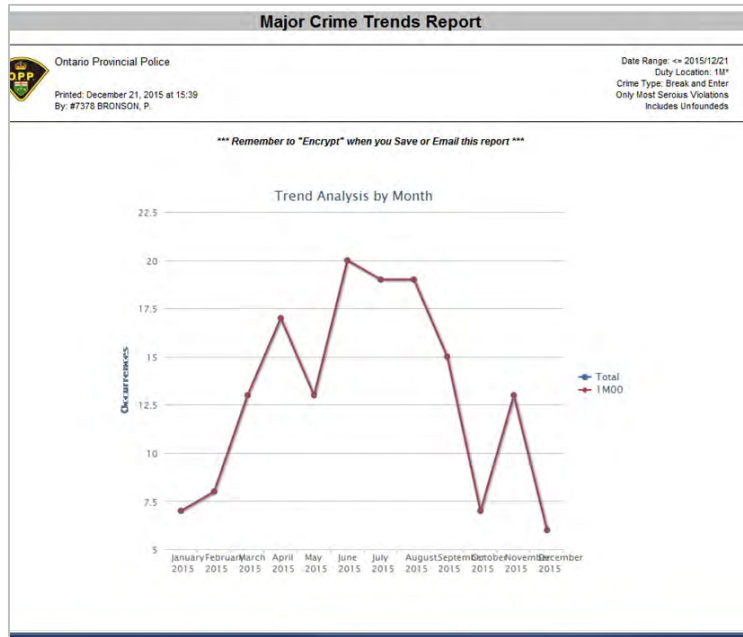
NYSP personnel can define custom output reports using the XSLT format. Output report definitions are stored in the NicheRMS database, and define the set of data to be generated from the database. From an end-user point of view, these custom output reports are available from NicheRMS report menus and they behave exactly like standard output reports.

Existing reports (whether Niche-provided or custom) can be added, removed, modified or replaced without changing any underlying program code or restarting the system. Niche provides training, samples and technical support that will allow the Agency to manage these processes. This allows customer agencies to extract whatever data they need from the database, formatted in any way necessary, and make the report available as a standard option for end users.

The following screen shots show examples of customer-created reports that are being run directly from NicheRMS. These reports can be interactive, as our examples show.



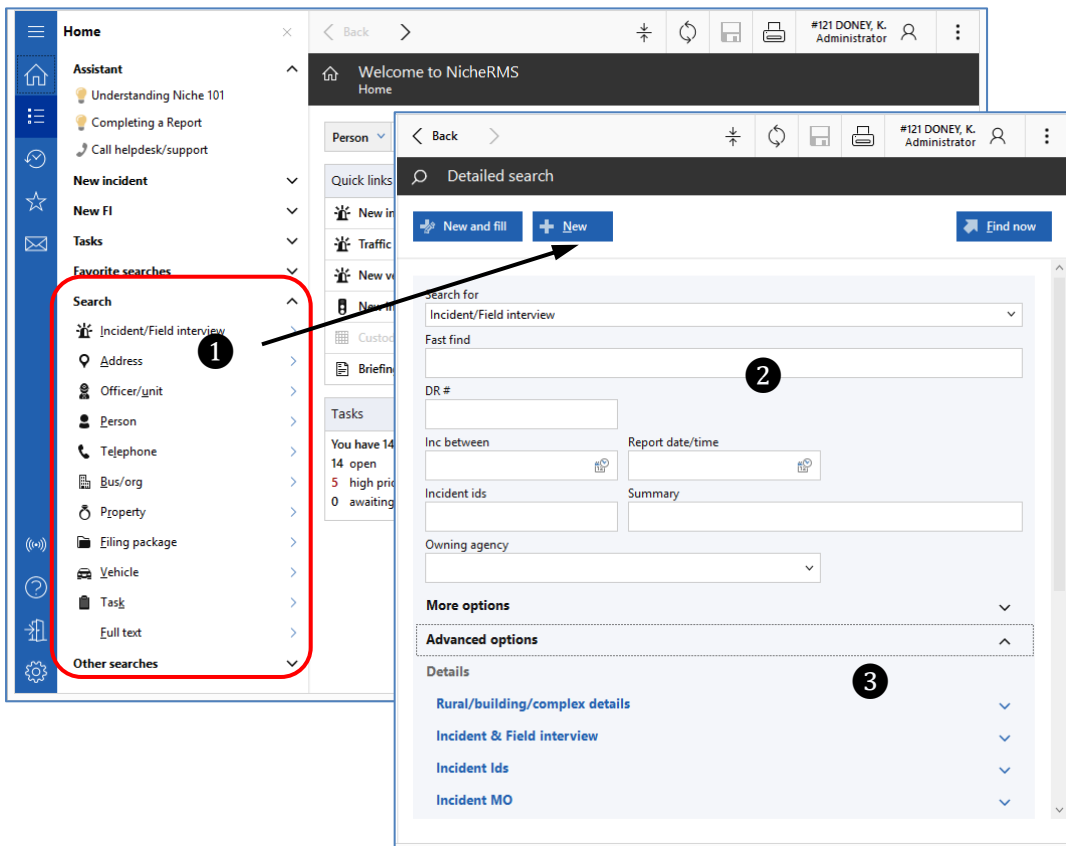
This customer uses a number of reports that an analyst can run to quickly identify trends, for example, the following “Major Crime Trends” report, which has a number of grouped UCR combinations as well as an option to select any single UCR code and review the current trend for that code(s).



Ad hoc reporting based on search results

The Navigation side panel in the NicheRMS Home view provides options for searching the NicheRMS database (1). Briefly:

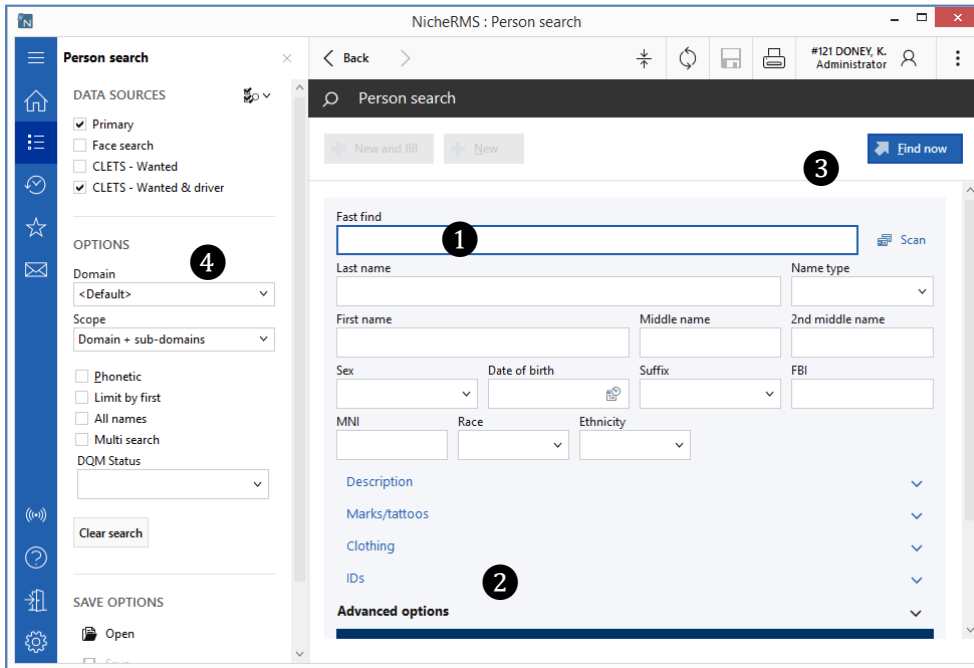
- Users click or tap a search option to display options for searching for a particular data type. For example, Incident/Field interview runs displays a view for running searches for Incident and Intelligence/Field Interview records. Person allows you to search for master index person records, etc.
- Each search view provides a **Fast find** field (2) for running a quick unstructured search, in addition to multiple advanced options (3), useful for performing the more structured searches required by analysts.



There is a separate search view for each NicheRMS record type. NicheRMS search views provided advanced options that allow users to search for a set of records by selecting structured data in multiple fields across multiple entities. For example, “Motor Vehicle Collisions in the past 30 days for Beat SP12.” When used in this way, NicheRMS searches provide analytical support with no further effort required.

NicheRMS provides search options for all record types. Our example below shows a Person search. Starting from the Home view, the user would start by clicking or tapping an option in the *Search* section of the sidebar.

When you display a *Search* view, it provides a **Fast find** field (1), and a set of fielded search options. Additional advanced search fields can be displayed by clicking a heading (2). The system provides a broad range of search criteria for generating sets of data required for reporting. Each type of search provides fields for the type of record you are looking for.



Users enter search details in the fields and click or tap **Find now** to run the search

- Use a **Fast find** search if you are looking for a specific record or you have a specific identifier, such as the person's name or an ID number.
- Search option buttons such as **Find now** are provided directly on the search view (3). Additional search options are available in the side panel (4).
- If you are unsure of the subject's name, but have other information about them, e.g., gender, date of birth, ethnicity, etc., enter that information in the fields below the **Fast find** field. The app provides even more detailed search options in the *Description*, *Marks/tattoos*, *Clothing*, *IDs*, and *Advanced search options* sections of the search view.
- Use **Advanced options** if the information you have is not specific enough to identify one particular record. Advanced searches are also useful for assembling a list of similar records based on multiple search fields. Click the heading to expand this section.

Search results are returned in a *Results* view that can be used to generate an ad hoc report. All users can run searches and select multiple records from a list of search results and immediately generate reports for display, export, emailing or printing. We have shown a generated statistical report below. Reports will be configured and added to meet NYSP requirements.

Analysts and other expert users can use these standard search options to generate and run complex queries against the NicheRMS database, and then use the results to generate output reports and data extracts. Users can print and export the set of search results for use in MS Excel or other external reporting tools.

The screenshot shows the NYS Law Enforcement RMS interface. The top navigation bar includes a 'Back' button, search filters, and user information for '#21729 USER, D. Administrator'. The main area displays search results for '6211012543' with 46 occurrence results. A detailed view of the occurrence is shown on the right, including 'Occurrence details', 'Involved persons', 'Involved addresses', 'Involved telephones/emails', 'Involved vehicles', and 'Involved property'. An arrow points from the 'Involved vehicles' field in the details to a Microsoft Excel spreadsheet below, which contains a table of search results.

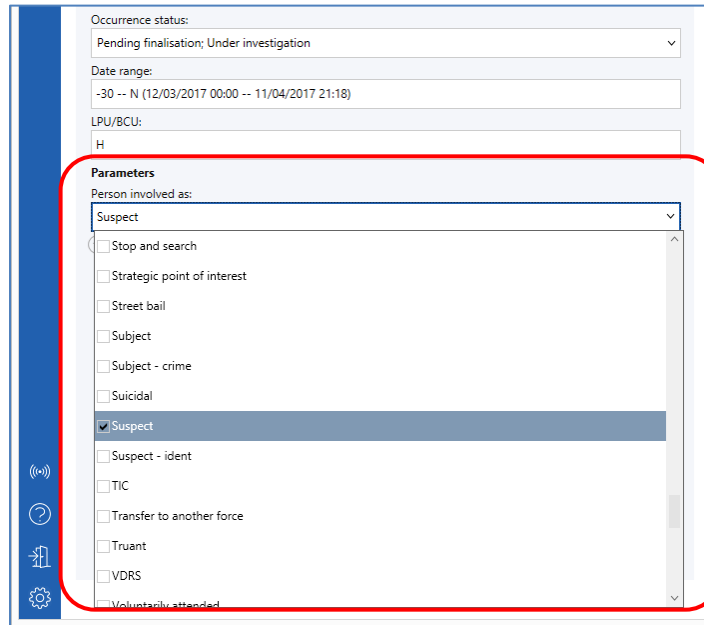
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1		Occurrence #	ORIS number	Reported	Occurrence	HO class	HO code	Outcome	Outcome	LPU	District	Beat	Street #	Street nar	City	Officer in	Officer
2	3	6211012543		5/4/2011	CR41 Thef	Theft of a 44	0	18: Investi	5/4/2011	H	UPLANDS	7601	4	LADY MAR	SWANSEA		
3	4	62110131709	20110093972	20/04/2011	CR41 Thef	Theft from 45	10	1: Chargec	25/04/2011	H	UPLANDS	7601	44	ALEXANDI	SWANSEA		
4	5	62110140971		27/04/2011	CR41 Thef	Theft from 45	10	18: Investi	27/04/2011	H	UPLANDS	7601	42	EDGEWAR	SWANSEA		
5	6	62110142198		28/04/2011	CR41 Thef	Theft of a 44	0	18: Investi	28/04/2011	H	UPLANDS	7601	19	DYFED AV	SWANSEA		
6	7	62110146127		1/5/2011	CR41 Thef	Theft from 45	10	18: Investi	2/5/2011	H	UPLANDS	7601	12	DYFED AV	SWANSEA		
7	8	62110148063		3/5/2011	CR41 Thef	Theft of a 48	1	18: Investi	3/5/2011	H	UPLANDS	7601	13	PENMAEN	SWANSEA		

Saved custom searches can be used to generate reports

Any search can be saved for re-use:

- Any user can set up their own searches using the standard NicheRMS searches and then save them for their own personal re-use in the future.
- Analysts, expert users and system administrators can create and save complex custom searches. The resulting saved search can be provided to specific users and units to run. When end-users load a custom saved search, all of the search fields appear in a single **Advanced search options** section, as shown in the example below, so they can simply select the options they want and click the **Find now** button.

The example below shows a custom search being used to search for Incident records based on incident status, date and time range, policing area and the involvement classification of persons linked to the incident. It has been saved and made available as a saved search for other users. Results will be returned as a list of links to incident records.

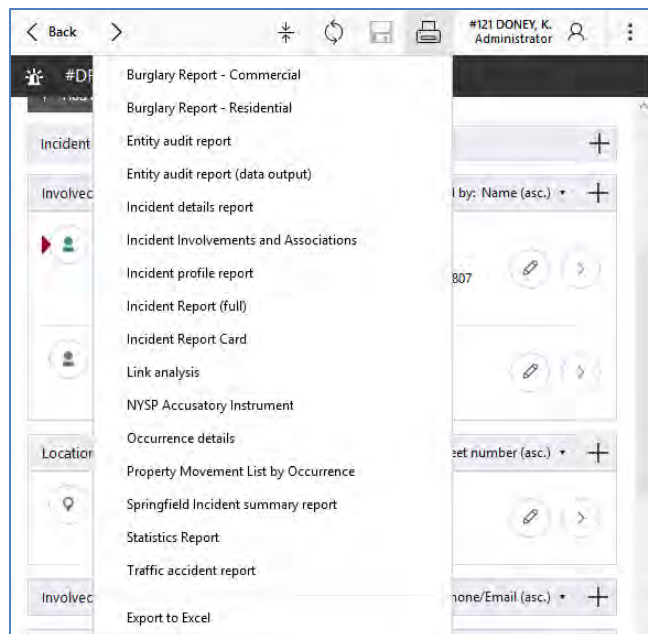


Generating and printing the reports

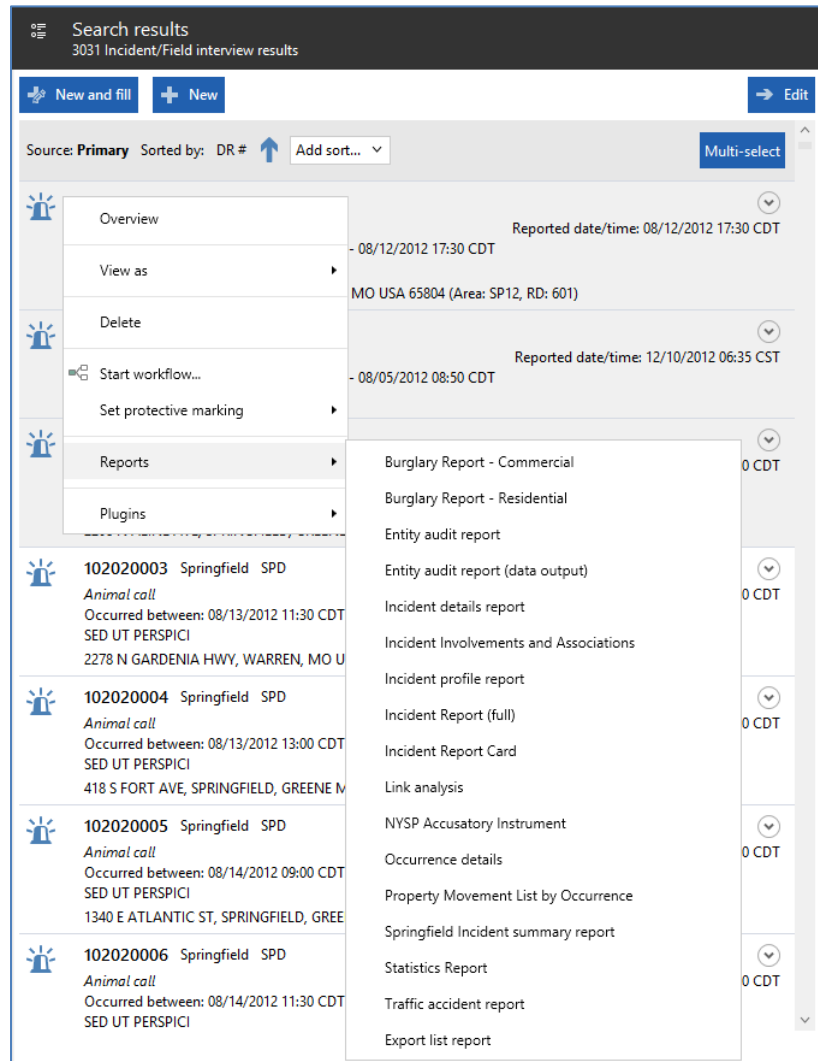
NicheRMS uses standard Microsoft printing, so printing works in the same way in NicheRMS as it does with other Microsoft applications. The system can print both text and images, separately or combined (*i.e.*, both attached photos and text reports that include images).

Users can click or tap the Printer icon in the toolbar to see a list of reports available for printing:

- The Home view provides summary report options.
- Individual Incident records and master index entity records list the output report options for that individual record.
- Users in different roles may see different report options.



- Users can also select one or more search results to generate reports based on those search results.



As we show in the example below, the print options window provides all of the standard Windows print options, in addition to some application-specific options such as Protective marking. Administrators can also set up custom output reports that allow users to select what data should be included in the report at the time of printing.

Another option is to save a NicheRMS report to a file. The user can then display or save the report in an XML format, so that it can be copied and pasted into different software for further manipulation.

Interaction with email systems

NicheRMS supports integration with MAPI-compliant email clients, such as Microsoft Outlook/Exchange for report output. This capability is available when generating output reports, allowing users to email (rather than print) report output. For certain reports, the application provides buttons or right-menu operations to assemble information and email it. NicheRMS also supports server-side integration with SMTP email servers.

The screenshot displays the NicheRMS interface. On the left, there is a sidebar with navigation icons and a list of filters such as 'Show occurrences:', 'Show occurrence IDs:', 'Show enquiry log:', etc. The main window shows a 'Report result' for 'Guernsey occurrence summary'. The report header includes 'Metropolitan Police', 'Printed: 30/07/2018 20:08:59 by 21729', and 'Occurrence: 0118000094'. Below this, the 'Occurrence details' section provides the following information:

- Report no.: 0118000094
- Dispatch type: Public Safety/Welfare
- Occurrence type: Domestic Incident
- Occurrence time: -
- Reported time: 29/03/2018 16:36
- Place of offence: 10 GLANYMOR ROAD, RUMNEY CARDIFF SOUTH GLAMORGAN, UK IR8 4VG (BCU: C, Section: TROWBRIDGE, Sector: CS, Beat: 3602)
- Source: Phone
- Priority: 3
- Clearance status: New
- Concluded: No
- Concluded date: -
- Summary: Police were called by a concerned neighbour
- Remarks: -

Management Information and Information Analysis

NicheRMS provides standard query and reporting tools that are useful both for operational officers – who may require this information for immediate operational use - and analysts, who need to search and collate data for use in identifying and analyzing trends, patterns and potential future crime. NicheRMS supports this by providing:

- A single, integrated, fully searchable database. NicheRMS uses a relational database server for data storage and retrieval. It is a robust, modern SQL server that provides consistent, secure access for system users and can be accessed by many business intelligence (BI) and crime analysis tools.
- A set of easy-to-use end-user data entry, search and reporting tools that are available out-of-the-box. Operational users have direct access to real-time data and can perform their own searches of this data, allowing police to make maximum use of all the data stored in the database. For example they can carry out a quick check of a person’s criminal history or review crimes associated with a particular location.
- The ability to export data into other data stores and formats for reporting. Agencies typically extract data from the primary database, or a replicated reporting database, to a data warehouse and then query it using commercial business intelligence and crime analysis tools. For more complex analysis of NicheRMS data, including sophisticated visualization, trend analysis and similar tasks, existing NicheRMS agencies are using a wide range of third-party tools such as the i2, Business Objects and Cognos tools.

Integrated database provides rich source for analysis

NicheRMS allows for a wide range of data to be stored and associated with incident and master index entity records. This data enters the system as users carry out everyday tasks to report on crime incidents and work on investigations—immediately providing a rich source of interconnected data. It is directly useful for identifying a subset of records that may be of interest to a particular officer or analyst.

Detailed searches can be set up very quickly using NicheRMS's standard search tools. Because the data is being collected and organized in a single integrated system, users can quickly set up a search to identify a subset of records that are of interest. For example, a search for females, aged 13-16, flagged as vulnerable, with an address in a specified policing area.

Some information is stored directly in the master indices. For example a master index Person record stores all of a person's known names and aliases, ID numbers and physical descriptions. Flags and Cautions can be added directly to this record, and users can store person-specific log entries and instances of police contact using a Person dossier that is linked to the Person record. Other data is added by linking the master index record to other records in the database. For example, Person records can be:

- Linked to Incidents and Intelligence/Field Interview records, with detailed involvement classifications. The system uses these links to automatically calculate repeat involvement information (repeat victim, repeat offender, *etc.*).
- Linked to arrests, charges and disposals and Filing packages.
- Linked to Addresses, Contacts, Vehicles, Property and Businesses/organizations (including criminal organizations and associates).

All of this data is available for searching and reporting, both by operational users and analysts.

Analytical support using third-party tools

The NicheRMS database is a standard relational database that can be accessed by BI and crime analysis tools. In addition to standard options for viewing and printing search results, NicheRMS data can be exported into other file formats for use with third-party analytical tools to generate charts and graphs from the assembled data. Our existing customers are using a wide range of third-party tools to provide analytical and reporting outputs from NicheRMS data: these include the i2, Business Objects, Cognos tools and Palantir.

In order to prevent the load created by BI/intelligence queries or ETL processes from affecting interactive performance, the installation can be set up to replicate data from the live NicheRMS database to a Reporting Server. This is a replicated version of the live NicheRMS against which BI and analysis tools are run. NicheRMS data can also be extracted from primary database or replicated reporting database, to a data warehouse and then queried using commercial BI and crime analysis tools.

Security

Standard security rules apply to all search results and generated reports. Users can only view and interact with the data that they are authorized for. If there is data that is protected based on role-based access or Access Control List (ACL) rules, users who are not authorized to view it will not be able to generate or find this information, even if they specifically query for it. Note that when records are restricted by way of ACL, all aspects of the record are restricted in the manner designed in the ACL. This means every link between any entity and an incident is restricted as well as the incident itself. This restriction includes all searching and reporting whether it be by way of a GUI search or an XSLT report search.

Requirement: Proposed Solution Architecture: Multi Tenancy					
Req. No.	Req. Status	Requirement Description			
T10	M	The Contractor shall provide a detailed description of its overall architectural solution in its proposal including, but not limited to, the following: <ul style="list-style-type: none"> • Approach to supporting multiple law enforcement entities in a single multi-tenant environment, including how the proposed solution ensures data integrity within specific law enforcement entities. 			
Provide a comprehensive description of how the proposed solution satisfies the requirement including technical specifications, capabilities, features, considerations, constraints, and limitations. Reference additional pages, if necessary. Indicate if the solution is offered or not offered →			<table border="1"> <tr> <td>Offered <input checked="" type="checkbox"/></td> <td>Not Offered <input type="checkbox"/></td> </tr> </table>	Offered <input checked="" type="checkbox"/>	Not Offered <input type="checkbox"/>
Offered <input checked="" type="checkbox"/>	Not Offered <input type="checkbox"/>				
Niche Technology response: see our response material immediately following this table.					

Niche Technology response – Multi-Tenancy

Overview

NicheRMS was originally designed for a very large, multi-tenant, multi-jurisdictional customer that included many individual agencies varying in size from large operations with hundreds of officers down to smaller detachments with fewer than 10 officers operating in remote areas. The system was built from the ground up specifically to support this type of multi-tenant use.

One of our first customers was a multi-agency, multi-jurisdictional cooperative called the Ontario Police Technology and Information Cooperative (OPTIC). Currently OPTIC has 43 agencies with a total of approximately 9,000 sworn officers. The agencies range in size from local police departments with five officers up to the Ontario Provincial Police with 6,500 officers. One of OPTIC’s requirements was configuration at the agency level because small agencies must do business differently than a 6,500-officer agency. Niche met this requirement. Since then we have supported a number of large multi-tenant installations in both North America and the UK.

Support for requirements

The Contractor shall provide a detailed description of its overall architectural solution in its proposal including, but not limited to, the following:

Approach to supporting multiple law enforcement entities in a single multi-tenant environment, including how the proposed solution ensures data integrity within specific law enforcement entities.

Niche Technology can support multiple law enforcement entities within the framework of a single multi-tenant NicheRMS installation. Data integrity is supported by providing each tenant/agency with its own separate domain. As we describe in our supplementary material below, data-sharing can be set up within this framework, with each agency able to determine what data they will share.

For more details, please see the overview provided below.

Supplementary material: Multi-tenant options in NicheRMS

NicheRMS supports multi-tenant installations – installations where multiple agencies or divisions within an agency are supported by a single instance of NicheRMS installation – as a standard feature. In this type of arrangement, data sharing options are managed using domains within the database for the installation. Agencies control which of their data is shared: sensitive data or data not pertinent for viewing by other agencies is classified during the course of everyday police work and can be automatically omitted from sharing using standard system security.

Note that in the description below, we use the term “agency” because the members of a multi-tenant installation are often agencies. However there may also be tenants within an agency, *e.g.*, divisions or units who require their own data domain because of size or the type of data they are dealing with, and this is also fully supported.

In a multi-tenant system, each agency/tenant is represented by a domain. Individual agency configurations are maintained individually within the larger installation – with agency-specific roles, workflow, system parameters, default field values, reports and other local rules and options. Niche's domain system allows for individual agency configurations within the larger installation – individual member agencies/tenants can set up agency-specific roles, workflow, system parameters, default field values, reports and other local rules and options.

Within this structure, Niche also offers unique domain-based multi-jurisdictional information sharing that allows police agencies to easily share RMS system data with other agencies or tenants. Multi-tenant Niche consortiums can search between agencies even on details such as tattoo descriptions, MO, victim relationships and verbiage (full text). The Niche project team has experience and expertise in guiding large customers through the process of implementing a multi-tenant system. It is our main area of specialty.

As another option, we have an InterNiche feature makes it possible for entirely separate NicheRMS installations (each with its own database) to share data. InterNiche works in any combination of multi-agency and/or single-agency instances. This makes a connection between NYSP and other NicheRMS installations possible. Niche is currently supporting multi-tenant and InterNiche installations in the United States, Canada and the UK. Many Niche customers are already sharing or planning to share their NicheRMS installations with partner agencies.

How are multi-tenant options set up?

NicheRMS uses a system of *domains* to organize data in the database, and we use this to create a flexible way to host multiple agencies/tenants within a single NicheRMS installation. Main features:

- All data records are tagged with a domain name.
- The domain tags identify which agency/tenant owns a particular record in the installation's single shared database.
- The domain tags determine access to the data – where when and how it will appear – throughout the rest of the system.
- Data records can be owned by a single tenant (*e.g.*, tagged with the domain name of a given police agency) or they can be shared among multiple police tenants (tagged with a parent domain).

In a multi-tenant installation, each tenant has a domain within a single NicheRMS database. This domain system supports individual configurations within a larger installation. Member agencies/tenants working within their own domains can set up agency-specific roles, workflow, system parameters, default field values, reports and other local rules and options.

Domains are used for:

1. **Security** – domain-related permissions determine what data will be available to users within an agency and to users in other domains within the same installation, e.g., users who are members within the domain for an agency might have view and update permissions on records, but users searching from a different domain in the same installation might have view access only.
2. **Searches** – users can determine the scope of searches by choosing domain options. For example, users can choose to search within one agency, within all agencies under a parent domain, all agencies in a geographic area, etc.
3. **Configuration** – Different agencies/tenants can be configured differently within the same installation. Often, global configuration options are implemented in a high level parent domain, with individual special configuration options implemented in the agency/tenant domains below the parent domain. This allows individual tenants to set up their own workflows, field defaults, business rules, data validation/retention rules and report options.

Different types of data can be held at different levels in the domain hierarchy and there is some flexibility in how this can be set up. For example, Person records could be held at a shared domain level that is available across all of the agency domains (allowing all users to access the same store of master index Person records), while officer's investigation reports and other Incident and Case management details could be held at the police agency domain level (not shared). Note that data sharing among police agencies can be set by default or manually overridden by a user with appropriate access.

Domains can also be geographic in nature. The structure is rooted at the "Universe" domain, followed by jurisdictions (typically countries, states, etc.), then by the actual NicheRMS installations and lastly the police agencies hosted inside those installations. For example, the domain for Springfield, MO, is "Universe/US/MO/Springfield Multi-Agency Host/Springfield PD".

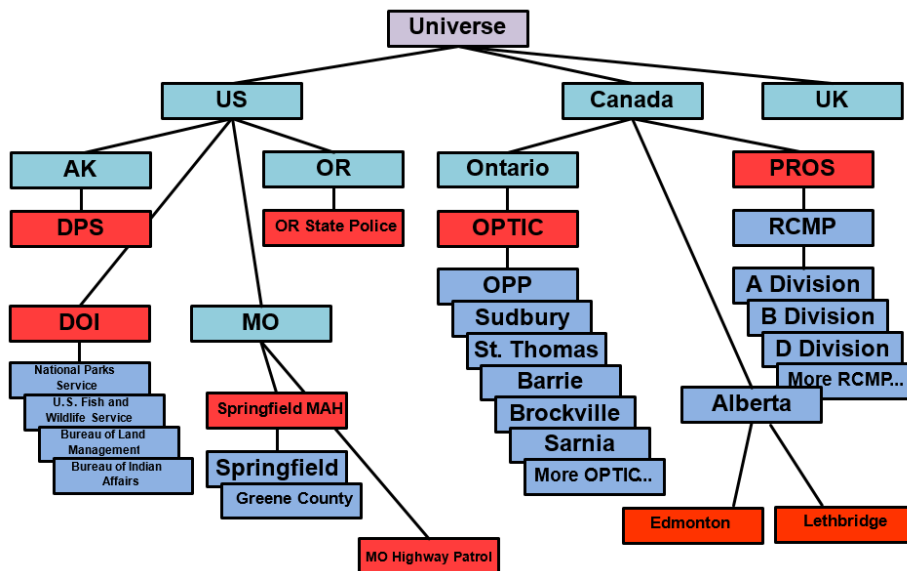
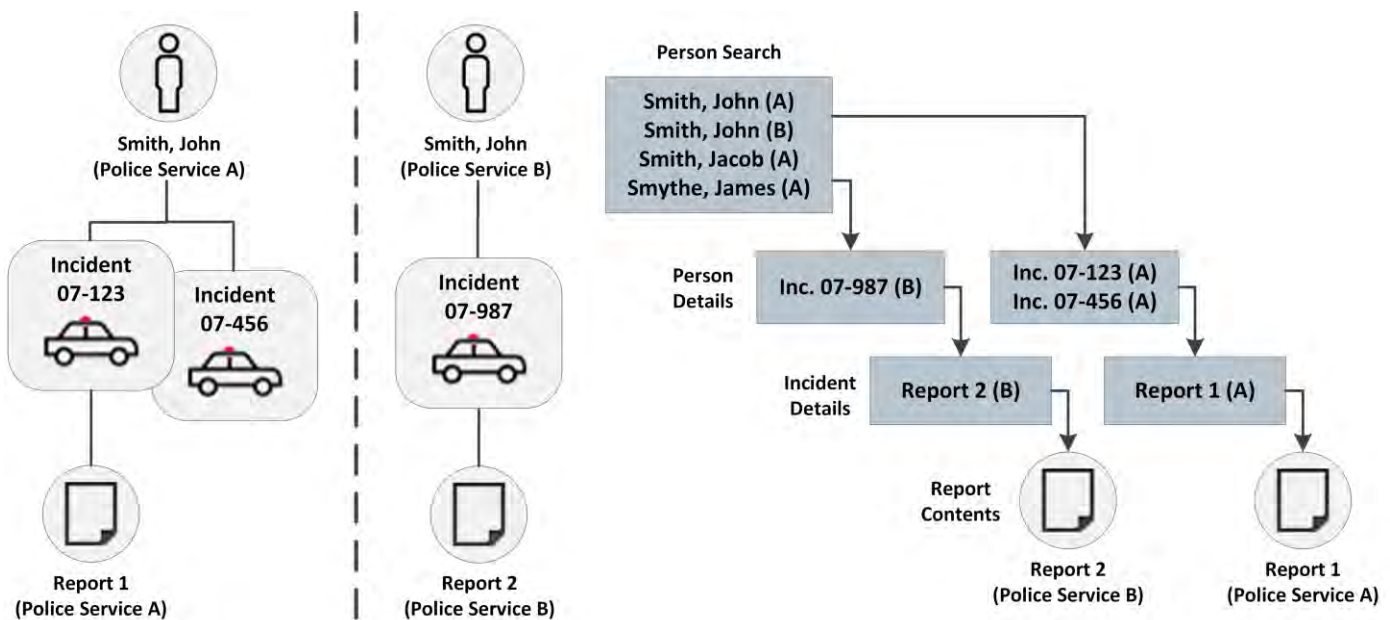


Diagram showing the domain structure of a number of NicheRMS installations. Note that the domain structure is rooted at Universe, followed by jurisdictions (typically countries, states, etc.), then by the actual NicheRMS installations (the red boxes) and lastly the police agencies hosted inside those installations. For example, the domain for Springfield, MO, is "/US/MO/Springfield MAH/Springfield".

Below are two examples of approaches to multi-agency domain structures. Note that these are examples only: NicheRMS can be configured for other approaches to information sharing. As part of the initial implementation project, Niche assists with determining the model the best suits police agency needs.

Approach 1: Per agency data management model

When a user enters data into NicheRMS, a domain tag is automatically attached to the record. This determines data ownership. In the “Per-agency data management model”, all the data created by a specific agency is tagged with their domain and is read only for users from other domains. The effect is complete separation of the data belonging to the various police agencies. Users from other domains have read-only access to other agency’s data. A police user can search their own data, data belonging to another police agency, or, by searching a parent domain, data belonging to multiple (or all) police agencies hosted in the system. Sharing can be controlled on a per-record basis if needed.



All data created by a police agency is tagged with the police agency’s domain. If multiple police agencies have contact with the same person, there will be multiple person records (one per police agency) for the person and a search of the common parent domain will return multiple person records.

With this model, if multiple police agencies/tenants have contact with the same person, it results in multiple person records (one per police agency) for that person, and a search of the common parent domain will return multiple person records. All of the shared data is available, but users may have to look at more than one person record to get a complete history of that person’s contact with police in the state.

Case Study

The Ontario Provincial Police/Ontario Police Technology Information Cooperative (OPP/OPTIC) project was the first large NicheRMS police project, going live in 2000. It comprises 41 police agencies, including the Ontario Provincial Police, serves 8,381 officers (about 10,000 users), and covers 416,000 square miles. OPP/OPTIC maintains a central server farm with multi-jurisdictional data sharing using the domain by agency model.

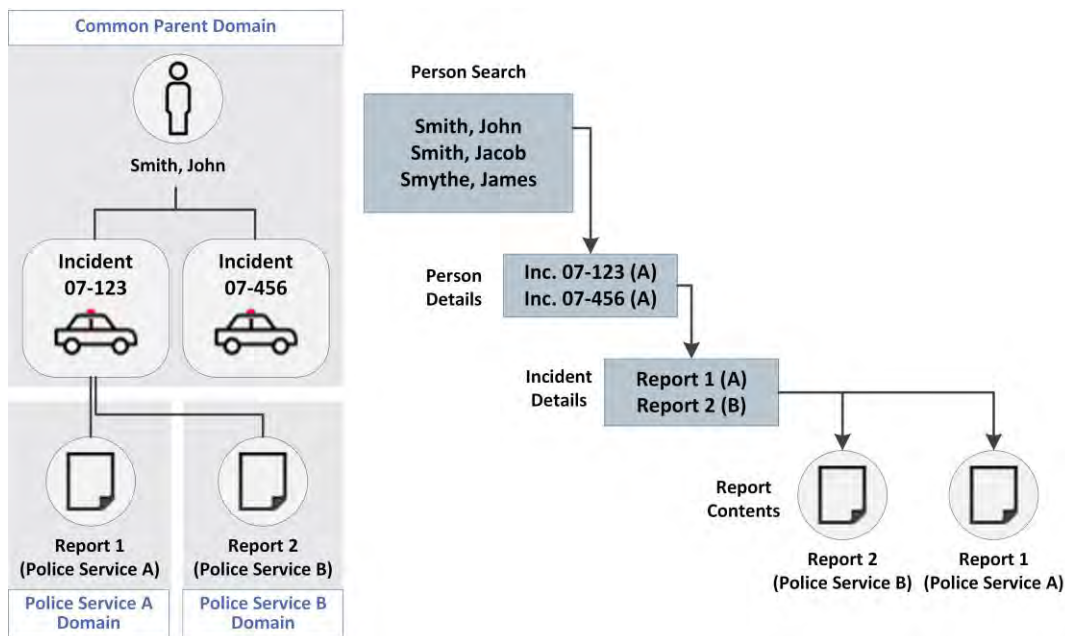
Approach 2: Shared data management model

In the Shared data management model, all master-index Person records and Incident records are held in a parent domain shared by all tenants of the system. The effect is that there is a single system-wide master index record for each person, jointly shared by all agencies/tenants. Incident records can be similarly shared by all tenants across the system. Shared Incident records are particularly useful when member police agencies regularly engage in joint investigations in which officers from multiple agencies contribute to the same incident. Investigation reports and other data collected during the investigation are still held in local police agency tenant domains, but the incident itself is shared.

Domain splitting decisions depend on police requirements. For example, it is possible to put master index Person records in a shared parent domain, while all other data belongs to individual police agencies. With NicheRMS, there are many possibilities on which entities are shared. The NicheRMS could be configured for the parent domain to contain whichever entities New York decides to master file at the state level.

Case Study

The RCMP PROS system supports federal policing and policing for 198 municipalities, 192 First Nations communities, and 29 EPPAs, comprising 14,000 police officers (2004 go-live). The system allows the RCMP and its partner agencies to maintain single shared person and incident records across Canada. The South Wales Police/Gwent project in the UK also uses this approach.

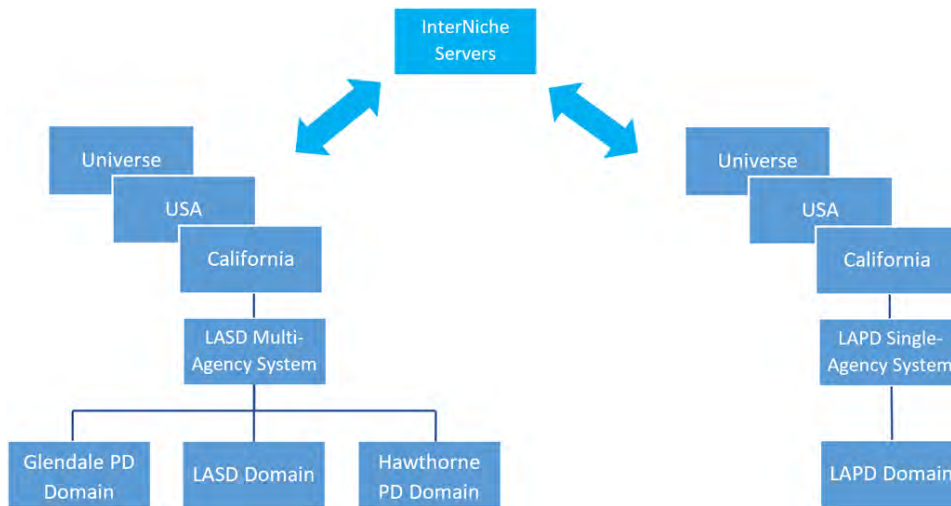


Person and incident records are held in a common parent domain, making them jointly owned, allowing multiple agencies to maintain a single master person record.

InterNiche data sharing with other installations

An InterNiche connection makes two completely separate Niche installations behave like a single shared system.

This allows officers in neighboring NicheRMS agencies to search and drill-down on data in detail. Cross-jurisdictional crime analysis and even workflow in joint investigations is happening on a large scale today. This could be set up between New York State and other agencies. The diagram below shows an example using LAPD and LASD. A multi-agency NicheRMS installation for LASD can be connected to a single-agency installation for LAPD using InterNiche. When LASD users set up a search, they can use a selector list to choose which domain(s) they would like to query, for example, LASD (selected by default) and Glendale, Hawthorne, LAPD, or “California” to search all agencies simultaneously.



Multi-agency shared-data installations have always been part of NicheRMS, and this feature is well tested and proven. InterNiche extends this data-sharing capability to multiple, independent installations, with servers connected via private or public wide area networks (or the cloud).

From a user's point of view, there is no difference between querying their own agency, querying other agency data on the same server, or querying multiple Niche installations across the region. All a user has to do is select which domains they want to include in the search. We provide an example of this below.

Searching in a multi-tenant or InterNiche installation

The example below shows a user view of searching other agencies' data: all a user has to do is type in the information they'd like to search on and select the domain(s) to choose which agency's data they'd like to search.

The **Data Sources** options allow you to select which databases will be searched (①). The default is *Primary* (i.e., the default database associated your login ID) but others may be available: you can use the checkboxes to add other databases to be searched at the same time.

Options (②) allows you to set important defaults for search domain and scope. In a multi-agency system, the user can select which agencies' domains to be included in the search.

The results returned can include records owned by other tenants or NicheRMS installations. The extent to which this external data will be available can be controlled by the agency associated with the particular domain that the data belongs to.

The screenshot displays the NicheRMS Person search interface. On the left, there are two dropdown menus: 'Domain' and 'Scope'. The 'Domain' menu is open, showing options: '<Default>', '<Current domain>', 'UNIVERSE', 'ALL AGENCIES', 'REPUBLIC', and 'SPRINGFIELD'. An arrow points from the 'UNIVERSE' option to the 'Domain' dropdown in the main interface. The 'Scope' menu is also open, showing options: 'Domain + sub-domains', 'Domain + parent-domains', 'Domain', and 'Full domain hierarchy'. An arrow points from the 'Domain + sub-domains' option to the 'Scope' dropdown in the main interface. The main interface has a left sidebar with navigation icons and a 'Person search' header. Below the header are sections for 'DATA SOURCES' (with checkboxes for Primary, Face search, CLETS - Wanted, and CLETS - Wanted & driver), 'OPTIONS' (with dropdowns for Domain and Scope, and checkboxes for Phonetic, Limit by first, All names, and Multi search), and 'SAVE OPTIONS' (with buttons for Open, Save as, and Save as (assign to)). The main search area contains a search bar with a magnifying glass icon and a 'Find now' button. Below the search bar are several input fields: 'Fast find', 'Last name', 'Name type', 'First name', 'Middle name', '2nd middle name', 'Sex', 'Date of birth', 'Suffix', 'FBI', 'MNI', 'Race', and 'Ethnicity'. There are also expandable sections for 'Description', 'Marks/tattoos', 'Clothing', 'IDs', and 'Advanced options' (which includes 'CLETS - Wanted & driver'). A 'Clear search' button is located below the search options. The top right corner shows a user profile for '#121 DONEY, K. Administrator' and standard window controls.

Requirement: Proposed Enterprise Solution Architecture		
Req. No.	Req. Status	Requirement Description
T11	M	<p>The Contractor shall provide a detailed description of its overall architectural solution in its proposal including, but not limited to, the following:</p> <ul style="list-style-type: none"> • NYS will be responsible for providing the site, environmental support, data/voice communications as well as all of the hardware as specified in the winning Contractor’s proposed solution. NYS will provide highly available systems at the primary Data Center with optional disaster recovery at a secondary site. • The Contractor shall specify all hardware and software required to implement its solution including, but not limited to, a depiction of hardware and software layers and storage, its’ proposed application solution, interfaces, production, non-production and training environments, and solution for high availability. One of the non-production environments must mirror the production environment. The training environment must be sized to accommodate 10% of the total users in the production environment. • Software specifications and attributes to support the Contractor’s solution and shall conform to NYS Information Technology Services (ITS) requirements, as follows: <ul style="list-style-type: none"> Proposed Operating System shall be one of the following: <ul style="list-style-type: none"> • IBM POWER AIX • Red Hat Enterprise Linux • Microsoft Windows Server Proposed Database (RDBMS) shall be one of the following: <ul style="list-style-type: none"> • Oracle (must run on AIX) • MS SQL • Other - if fully managed and supported by Contractor* If the solution is web based, proposed middleware components shall be one of the following: <ul style="list-style-type: none"> • Apache • Microsoft IIS/IBM HTTP • WebSphere Application Server • JBOSS • Other middleware components fully managed and supported by Contractor* • Proposed Solution shall operate with the NYS EIAM Service.

		<ul style="list-style-type: none"> Proposed solution shall be able to run effectively within a virtual server environment running on an approved operating system (see above). The Contractor’s proposed solution must be certified and supported on the above hardware and software system distributions with a preference to maintain the latest production phase lifecycle (two-year cycle). The Contractor’s proposed solution shall support the capability for NYS ITS to comply with qualified Critical and Important Security errata advisories and Vulnerability patching in compliance with NYS Enterprise Information Security Office (EISO) requirements for all the hardware and software specifications identified above. <p>* NYS will consider alternatives as long as the alternative proposed is fully managed and supported as part of the day to day operation of the Records Management System. Implementation and operation must not require specialized staff, specialized training or skills AND all NYS data contained within must be fully accessible by State resources.</p>	
<p>Provide a comprehensive description of how the proposed solution satisfies the requirement including technical specifications, capabilities, features, considerations, constraints, and limitations. Reference additional pages, if necessary. Indicate if the solution is offered or not offered →</p>		<p>Offered <input checked="" type="checkbox"/></p>	<p>Not Offered <input type="checkbox"/></p>
<p>Niche Technology response: see our response material immediately following this table.</p>			

Niche Technology response – Application Performance

Overview

We have provided a detailed overview of our system architecture in response to [Requirement T8](#) on page 32. See page 36. Please see our Supplementary materials section below for details of the hardware and software infrastructure we recommend to support our system architecture.

Support for requirements

The Contractor shall provide a detailed description of its overall architectural solution in its proposal including, but not limited to, the following:

NYS will be responsible for providing the site, environmental support, data/voice communications as well as all of the hardware as specified in the winning Contractor’s proposed solution. NYS will provide highly available systems at the primary Data Center with optional disaster recovery at a secondary site.

Niche Technology complies with this and can provide recommendations and guidance for NYS to carry out the necessary setup and support. Please see our Supplementary materials section below for details of the hardware and software infrastructure we recommend to support our system architecture.

The Contractor shall specify all hardware and software required to implement its solution including, but not limited to, a depiction of hardware and software layers and storage, its' proposed application solution, interfaces, production, non-production and training environments, and solution for high availability. One of the non-production environments must mirror the production environment. The training environment must be sized to accommodate 10% of the total users in the production environment.

Niche Technology complies with this and can provide recommendations and guidance for NYS to carry out the necessary setup and support. Please see our Supplementary materials section below for details of the hardware and software infrastructure we recommend to support our system architecture. Also see the detailed overview of our system architecture in response to [Requirement T8](#) (page 36).

You will note that our recommendations specifically include the setup of additional non-production and training environments, e.g., for Disaster Recovery, Training, Testing and development

Software specifications and attributes to support the Contractor's solution and shall conform to NYS Information Technology Services (ITS) requirements, as follows:

Proposed Operating System shall be one of the following:

- ***IBM POWER AIX***
- ***Red Hat Enterprise Linux***
- ***Microsoft Windows Server***

NicheRMS uses Microsoft Windows Server. Please see our Supplementary materials section below for further details.

Proposed Database (RDBMS) shall be one of the following:

- ***Oracle (must run on AIX)***
- ***MS SQL***
- ***Other - if fully managed and supported by Contractor****

NicheRMS uses MS SQL. Please see our Supplementary materials section below for further details.

If the solution is web based, proposed middleware components shall be one of the following:

- ***Apache***
- ***Microsoft IIS/IBM HTTP***
- ***WebSphere Application Server***
- ***JBOSS***
- ***Other middleware components fully managed and supported by Contractor****

NicheRMS is not a web-based solution.

Proposed Solution shall operate with the NYS EIAM Service.

NicheRMS will operate within the NYS EIAM Service. More information is provided in our response to [Requirement T6](#) on page 14.

Proposed solution shall be able to run effectively within a virtual server environment running on an approved operating system (see above).

A large number of NicheRMS customers of all sizes (up to approximately 10,000 sworn officers) host their production RDBMS instances within VMware.

Further, the first customer to host a NicheRMS production environment in Azure went into production in Q2 2018.


In general, the decision to run the RDBMS layer in a virtual environment would depend on the following:

- Whether the host servers can provide VM sizing that matches the specification provided above, with no overcommit at the host level, *i.e.*, guaranteed computational resources.
- Whether the customer has sufficient expertise with the platform that they can reasonably support the virtualization layer in cooperation with the administrators who will be monitoring and otherwise supporting the NicheRMS application server and database server layers.

The Contractor's proposed solution must be certified and supported on the above hardware and software system distributions with a preference to maintain the latest production phase lifecycle (two-year cycle).

NicheRMS complies with this. Our software and processes are regularly updated to support current and future hardware and system software. Please see our Supplementary materials section below for further details.

The Contractor's proposed solution shall support the capability for NYS ITS to comply with qualified Critical and Important Security errata advisories and Vulnerability patching in compliance with NYS Enterprise Information Security Office (EISO) requirements for all the hardware and software specifications identified above.

NicheRMS complies with this. Our software and processes are regularly updated to support current and future hardware and system software. Please see our Supplementary materials section below for further details. 

**** NYS will consider alternatives as long as the alternative proposed is fully managed and supported as part of the day to day operation of the Records Management System. Implementation and operation must not require specialized staff, specialized training or skills AND all NYS data contained within must be fully accessible by State resources.***

Supplementary material: NicheRMS recommended infrastructure

This section details Niche Technology’s recommended specifications to support a proposed deployment of NicheRMS by NYSP. The information in this section is based on:

- Approximate number of officers (excluding support staff): 5,000
- Specifications and performance statistics from comparably-sized deployments of NicheRMS
- A comparative survey of results from standard server benchmarks, including:
 - SAP 2-tier ("sd2tier")
 - TPC-C
 - TPC-E
 - SPECINT2006

Server specifications

Database servers

Read/write database host (2 node active/passive cluster)

Operating system	One of: <ul style="list-style-type: none"> • Windows Server 2016 Standard Edition • Windows Server 2016 Datacenter Edition
Database server	One of: <ul style="list-style-type: none"> • SQL Server 2016 Enterprise Edition • SQL Server 2017 Enterprise Edition (support expected Q3/Q4 2018)
CPU	1x12 core Xeon Gold 6136 processor, or performance equivalent
RAM	192 GB
Storage	<p>Production NicheRMS databases range in size from 25 GB to 10 TB+. Required storage quantities are heavily dependent on the volume of scanned documents, images, and imported data; approximately 85% of storage required by a NicheRMS database can be BLOB data.</p> <ul style="list-style-type: none"> • Fielded data <ul style="list-style-type: none"> ▪ Initial storage allocation: 250 GB ▪ Latency: less than 10 ms ▪ Throughput (8 KB): 35 MB/sec ▪ Throughput (64 KB): 150 MB/sec • Unfielded (<i>i.e.</i>, binary/BLOB) data <ul style="list-style-type: none"> ▪ Initial storage allocation: 1 TB ▪ Latency: less than 15 ms ▪ Throughput (8 KB): 35 MB/sec ▪ Throughput (64 KB): 150 MB/sec • Transaction log <ul style="list-style-type: none"> ▪ Initial storage allocation: 64 GB

	<ul style="list-style-type: none"> ▪ Latency: less than 5 ms ▪ Throughput: At least 100 MB/sec, ideally much higher if being used to support synchronous mirroring of any sort <p>Notes</p> <ul style="list-style-type: none"> • The starting points listed above are expected to be sufficient for up to three years, providing that there is not an initial legacy data import. • The system will rarely reach the throughput detailed above; the specification is intended to cover periods where I/O is high due to index maintenance, backups, clean up tasks, mass data imports, and unexpected issues such as poor query plan selection. • It is desirable but not required to place the transaction log LUN on enterprise SSD storage to ensure that the transaction log does not become a bottleneck to the various processes that depend on it. • RAID 1+0 or a similar SAN-level scheme/distribution should be used for the best performance and redundancy. <p>Customers may choose to use RAID 5/6 (or SAN equivalent) for binary data such as images and report narratives, which are stored in a designated part of the NicheRMS data model/schema and do not have the same performance requirements as fielded data.</p>
<p>Clustering considerations</p>	<p>A traditional failover cluster typically requires shared storage (e.g., SAN) that is certified by the vendor and Microsoft for use in a SQL Server failover cluster.</p> <p>An AlwaysOn AG replica can also be used for local HA, but this comes at the expense of additional storage and potential latency effects if the solution infrastructure is not sufficient to keep up with the volume of change.</p> <p>If synchronous AlwaysOn replication is expected to be used, the system storage infrastructure needs to be architected appropriately, <i>i.e.</i>, high throughput LUNs (ideally pure SSD) for the transaction log and fielded data.</p> <p>The rate of NicheRMS data change is relatively low, this would rarely occur during normal operation, but could be caused by un-throttled maintenance jobs, data imports, clean up scripts, <i>etc.</i></p>

Reporting/audit database host (1, required)

<p>Purpose</p>	<p>Offloading auxiliary database services from the primary database server. Required for projects that use a Niche-provided export interface or use the NicheRMS audit functionality, and recommended for customers maintaining a data warehouse, executing business intelligence extracts, <i>etc.</i></p>
<p>Requirement level</p>	<p>Optional, recommended</p>
<p>Operating system</p>	<p>One of:</p> <ul style="list-style-type: none"> • Windows Server 2016 Standard Edition • Windows Server 2016 Datacenter Edition

Database server	<p>One of:</p> <ul style="list-style-type: none"> • SQL Server 2016 Enterprise Edition • SQL Server 2017 Enterprise Edition (support expected Q3/Q4 2018) <p>Notes:</p> <ul style="list-style-type: none"> • The SQL Server version (SQL Server 2016, SQL Server 2017) should match the version used by the primary servers • Customers may use Standard Edition for this server, providing that they are comfortable with the limitations that SKU. For example, Standard Edition can only use 128 GB of memory, cannot be used to provide read-only AG replica access, <i>etc.</i>
CPU	1x12 core Xeon Gold 6136 processor, or performance equivalent
RAM	192 GB
Storage	<p>Similar performance characteristics to the primary database server, although RAID 5/6 (or SAN equivalent) is commonly used.</p> <p>The storage requirements may vary substantially and depend on:</p> <ul style="list-style-type: none"> • Reporting: How many replicas of production are maintained and whether secondary databases + tables are required to support reporting • Audit: The queryable audit database requires approximately 3-4 MB per officer/day, (<i>i.e.</i>, 1.5x the size of the raw uncompressed audit log files).

Virtualization of the database layer

A large number of NicheRMS customers of all sizes (up to approximately 10,000 sworn officers) host their production RDBMS instances within VMware.

Further, the first customer to host a NicheRMS production environment in Azure went into production in Q2 2018.

In general, the decision to run the RDBMS layer in a virtual environment would depend on the following:

- Whether the host servers can provide VM sizing that matches the specification provided above, with no overcommit at the host level, *i.e.*, guaranteed computational resources.
- Whether the customer has sufficient expertise with the platform that they can reasonably support the virtualization layer in cooperation with the administrators who will be monitoring and otherwise supporting the NicheRMS application server and database server layers.

Application (NDS) servers (10)

Purpose	Application (NDS) and interface services for NicheRMS
Requirement level	Required
Operating system	Windows Server 2016 Standard Edition
CPU	1x4-core (or 4 vCPU) server-grade processor, e.g., a modern Intel Xeon. The CPU performance target for an NDS instance is a SpecInt 2006 rate score of 100-160 across 4 logical CPUs (cores, vCPUs, etc.).
RAM	8 GB
Storage	Approximately 450 GB local disk, in a RAID 1 or other fault tolerant configuration.
Network	Two or more network adapters; this allows physical separation of the user-facing load balanced IP address and the private/database-facing IP address.
Typical configuration	<p>The NDS estate for the proposed deployment would likely be split in the following way:</p> <ul style="list-style-type: none"> • 7 NDS servers that are load balanced for end user access; this load balancing is achieved via standard TCP load balancing. • 3 NDS servers dedicated to interfaces to external systems such as CAD, NicheRMS web services, etc. <ul style="list-style-type: none"> ○ Critical interfaces such as the CAD-to-RMS import are configured so that they can run on any of the servers, but default to running on an interface NDS when it is available. ○ Non-critical interfaces/processes are configured to only run on the interface servers, i.e., they do not migrate over to the load-balanced end user NDS servers. <p>This configuration allows for servicing of interface-specific hardware and software with minimal user disruption.</p>
Virtualization	<p>Niche Technology Inc. supports customers who pursue virtualization of the NicheRMS server application using VMware.</p> <p>NDS servers that are hosted in a virtualized environment are sized to match physical specs.</p>

General notes

- New server hardware, operating systems, and database software should be 64-bit. NicheRMS does support 32-bit OS environments, but they should not be used in a production environment due to the limitations on handling larger amounts of memory.
- The above database storage estimates do not account for storage of raw NDS audit logs, which amount to roughly 2 MB/officer/day, but compress by approximately 80%. These are estimates that will vary with the actual number of end users that routinely use the system and the overall complexity of the job those users are doing.

Client Workstations

Purpose	Provide end user access to NicheRMS
Operating system	Windows Vista SP2 or higher
CPU	Intel Core2 Duo @ 2.2 GHz or better preferred
RAM	2 GB
Storage	The current NicheRMS desktop install uses roughly 400 MB of storage. This does not account for system prerequisites, additional mobile applications, or custom plug-ins.
Display	<ul style="list-style-type: none"> • NicheRMS desktop and NicheRMS mobile applications: Minimum resolution of 1024x768 • NicheRMS tablet-compatible mobile application: A minimum of a 7" display. • All applications: Video adapter or virtualization suite that is fully compatible with WPF applications
Prerequisite software	<ul style="list-style-type: none"> • Microsoft DHTML editor • Internet Explorer 7 or higher • Microsoft .NET 4.6
Common supporting software	<ul style="list-style-type: none"> • Microsoft Word – this is the most common format used for storing documents in NicheRMS • Other productivity software (Excel, WordPerfect, Adobe Viewer, Adobe Acrobat, etc.)
Device-specific software	<p>NicheRMS supports a variety of optional hardware add-ons. This currently includes image capture devices, barcode scanners, card readers, signature tablets, and barcode printers.</p> <p>These devices are typically installed on a small subset of the workstation base, and may require additional drivers and software.</p> <p>Any device-specific requirements are in addition to the core NicheRMS application requirements.</p>
Desktop/application virtualization	<p>Niche supports the deployment of NicheRMS user applications in virtualized/streamed environments, e.g., Citrix/RDP services/etc. However, Niche does not perform exhaustive in-house testing using these packages because there are too many possible variations.</p> <p>Customers are encouraged to test their version of NicheRMS in their desired environment, with their proposed configuration.</p> <p>Niche will work to fix any incompatibilities found. Customers may have to upgrade to the latest version of NicheRMS in order for Niche to provide related fixes.</p>
General notes	<p>NicheRMS runs well on any modern PC.</p> <p>The specifications above reflect known configurations that run well for regular users at current customer sites.</p>

	Hardware specifications account for typical use, which includes using Microsoft Word for forms, as well as using Internet Explorer and other related software at the same time as the NicheRMS applications.
Accounting for power users	It is suggested that "power users" (e.g., intel analysts) and those in high-volume or otherwise time-sensitive roles (e.g., custody, contact center) receive higher end workstations when possible. In specific, it is useful for power user workstations to have relatively high single-threaded (i.e., per-core) CPU performance.

Additional environments

NicheRMS customers usually maintain one or more additional environments that support the operational environment; the section below discusses some of these environments.

In contrast to the operational hardware, the hardware requirements for the additional environments depend heavily on the customer's internal business requirements as opposed to any specific resource requirements of NicheRMS.

In practice, the lines between most of these environments are somewhat blurry.

For example, it is common for one environment to be used for training and for testing of core functionality, while another system is used for development and occasionally for testing certain interfaces.

Disaster recovery

NicheRMS customers typically deploy a physically remote disaster recovery (DR) site. The database on this site is generally maintained by transaction log shipping or database mirroring.

The DR site is often a slightly smaller version of the operational environment, though some customers choose to deploy an identical set of hardware at their DR site.

Ultimately, the features of the DR site reflect the customer's required level of consistency between the two sites. That is, if the DR site is expected to behave exactly as the operational site, it needs to be specified similarly.

Comparison of selected operational and DR site features

# of NDS servers	In some cases, the DR site may have slightly fewer NDS servers. This may involve: <ul style="list-style-type: none"> • Consolidating all interface traffic to a single NDS server. • Reducing the number of end user servers that are available if the user load is guaranteed to be lower than usual while the disaster recovery is in use.
# of primary database servers	Due to the importance of this component, many DR sites have the same number of primary database servers as in production: an active/passive cluster consisting of two nodes. With that said, some agencies choose to implement a single non-clustered database server in DR.
# of secondary database servers (reporting/audit/archive)	DR sites may or may not use separate database servers for these jobs.

	A common option is to have the DR site's primary database server fill these roles, while acknowledging that this option may lead to reduced performance while the DR site is operational.
--	---

Training

The following specifications should be sufficient for the training needs of most agencies, although larger agencies that are planning mass training for an "all-at-once" initial rollout may need to expand these specifications to meet their requirements.

Database server

Purpose	Database server for training environment.
Operating system	Windows Server 2016 Standard Edition
Database server	One of: <ul style="list-style-type: none"> • SQL Server 2016 Standard Edition • SQL Server 2017 Standard Edition (support expected Q2/Q3 2018)
CPU	1x4-core server-grade processor (e.g., Intel Xeon); recommendation available on request
RAM	16 GB
Storage	Dependent on the size and quantity of training databases that are used. It is suggested that this server have at least 100 GB available for database storage, as it is normal to maintain multiple training databases that are used for parallel training classes and different app versions. Some fault-tolerant level of RAID may be appropriate (e.g., RAID 1), depending on the customer's required level of availability.

Application (NDS) server(s)

Purpose	RMS server (NDS) and interface services for training environment
Operating system	Windows Server 2016 Standard Edition
CPU	1x4-core server-grade processor (e.g., Intel Xeon); recommendation available on request
RAM	8 GB
Storage	Any basic storage devices should suffice for this task; some fault-tolerant level of RAID may be appropriate (e.g., RAID 1), depending on the customer's required level of availability.
Note	Some agencies choose to run the training site's NicheRMS application server on the same system as the training DBMS, though many deploy a separate NDS server for training.

Testing and development

NicheRMS sites generally include one or more testing and development environments.

The number of distinct environments and the exact hardware and software requirements depend heavily on the type of testing and development being performed.

Another significant factor is whether the customer feels that systems can be shared by different purposes.

The following are common options for testing and development environments:

Basic test environment

- Used by project staff when testing new versions and performing gap analysis.
- The hardware specifications for such a system are modest.
 - Some agencies have a shared training/test environment, while others deploy individual environments for these purposes.
 - SQL Server can either be hosted on the server that hosts the NicheRMS application server (NDS), or NDS can be pointed at a shared database server to reduce licensing costs.

Pre-prod environment

- Typically hosts a copy of the production database, or a database of similar size/scope.
- These environments have production-grade hardware specifications, although they are often cut down to a certain extent.
- Use of these environments reduces risk by allowing for very realistic testing and analysis without disrupting the production environment.

Niche customers have previously used these environments for the following tasks:

- Test of major version upgrade processes
- Data import/migration testing
- Stress testing of new NicheRMS versions
- Performance-related troubleshooting/analysis
- Refining database management practices
- Final user acceptance testing when moving between major versions of NicheRMS

Development

- Agencies that perform significant internal development may have dedicated development environments.
- A customer may be able to deploy SQL Server Development Edition into their development environment.

This allows developers to test Enterprise-level features at a much lower cost than purchasing another Enterprise license for the development environment.

The various MSDN subscriptions also include development tools (e.g., Visual Studio) that can be used to develop custom applications that interact with NicheRMS.

- These systems are also often used for testing external interfaces that may not be configured for basic functionality testing.

Requirement: Proposed Solution Architecture: High Availability			
Req. No.	Req. Status	Requirement Description	
T12	M	<p>The Contractor shall provide a description of the recommended approach for NYS to achieve a highly available environment. The Contractor's proposal and shall include, but not be limited to, the following:</p> <ul style="list-style-type: none"> • How the architecture proposed by the Contractor will meet the application performance requirements • Redundancy, and single points of failure • Fault tolerance • Session/load balancing, (if applicable) • Mirrored data • Backup, restore and recovery plans for all data, including any impact on production, throughput and response times. • Any additional high availability features that the proposed solution includes which would allow New York State continued system availability when components of the system are unavailable. 	
<p>Provide a comprehensive description of how the proposed solution satisfies the requirement including technical specifications, capabilities, features, considerations, constraints, and limitations. Reference additional pages, if necessary. Indicate if the solution is offered or not offered →</p>			<p>Offered <input checked="" type="checkbox"/></p>
			<p>Not Offered <input type="checkbox"/></p>
<p>Niche Technology response: see our response material immediately following this table.</p>			

Niche Technology response – High Availability

Overview

NicheRMS is a 24/7 high availability system, frequently reported by IT managers to be among the most reliable of all systems that they run. When set up and configured as advised by Niche, there are no single points of hardware failure, and the system is resilient enough to maintain the required system response time and uptime regardless of cause of the failure. The system detects and recovers from failures with no human intervention, making after-hours emergency service calls rare.

Support for requirements

The Contractor shall provide a description of the recommended approach for NYS to achieve a highly available environment. The Contractor's proposal and shall include, but not be limited to, the following:

How the architecture proposed by the Contractor will meet the application performance requirements

NicheRMS is designed to be a highly availability. Niche customers average 2,467 sworn officers in size and place an urgent call for support once every 3.7 years on average. From Queensland Police: "Our production database size is 8TB...we've had no downtime attributable to NicheRMS software problems in over a decade". For more details, please see our responses below.

Redundancy, and single points of failure / Fault tolerance

When set up and configured as advised by Niche Technology, there are no single points of hardware failure, and the system is resilient enough to maintain the required system response time and uptime regardless of cause of the failure. The system will detect and recover from failures with no human intervention. For more details, please see the Supplementary material section below.

Session/load balancing, (if applicable)

The Niche Data Servers (NDS) servers themselves are load balanced, providing both load sharing and redundancy in case of an NDS server hardware failure. For more details, please see the Supplementary material section below.

Mirrored data

NicheRMS supports mirrored data, for example this is used to maintain a Disaster Recovery site, as we describe below in our Supplementary material section.

Backup, restore and recovery plans for all data, including any impact on production, throughput and response times.

The NDS (application) server software is designed with hardware redundancy allowing the system to tolerate a database server failover. If network connections to the database server are lost, the NDS software attempts to reconnect and re-run any transactions that were aborted. This retry, combined with the automatic SQL Server database failover and recovery, assures that no work is lost during a failover. The only noticeable effect is that the system pauses while the failover occurs.

NicheRMS supports any backup tools that works with Microsoft SQL Server. Backup procedures do not impact production, throughput or response times.

Any additional high availability features that the proposed solution includes which would allow New York State continued system availability when components of the system are unavailable.

Please see the Supplementary material section below.

Supplementary material: High availability

NicheRMS is designed for 24/7/365 operation. Our contractual target for system availability is normally 99.5% (or 99.7%, depending on how it is measured), although our users almost always report a higher uptime. Niche customers average 2,467 sworn officers in size and place an urgent call for support once every 3.7 years on average. From Queensland Police: "Our production database size is 8TB...we've had no downtime attributable to NicheRMS software problems in over a decade".

We encourage the NYSP to talk to our current customers about whether the availability of their NicheRMS systems is acceptable, and to do the same for other potential vendors.

There is no routine downtime required for NicheRMS maintenance. However, downtime is required for software upgrades. The downtime can be minimized through proper planning and preparation, but cannot be eliminated. For longer periods planned downtime, it is possible to provide read-only access to the system while the upgrade is taking place. This significantly mitigates officer safety issues by providing officers with most of the information that they would have had access to under normal circumstances, although officer efficiency is still affected.

Resilient system design

NicheRMS is a 24/7 high availability system, frequently reported by IT managers to be among the most reliable of all systems that they run. When set up and configured as advised by Niche Technology, there are no single points of hardware failure, and the system is resilient enough to maintain the required system response time and uptime regardless of cause of the failure. The system will detect and recover from failures with no human intervention. After-hours emergency service calls are very rare.

Hardware redundancy

All computer hardware can fail unexpectedly. Typical repair time is 4 — 24 hours, which is not acceptable for any critical operational system. NicheRMS avoids downtime due to hardware failures as follows:

- Database servers are configured in a cluster. If the primary server fails, the secondary database server takes over the NicheRMS database instance from the primary server.
- The database is stored on redundant (RAID) disks, typically on a SAN shared by the machines in the database server cluster.
- The NDS (application) server software is designed to tolerate a database server failover. If network connections to the database server are lost, the NDS software attempts to reconnect and re-run any transactions that were aborted. This retry, combined with the automatic SQL Server database failover and recovery, assures that no work is lost during a failover. The only noticeable effect is that the system pauses while the failover occurs.
- The NDS servers themselves are load balanced, providing both load sharing and redundancy in case of an NDS server hardware failure.
- Any part of the system can be run in a virtual environment, providing an additional option for automatic recovery from hardware failures.

Disaster recovery

NicheRMS supports a remote disaster recovery (DR) site in the following ways:

- The DR site can be maintained as a “warm standby” site using SQL Server log shipping or asynchronous database mirroring. The use of asynchronous processes for maintaining the DR site data means that failover to the DR site should be manually triggered. This is normally acceptable as failover to DR is either deliberate (e.g., to allow hardware or network maintenance at the primary site) or is the result of a catastrophic (and very rare) event.
- The DR site can potentially be maintained using synchronous database mirroring, which could allow instantaneous automatic failover. However, this configuration requires some NicheRMS development and requires substantial evaluation and testing because it can have a significant performance impact.
- The DR site can be maintained as a “cold standby” site using SAN mirroring. Failover could be automatic using tools external to NicheRMS, but is more likely to be manual.
- Network resiliency is the responsibility of the police agency.

High software reliability

It is important that the system software, and in particular the server software, which simultaneously handles hundreds of users, operate reliably. The NicheRMS NDS application server software has been designed for continuous operation. Specifically, NDS has the following features:

- Robust internal exception handling that aborts individual operations without affecting the operation of the server software as a whole. These exceptions deal with user, data and programming errors.

- Sophisticated “smart pointer” memory management to prevent memory leaks that cause software failure after long periods of operation.
- Special memory management for large in-memory objects that avoids memory heap fragmentation, which can lead to exhaustion of memory resources after long periods of operation.
- Automated regression testing to catch server programming errors prior to release.
- Detailed server logging to allow most server errors to be detected, diagnosed and corrected from log files without reproducing the error or waiting for it to recur.

Additionally, Niche uses source code control procedures that allow Niche developers to determine which customers are affected by any bug found in the system, either by Niche or by a customer, and to develop any necessary patches for all customers.

Performance monitoring

Thorough system monitoring is essential for reliable operation. NicheRMS monitoring is performed using tools that are compatible with the standard Windows Performance and Alerts service, such as Perfmon. Use of a standard performance-monitoring solution allows customers to integrate NicheRMS monitoring into their system administration processes. For a detailed overview of our support for performance monitoring, please see our responses to [Requirement T4](#) on page 3.

Concurrent access

NicheRMS avoids long-term record locking by using short transactions and application-level mechanisms to drive users to specific records of interest, rather than using an overt "checking out" of in-use records.

The overall application-level locking model is optimistic, *i.e.*, first in wins. The system is designed to support large numbers of users accessing the system simultaneously. To support this, NicheRMS provides multi-function database records that can be updated by multiple users concurrently. Multiple users can work in the same logical NicheRMS record simultaneously without interfering with one another, because each high-level record consists of multiple lower-level entities that can be independently edited.

This is facilitated by the NicheRMS tasking system, which allows specific items of work to be assigned to each team member. While some work will need to be completed in a sequence, other work can take place simultaneously. This means that different personnel can work on the same high-level record at the same time. For example, one officer can open the record to add Log entries at the same time that a member of a Records unit is checking the links to involved persons, vehicles and addresses.

Concurrency control is provided at the level of individual reports that may be attached to a database record, for example, an individual Supplementary report that may be attached to an Occurrence record. For an individual report, only one user can have the report open at a time. Access is restricted to the user who created the report and to that user's supervisor(s).

In addition, the system is configured with Modify and Delete Grace Periods that cause reports to become locked against further modification or deletion after a defined period of time, for all users except system administrators.

Finally, the system is capable of detecting editing conflicts when handling binary records, such as large narrative reports. In these cases, the user is warned that the report has been modified since the last time they retrieved the report from the database, and they are offered an opportunity to save their local changes so they can resolve the differences.

At the RDBMS level, NicheRMS uses the default SQL Server read committed (pessimistic) isolation level, using isolation level overrides and specific locking directives as required to achieve the appropriate levels of performance and data consistency

Requirement: Client System Specifications				
Req. No.	Req. Status	Requirement Description		
T13	M	<p>The Contractor shall provide minimum AND optimum client system specifications for the proposed solution. Responses are for informational purposes only and will not be scored. The Contractor’s response to this requirement shall address, at a minimum, the following:</p> <ul style="list-style-type: none"> • In-car computer system hardware specifications (e.g., RAM, CPU, storage, peripheral ports) • Desktop computer system hardware specifications (e.g., RAM, CPU, storage, peripheral ports) • In-car client over the air network communication specifications • Client operating system specifications • Supported peripherals (e.g., barcode scanner, signature pad, etc) • Supported mobile handheld devices, platforms and specifications • Prerequisite third party client software components (e.g., browser, .NET framework, SQL Express client, etc.) • Any constraints or limitations affecting client-server functionality (e.g., system time variation tolerance, network bandwidth/capacity specifications, network latency tolerance, etc.) 		
Reference additional pages, if necessary. Indicate if the solution is offered or not offered →		<table border="1"> <tr> <td>Offered <input checked="" type="checkbox"/></td> <td>Not Offered <input type="checkbox"/></td> </tr> </table>	Offered <input checked="" type="checkbox"/>	Not Offered <input type="checkbox"/>
Offered <input checked="" type="checkbox"/>	Not Offered <input type="checkbox"/>			
For details on our recommended client system specifications, please see our detailed response to requirement T11 on page 63.				

Niche Technology response – Client System Specifications

Overview

We have provided a detailed overview of our system architecture in response to [Requirement T8](#) on page 32. See page 36. Please see our Supplementary materials section for [Requirement T11](#) (page 63) for full details of the hardware and software infrastructure we recommend to support our system architecture. For convenience, we have provided a copy of the client system specifications below in our Supplementary materials section.

Support for requirements

The Contractor shall provide minimum AND optimum client system specifications for the proposed solution. Responses are for informational purposes only and will not be scored. The Contractor’s response to this requirement shall address, at a minimum, the following:

In-car computer system hardware specifications (e.g., RAM, CPU, storage, peripheral ports)

NicheRMS runs well on any modern PC, and can be run on any Windows device that meets the specifications provided in the Supplementary materials section below. The same NicheRMS app runs on both desktop and mobile systems such as laptop computers and tablets.

The NicheRMS Universal app can be installed natively on a range of Windows OS devices (Windows 7, 8.1 and 10), including PCs, laptops, tablets, notebooks and touchscreen combination devices. Any modern commercial 3G/4G/LTE will provide ample bandwidth to support the NicheRMS app. This will allow all users access to the system whether they are in an office, a patrol vehicle or other mobile location.

Desktop computer system hardware specifications (e.g., RAM, CPU, storage, peripheral ports)

NicheRMS runs well on any modern PC, and can be run on any Windows device that meets the specifications provided in the Supplementary materials section below. The same NicheRMS app runs on both desktop and mobile systems such as laptop computers and tablets.

The NicheRMS Universal app can be installed natively on a range of Windows OS devices (Windows 7, 8.1 and 10), including PCs, laptops, tablets, notebooks and touchscreen combination devices. Any modern commercial 3G/4G/LTE will provide ample bandwidth to support the NicheRMS app. This will allow all users access to the system whether they are in an office, a patrol vehicle or other mobile location.

In-car client over the air network communication specifications

NicheRMS tolerates low bandwidth, high latency 3G/4G mobile networks. Any modern commercial 3G/4G/LTE network provides ample bandwidth to support the NicheRMS app.

Network bandwidth requirements depend on how the system is used. For basic use, 33kbps per active user (typically 10% of logged in users) has been found to be sufficient. Clerical staff require more bandwidth because they usually work faster than officers. Access to large images, scanned documents and Word forms dramatically increases required bandwidth. For more on this, please see the detailed overview of our system architecture in response to [Requirement T8](#) on page 32.

Client operating system specifications

We provide complete client operating system specifications in the table provided below in our Supplementary materials section.

Supported peripherals (e.g., barcode scanner, signature pad, etc)

NicheRMS supports a variety of optional hardware add-ons. This currently includes image capture devices, barcode scanners, card readers, signature tablets, and barcode printers. Please see the table provided below in our Supplementary materials section.

Supported mobile handheld devices, platforms and specifications

The NicheRMS Universal app can be installed natively on a range of Windows OS devices (Windows 7, 8.1 and 10), including PCs, laptops, tablets, notebooks and touchscreen combination devices. Please see the table provided below for more details.

Prerequisite third party client software components (e.g., browser, .NET framework, SQL Express client, etc.)

Please see the table provided below for details of prerequisite software and commonly-used optional software.

Any constraints or limitations affecting client-server functionality (e.g., system time variation tolerance, network bandwidth/capacity specifications, network latency tolerance, etc.)

NicheRMS tolerates low bandwidth, high latency 3G/4G mobile networks. Any modern commercial 3G/4G/LTE network provides ample bandwidth to support the NicheRMS app.

Supplementary material: Client system specifications

Client Workstations

Purpose	Provide end user access to NicheRMS
Operating system	Windows Vista SP2 or higher
CPU	Intel Core2 Duo @ 2.2 GHz or better preferred
RAM	2 GB
Storage	The current NicheRMS desktop install uses roughly 400 MB of storage. This does not account for system prerequisites, additional mobile applications, or custom plug-ins.
Display	<ul style="list-style-type: none"> NicheRMS desktop and NicheRMS mobile applications: Minimum resolution of 1024x768 NicheRMS tablet-compatible mobile application: A minimum of a 7" display. All applications: Video adapter or virtualization suite that is fully compatible with WPF applications
Prerequisite software	<ul style="list-style-type: none"> Microsoft DHTML editor Internet Explorer 7 or higher Microsoft .NET 4.6
Common supporting software	<ul style="list-style-type: none"> Microsoft Word – this is the most common format used for storing documents in NicheRMS Other productivity software (Excel, WordPerfect, Adobe Viewer, Adobe Acrobat, etc.)
Device-specific software	<p>NicheRMS supports a variety of optional hardware add-ons.</p> <p>This currently includes image capture devices, barcode scanners, card readers, signature tablets, and barcode printers.</p> <p>These devices are typically installed on a small subset of the workstation base, and may require additional drivers and software.</p> <p>Any device-specific requirements are in addition to the core NicheRMS application requirements.</p>
Desktop/application virtualization	<p>Niche supports the deployment of NicheRMS user applications in virtualized/streamed environments, e.g., Citrix/RDP services/etc.</p> <p>However, Niche does not perform exhaustive in-house testing using these packages because there are too many possible variations.</p> <p>Customers are encouraged to test their version of NicheRMS in their desired environment, with their proposed configuration.</p> <p>Niche will work to fix any incompatibilities found. Customers may have to upgrade to the latest version of NicheRMS in order for Niche to provide related fixes.</p>
General notes	NicheRMS runs well on any modern PC.

	<p>The specifications above reflect known configurations that run well for regular users at current customer sites.</p> <p>Hardware specifications account for typical use, which includes using Microsoft Word for forms, as well as using Internet Explorer and other related software at the same time as the NicheRMS applications.</p>
Accounting for power users	<p>It is suggested that "power users" (e.g., intel analysts) and those in high-volume or otherwise time-sensitive roles (e.g., custody, contact center) receive higher end workstations when possible.</p> <p>In specific, it is useful for power user workstations to have relatively high single-threaded (i.e., per-core) CPU performance.</p>

Requirement: Transactional Content Processing and Management			
Req. No.	Req. Status	Requirement Description	
T14	M	<p>The Contractor shall provide a comprehensive description of their approach to content management and content processing, including but not limited to:</p> <ol style="list-style-type: none"> 1. Ability for the solution to capture, process and manage transactional content, defined as a system of record for managing process related documents, including, but not limited to, the following: <ul style="list-style-type: none"> o Electronic document files o Electronic images o Audio / Video files <p>The proposed solution should identify the type of file formats that will be supported as part of the system.</p> 2. Ability for the solution to store, manage and retrieve transactional content in a New York State Information Technology Services (ITS) provided enterprise content management repository 3. If the proposed solution does not leverage the NYS ITS enterprise content management repository (requirement T14 - Item #2), describe how the proposed system demonstrates compliance with system performance, reliability, availability and scalability in reference to user population characteristics as defined in RFQ Table 1 Expected Implementation Schedule, and if the proposed solution uses a relational database to store content in a CHARACTER or BINARY LARGE OBJECT (CLOB or BLOB) attribute. 4. If the proposed solution does not leverage the NYS ITS enterprise content management repository (requirement T14 - Item #2), describe the recommended data maintenance and data recovery measures for handling file system growth for the relational database if it is used as a storage area for transactional content. 	
<p>The Contractor shall provide a comprehensive description of how the proposed solution satisfies the requirement including technical specifications, capabilities, features, considerations, constraints, and limitations. Reference additional pages, if necessary.</p> <p>Reference additional pages, if necessary. Indicate if the solution is offered or not offered →</p>		<p>Offered <input checked="" type="checkbox"/></p>	<p>Not Offered <input type="checkbox"/></p>
<p>Niche Technology response: see our response material immediately following this table.</p>			

Niche Technology response – Transactional Content Processing and Management

Overview

External files, including digital media content can be attached to NicheRMS records including Incident records, and master index records for persons, addresses, vehicles and property, *etc.* You can link external files to any of these record types by browsing to their Windows folder location and selecting them. Some imported files will be stored directly in the NicheRMS database as attachments to NicheRMS database records. Other larger digital files such as audio and video are not stored within NicheRMS. They are stored outside and NicheRMS holds the URL to launch the file. In all cases, the file in question will be available to authorized users.

Support for requirements

1. ***Ability for the solution to capture, process and manage transactional content, defined as a system of record for managing process related documents, including, but not limited to, the following:***
 - ***Electronic document files***
 - ***Electronic images***
 - ***Audio / Video files***

The proposed solution should identify the type of file formats that will be supported as part of the system.

External document files, images and audio/visual files can either be imported into NicheRMS and attached directly to the Incident or other database record to which they apply, or they can be stored in an external content management system. Access to files in an external content management system is provided via URL, i.e., the record in NicheRMS provides a URL that users can follow to access the content.

There are no restrictions on the number of files that can be added: However, if users are opening a file of a particular type, they must have an application installed that is capable of opening the file, e.g., Windows Media Player, Adobe Reader, Microsoft Word, Excel, etc. Once imported, users can click or tap a link to open it. The file opens using the application associated with the file type.

There is no technical limit on the type of file format that can be supported. Customer administrators set system parameters to control which file types are allowed to be imported into NicheRMS and the file size. This prevents users from attaching non-standard files for which other users do not have installed viewers/editors. If a file is larger than allowed, the user is warned and the file is not imported.

2. ***Ability for the solution to store, manage and retrieve transactional content in a New York State Information Technology Services (ITS) provided enterprise content management repository.***

NicheRMS can be interfaced to a Digital Asset Management System (DAMS) or enterprise content management system. It is also possible to store some documents and files inside NicheRMS and some outside.

Although the limit is adjustable, we generally recommend that files over about 10MB in size not be stored in the NicheRMS database. NicheRMS can be configured to disallow very large files from being stored in the NicheRMS database.

Please see our Supplementary materials section below for more on this.

- 3. If the proposed solution does not leverage the NYS ITS enterprise content management repository (requirement T14 - Item #2), describe how the proposed system demonstrates compliance with system performance, reliability, availability and scalability in reference to user population characteristics as defined in RFQ Table 1 Expected Implementation Schedule, and if the proposed solution uses a relational database to store content in a CHARACTER or BINARY LARGE OBJECT (CLOB or BLOB) attribute.**

As we have said, NicheRMS can be interfaced to a Digital Asset Management System (DAMS) or enterprise content management system. It is also possible to store some documents and files inside NicheRMS and some outside.

Files stored in the database are compressed with LZ77 compression, which can be uncompressed using the WinZip® application or GZIP (gnu ZIP). LZ77 compression is essentially what the WinZip application uses for all files, except that the WinZip file format supports a directory structure on top of the basic file compression. However, WinZip also uncompresses the raw LZ77 format that we use. Administrators can locate BLOB records by searching for a Hostid that matches the allowed entity type (e.g., 1655% and type LIKE '%DOC%').

- 4. If the proposed solution does not leverage the NYS ITS enterprise content management repository (requirement T14 - Item #2), describe the recommended data maintenance and data recovery measures for handling file system growth for the relational database if it is used as a storage area for transactional content.**

See our answers above. Note that growth in database size does not usually have a serious impact on system load. It does, of course, require the storage subsystem to grow, but modern SAN systems allow expansion of storage and the database server allows the database to be extended on a single storage volume or onto multiple storage volumes.

Supplementary material: Transactional Content Processing and Management

External files, including digital media content can be attached to NicheRMS records including incident records, and master index records for persons, addresses, vehicles and property, etc. You can link external files to any of these record types by browsing to their Windows folder location and selecting them. The imported file is stored as an attachment to the NicheRMS database record.

Numbers and types of files

There are no restrictions on the number of files that can be added: However, if users are opening a file of a particular type, they must have an application installed that is capable of opening the file, e.g., Windows Media Player, Adobe Reader, Microsoft Word, Excel, etc. Once imported, users can click or tap a link to open it. The file opens using the application associated with the file type.

Your administrators set system parameters to control which file types are allowed to be imported into NicheRMS and the file size. This prevents users from attaching non-standard files for which other users do not have installed viewers/editors. If a file is larger than allowed, the user is warned and the file is not imported.

File sizes

Although the limit is adjustable, we generally recommend that files over about 10MB in size not be stored in the NicheRMS database. NicheRMS can be configured to disallow very large files from being stored in the NicheRMS database.

External files can also be bulk-imported using the NicheRMS Bulk Document Loader (BDL), a utility that is included with the NicheRMS software. As a first step, a high volume scanner can be used to bulk-scan the

documents into a Windows folder. The BDL accesses the Windows folder and attaches the files to specified NicheRMS records.

NicheRMS provides a unified user experience covering both documents and photos stored within NicheRMS, and digital assets stored in an enterprise content management repository, as we describe below.

Documents and photos, including bit-maps, TIFF files, PDFs, Excel and Word files:

Users can import and attach these types of files directly to relevant NicheRMS records, and once imported, they can be opened directly in the app.

If you prefer NOT to store scanned documents in the NicheRMS database, NicheRMS can also be interfaced to a Digital Asset Management System (DAMS) or enterprise content management system. It is also possible to store some documents inside NicheRMS and some outside.

The user process for accessing documents stored in NicheRMS is very similar to the process for accessing documents held in a DAMS or content management system, *i.e.*, users do not have to be concerned with where a document is stored. They just click a link to display the file.

Audio and video files

Larger digital assets such as audio and video are not stored within NicheRMS. They are stored outside and NicheRMS holds the URL to launch the file.

For the user, there isn't much difference between accessing a document in the NicheRMS database and a digital asset stored in a DAMS or enterprise content management system.

When users follow a link from NicheRMS to the digital file, it retrieves the data from the DAMS. This allows NicheRMS users to access and manage video (*e.g.*, CCTV or body-worn video) while working in NicheRMS. NicheRMS data export processes can export the references to the videos or the actual videos, depending on requirements of the export process and the capabilities of the video storage/management system being used.

w