RESOLUTION NO. 2022 - 442

A RESOLUTION BY THE BOARD OF COUNTY COMMISSIONERS OF ST. JOHNS COUNTY, FLORIDA, AUTHORIZING THE COUNTY ADMINISTRATOR, OR DESIGNEE, TO EXECUTE AMENDMENT 2 TO MISC NO: 17-87; MASTER PURCHASE AGREEMENT BETWEEN ST. JOHNS COUNTY, FL, AND MOTOROLA SOLUTIONS, INC., FOR THE UPGRADE AND MODERNIZATION OF EXISTING TECHNOLOGY IN THE AMOUNT OF $14,716,774.00 WHICH INCLUDES THE PURCHASE, INSTALLATION, SUBSCRIPTION AND SERVICES FOR ALL ITEMS.

RECITALS

WHEREAS, the County currently owns, operates, and maintains the public safety interoperable radio systems for the provision of public safety services providing law enforcement, firefighting, ambulance, emergency medical, emergency management, and other emergency government-related services to the citizens of St. Johns County; and

WHEREAS, the County and Motorola Solutions, Inc ("Motorola"), entered into a Master Purchase Agreement in March 2017, to allow for the purchase of products and services in support of the interoperable radio systems as needed to maintain the system(s) up-to-date with technology, in order to best serve the County; and

WHEREAS, the proposed upgrade will provide updated technology, equipment, and service that will allow SJC Fire Rescue and St. Johns County Sheriff's Office to maximize the public safety services which utilize the interoperable radio systems throughout the County; and

WHEREAS, Motorola will provide equipment, technology upgrades, subscriptions and services to ensure the highest level of performance of the existing systems and all newly added components and equipment; and

WHEREAS, the attached Amendment 2 to the Master Purchase Agreement sets forth the obligations of the County and Motorola; and

WHEREAS, the County intends to finance the funds to support the cost of executing Amendment 2, and will appropriate funds within the appropriate fiscal years, as outlined in Motorola's proposal.

NOW, THEREFORE BE IT RESOLVED BY THE BOARD OF COUNTY COMMISSIONERS OF ST. JOHNS COUNTY, FLORIDA, as follows:

Section 1. The above Recitals are incorporated by reference into the body of this Resolution and such Recitals are adopted as finds of fact.

Section 2. The County Administrator, or designee, is hereby authorized to execute Amendment 2 to the Master Purchase Agreement.

Section 3. To the extent that there are typographical and/or administrative errors that do not change the tone, tenor, or concept of this Resolution, then this Resolution may be revised without subsequent approval by the Board of County Commissioners.

PASSED AND ADOPTED by the Board of County Commissioners of St. Johns County, Florida, on this 15th day of November, 2022.

BOARD OF COUNTY COMMISSIONERS OF ST. JOHNS COUNTY, FLORIDA

By: Henry Dean
Chair

ATTEST: Brandon J. Patty,
Clerk of Circuit Court & Comptroller

By: Robin L Pilcher
Deputy Clerk

NOV 17 2022
Rendition Date_____

AMENDMENT TWO TO THE MASTER PURCHASE AGREEMENT BETWEEN ST. JOHNS COUNTY AND MOTOROLA SOLUTIONS, INC.

THIS AMENDMENT TWO TO THE AGREEMENT, by and between St. Johns County Board of County Commissioners, Florida (County), and Motorola Solutions, Inc., a Delaware corporation authorized to transact business in the State of Florida (Motorola); collectively referenced as "Parties".

WHEREAS, the County and Motorola entered into a Master Purchase Agreement No. 227662 for radio communications equipment, products and services, dated March 23, 2017 ("Agreement");

WHEREAS, the County and Motorola signed the Amendment One to the Agreement on June 25, 2019 to provide certain products and services described in said amendment;

WHEREAS, Section 16.8 of the Agreement provides that any changes to the Agreement must be documented in writing and signed by each party's authorized signatories;

WHEREAS, the parties wish to include additional equipment and services to the Agreement;

And

NOW, THEREFORE, the County and Motorola hereby agree to add the terms and conditions to the Agreement as follows:

1. The exhibits listed below are incorporated into and made a part of this Agreement:

Exhibit A	Payment Schedule
Exhibit B	Motorola's Proposal dated September 12, 2022 (the "Proposal")
Exhibit C	Additional Terms and Conditions: 1. Subscription Software Addendum 2. Data Processing Addendum

For clarity, the terms and conditions described in Exhibit C would prevail over the ones in the Agreement (No. 227662) only with respect of the offering described in the Proposal.

2. TERM

The parties wish to continue using the renewal option stated in Section 4 of the Agreement.

3. CONTRACT PRICE. The Contract Price in U.S. dollars is modified to include an additional $14,716,774, for the work described in Motorola's Proposal, Exhibit B. The pricing summary is set forth in Section 5 Pricing of Exhibit B. Motorola has priced the services, Software, and Equipment as an integrated system. A reduction in Software or Equipment quantities, or services, may affect the overall Contract Price, including discounts if applicable.

4. Customer affirms that a purchase order or notice to proceed is not required for contract performance or for subsequent years of service, if any, and that sufficient funds have been appropriated in accordance with applicable law. The Customer will pay all invoices as received from Motorola and any changes in scope will be subject to the change order process as described in this Agreement. At the time of execution of this Agreement, the Customer will provide all necessary reference information to include on invoices for payment in accordance with this Agreement.

5. INFLATION REVIEW. For multi-year agreements, at the end of the first year of the Agreement and each year thereafter, a CPI percentage change calculation shall be performed using the U.S. Department of Labor, Consumer Price Index, "All Items," Unadjusted Urban Areas (CPI-U). Should the annual inflation rate increase greater than 3% during the previous year, Motorola shall have the right to increase all future

maintenance prices by the CPI increase amount exceeding 3%. "All Items," not seasonally adjusted shall be used as the measure of CPI for this price adjustment. The adjustment calculation will be based upon the CPI for the most recent twelve (12) month increment beginning from the most current month available as posted by the U.S. Department of Labor (http://www.bls.gov) immediately preceding the new maintenance year. For purposes of illustration, if in Year 5 the CPI reported an increase of 8%, Motorola may increase the Year 6 price by 5% (8%-3% base).

Except as set forth in this Amendment Two, all other terms and conditions of the Agreement remain unchanged and in full force and effect.

IN WITNESS WHEREOF, the County and Motorola execute this Amendment Two to the Agreement as follows:

St. Johns County Board of County
Motorola Solutions, Inc.

Motorola: Motorola Solutions, Inc.

By: _____

Name: _____

Title: _____

Date: _____

Customer: St. Johns County FL Board of County Commissioners

By: _____

Name: _____

Title: _____

Date: _____

EXHIBIT A

Payment Schedule for PSA System Agreement

Except for a payment that is due on the Effective Date, Customer will make payments to Motorola within thirty (30) days after the date of each invoice. Customer will make payments when due in the form of a check, cashier's check, or wire transfer drawn on a U.S. financial institution. If Customer has purchased additional Professional or Subscription services, payment will be in accordance with the applicable addenda. Payment for the System purchase will be in accordance with the following milestones.

System Purchase Including Yrs 2&3 APXNext Software Subscriptions (excluding Subscribers)

1. **20% of the System Price due upon Execution of Contract (due upon receipt);**
2. **20% of the System Price due upon Completion of Project Kickoff/Contract Design Review;**
3. **35% of the System Price due upon Delivery of applicable System Hardware and Application Software to Customer Site;**
4. **10% of the System Price due upon Installation at Customer Site;**
5. **10% of the System Price due upon Successful Completion of System Live Cut; and**
6. **5% of the System Price due upon Final Acceptance.**

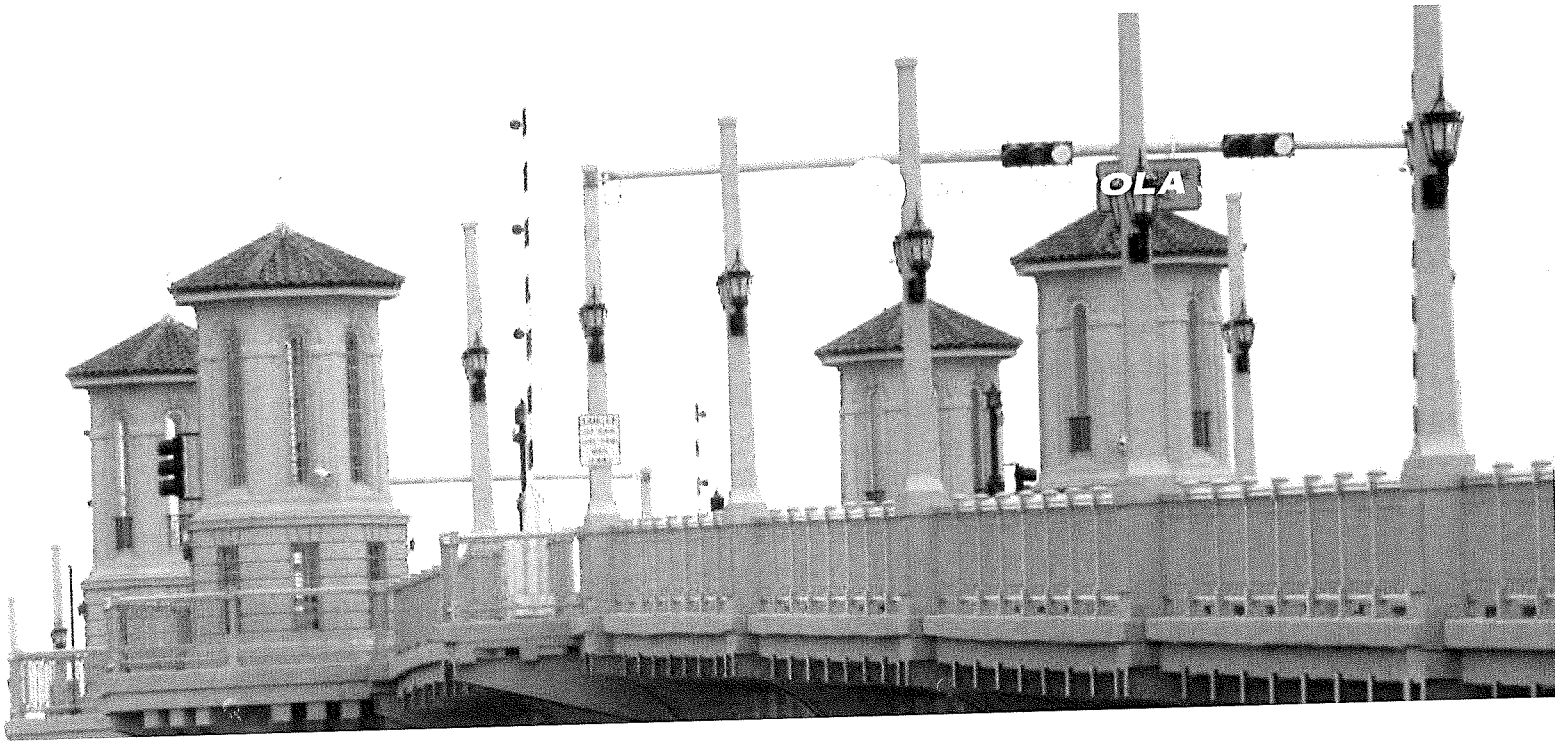
100% of the Subscriber Contract Price will be invoiced upon shipment (as shipped).

Motorola shall make partial shipments of equipment and will request payment upon shipment of such equipment. In addition, Motorola shall invoice for installations completed on a site-by-site basis or when professional services are completed, when applicable. The value of the equipment shipped/services performed will be determined by the value shipped/services performed as a percentage of the total milestone value. Unless otherwise specified, contract discounts are based upon all items proposed and overall system package. For invoicing purposes only, discounts will be applied proportionately to the FNE and Subscriber equipment values to total contract price. Overdue invoices will bear simple interest at the maximum allowable rate by state law.

For Lifecycle Support Plan Services:
Motorola will invoice Customer annually in advance of each year of the plan.

EXHIBIT B

MOTOROLA PROPOSAL DATED SEPTEMBER 12, 2022



Proposal

St. Johns County, FL

State-of-the-Art Technology for a Safe and Resilient Community

September 12, 2022

Motorola Solutions, Inc.
401 E. Las Olas Boulevard, 16th Floor
Ft. Lauderdale, FL 33301

September 12, 2022

Hunter Conrad, Administrator
St. Johns County Administration
500 San Sebastian View
St. Augustine, Florida 32084

Subject: Public Safety Technology for a Safe and Resilient Community

Dear Mr. Conrad:

Motorola Solutions, Inc. (Motorola Solutions) appreciates the opportunity to provide your first responders the APX NEXT technology, combining LMR and LTE for the first time, and our PremierOne Suite of applications to achieve better outcomes for your citizens and first responders. This is life-saving technology that will continue to change the way your first responders operate for years to come. Our design includes:

- **APX NEXT Radios**, with Radio Central for device management, for the Sheriff's Office and Fire Rescue to upgrade and modernize their existing 2011 technology. APX NEXT includes CommandCentral Aware Mapping for a web-based common operating picture to enhance collaboration and decision–making. You can view all your first responder's location-based data together, on a single map display.
- Addition of the Sheriff's Office to the existing County **PremierOne CAD/Mobile** System for improved collaboration, allowing a coordinated and quick response when your citizens call 911 and need help. PremierOne CAD will display location data from APX Next subscribers by importing SmartLocate data, making it safer for your first responders.
- Sheriff's Office **PremierOne Records/Mobile** provides complete integration across the suite of applications by accurately capturing and securing all records data into a single repository for advanced information sharing, powerful efficiencies and security.
- Sheriff's Office **Jail Solution for PremierOne** captures and integrates corrections data system-wide, creating seamless data flow, and allowing users to process inmates from start to finish more efficiently, while also improving jail safety and drastically improving the release process.

Motorola Solutions and St. Johns County have been partners for many years, providing mission critical communications and software solutions to enhance the lives of your citizens while keeping your first responders safe. We look forward to continuing this partnership for many years to come. Given the breadth of our solution, our deployment will be a phased implementation, allowing the County flexibility and not over burdening staff. The benefit of contracting for all of these solutions at one time is the economy of scale that Motorola Solutions is able to pass on to the County which translates to **$1,615,600 dollars of additional incentive** above and beyond the contract discounts.

Motorola Solutions, Inc.
401 E. Las Olas Boulevard, 16th Floor
Ft. Lauderdale, FL 33301

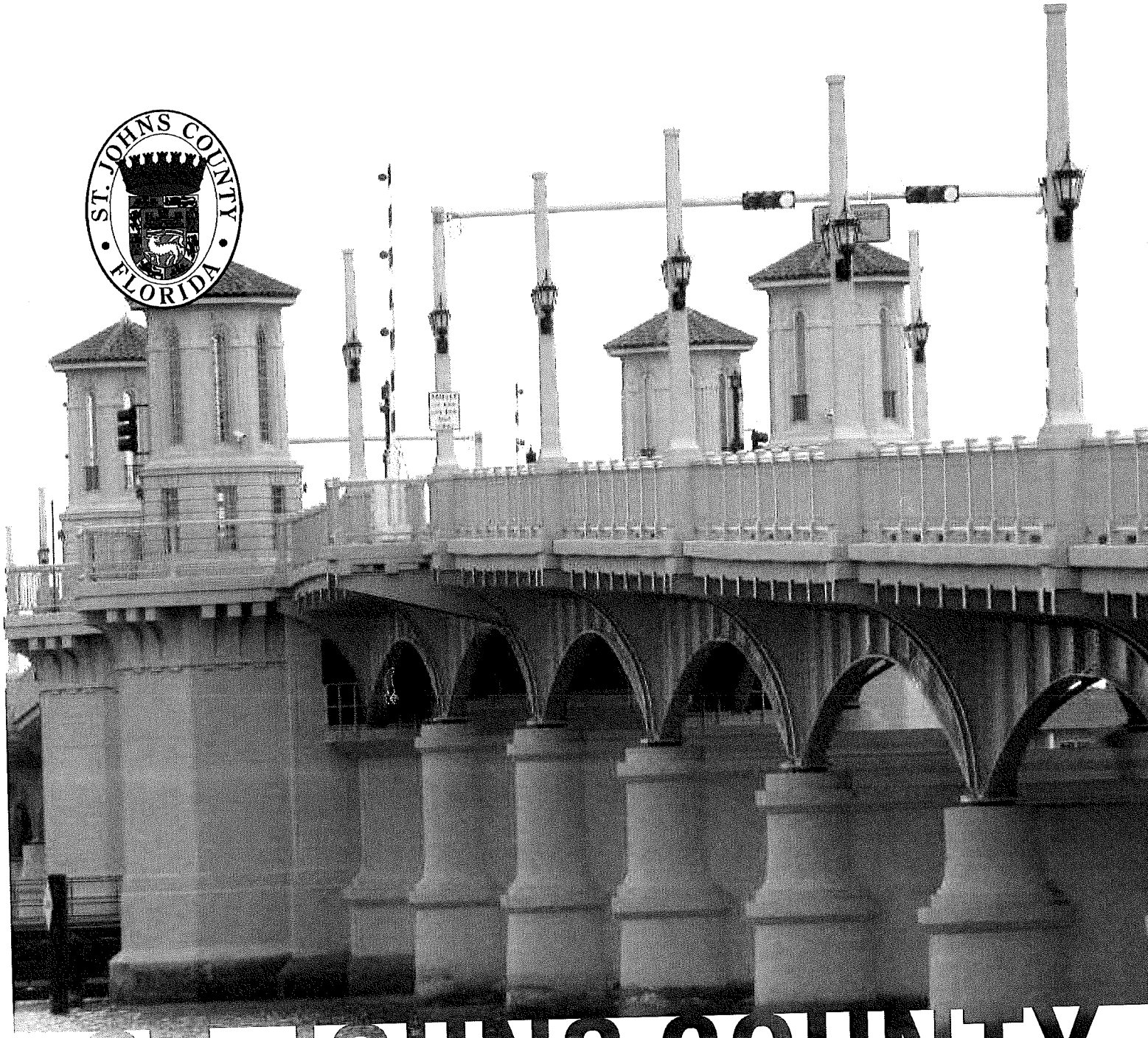
Motorola Solution's proposal is conditional upon a negotiated Second Amendment to the existing Master Purchase Agreement between St. Johns County and Motorola Solutions, Inc. **Pricing will remain valid until November 18, 2022.**

Motorola Solutions is honored to partner with St Johns County first responders and appreciates consideration of this proposal. Any questions the County has regarding this proposal can be directed to Michelle Poole, Area Sales Manager, 904-814-9938 or at michelle.poole@motorolasolutions.com. Our goal is to provide St. Johns County with the best products and services available in the communications industry. We thank you for the opportunity to present our proposed solution.

Sincerely,
MOTOROLA SOLUTIONS, INC.

Scott Adler
Regional Vice President, Southeastern Territory
North America Government Markets

Table of Contents

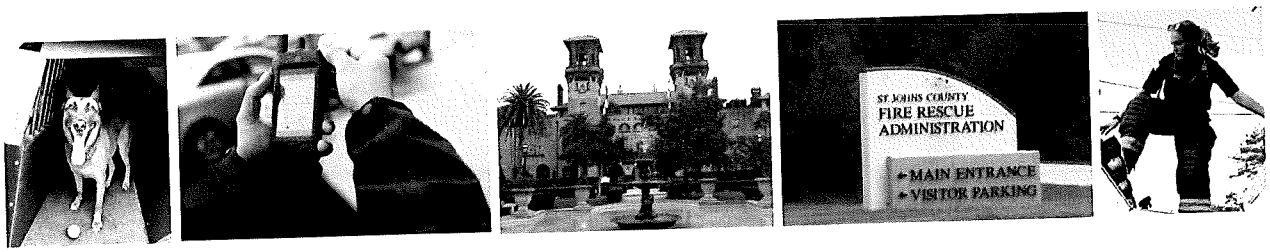


ST. JOHNS COUNTY

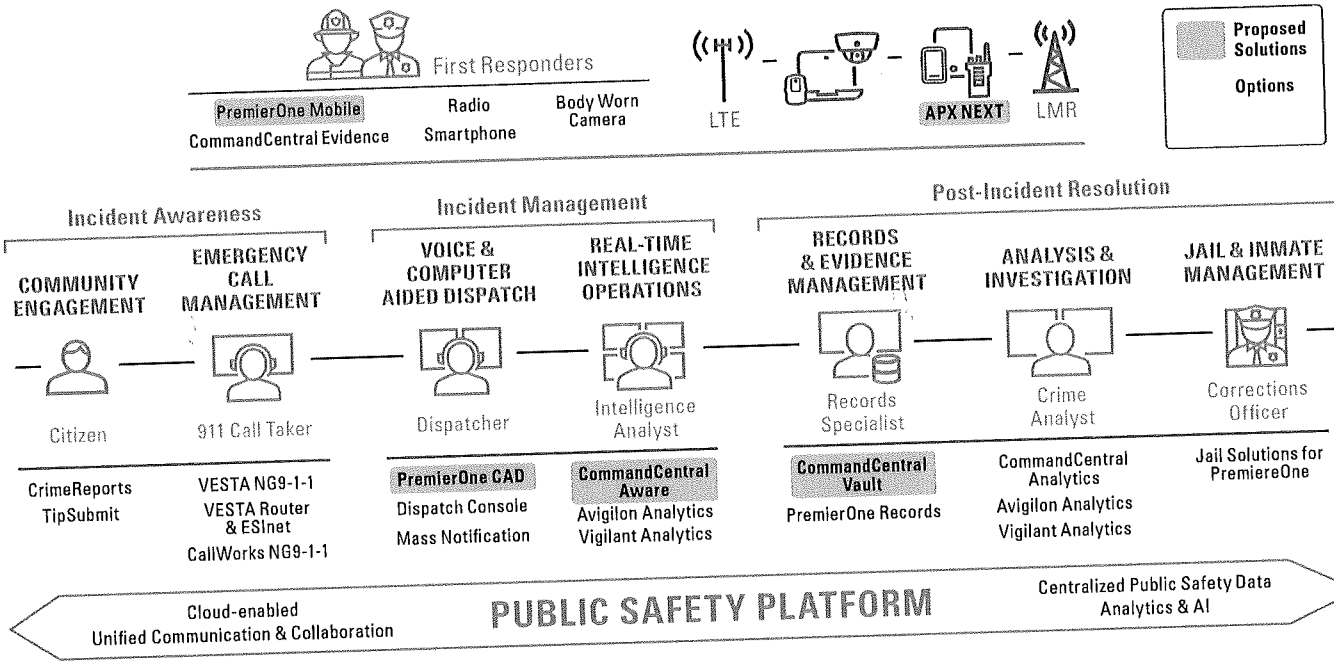
STATE-OF-THE-ART TECHNOLOGY FOR A SAFE & RESILIENT COMMUNITY

EXECUTIVE SUMMARY

MOTOROLA SOLUTIONS



Motorola Solutions' proposed end-to-end suite of mission critical voice and data technology is the future of proactive and technology-driven public safety. It combines our proven P25 infrastructure with the industry's only fully integrated LMR/LTE device and a wealth of leading-edge advancements in CAD and Real Time Crime Center applications to deliver better results in the suppression and prevention of crime.



The current proposal offers a comprehensive solution to unify and simplify operations, improving St. Johns County's ability to reduce crime and to collaborate with other agencies for the protection of your citizens. It modernizes your handheld devices, maximizing the benefit of your current radio network and adds new technology to create end-to-end operational efficiencies that will improve outcomes throughout the County.

We believe that this is an opportunity for St. Johns County to become a leader in the state of Florida, seizing the opportunity to deploy this technology, combining LMR and LTE for the first time, and protecting citizens and first responders with the best new and emerging technology for voice and data. This is life-saving technology that will help you to expand services and "take care of people" for St. Johns County.

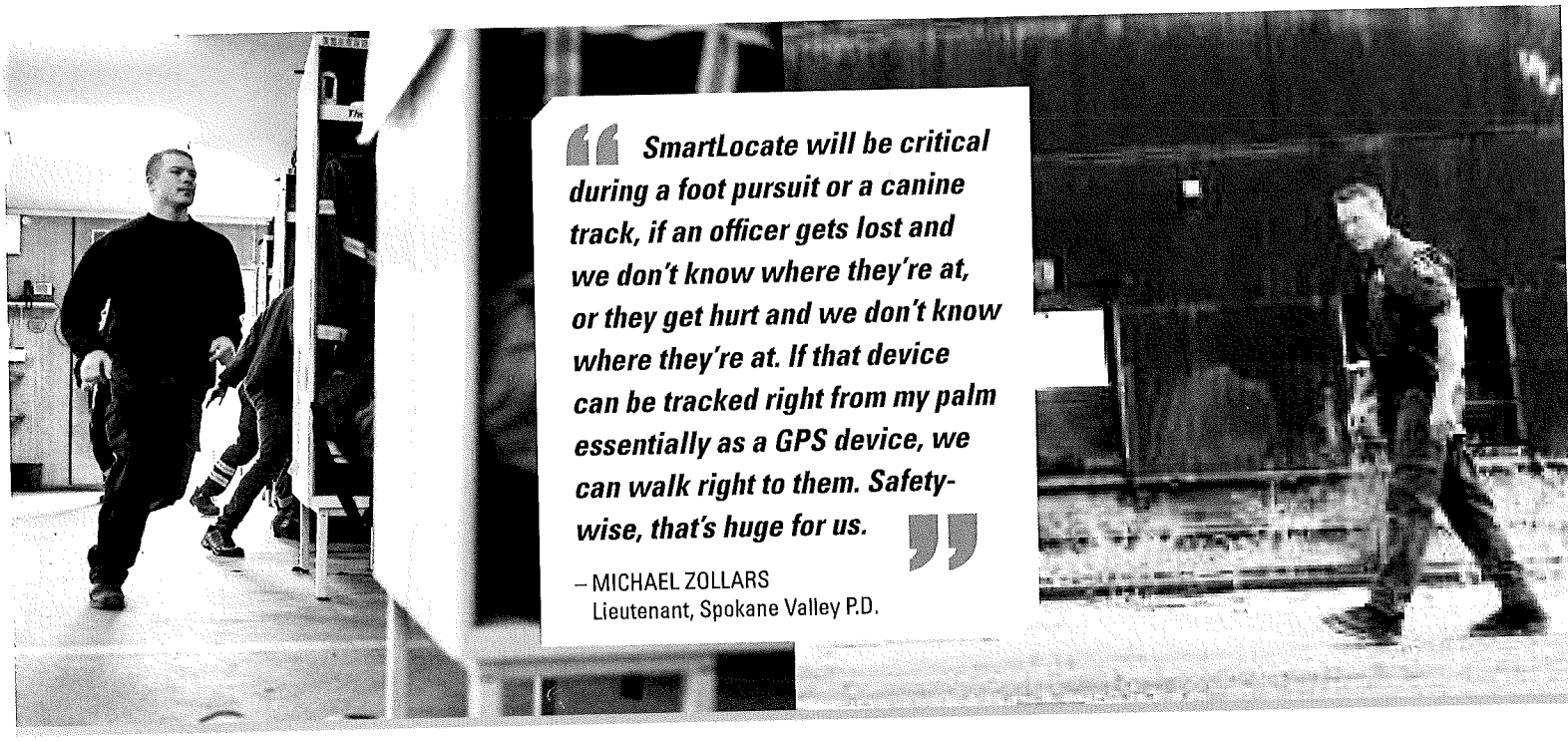
> ***"This is an evolution...It's important that we don't lose sight of the fact that the radio, number one, needs to be able to push that green button and talk to someone on the other end. But at the same time, we're now seeing these technologies being integrated with new things – cameras, phones, email, messaging, pictures."***
>
> – KEVIN ASWINANUN
> Management Information Systems
> Coordinator, Prince William County P.D.

APX NEXT DEVICES

Motorola Solutions is proposing APX NEXT radios for St. Johns County, to upgrade and modernize your existing technology.

Feature	APX 6000/6000XE	APX NEXT/XE
SmartConnect* – Seamless PTT over LTE & LMR	✗	✓
SmartLocate* – Seamless Location Tracking over LTE & LMR	✗	✓
SmartMapping* – Location Tracking on Device Screen	✗	✓
SmartMessaging* – Multimedia Messaging	✗	✓
ViQi Virtual Partner* – Voice Database Query	✓ (over LMR)	✓
ViQi **Voice Control**	✗	✓
Broadband	✗	✓ LTE & WiFi
All-Band Option	✗	✓
Standard Channels	1000	3000
Encryption over LTE	✗	✓
HazLoc	Class I, Div 1	Class I, Div2
Adaptive Noise Suppression	✗	✓
Integrated Bluetooth	✓ 2.0	✓ 5.0

**Available only with LTE*



> ***SmartLocate will be critical during a foot pursuit or a canine track, if an officer gets lost and we don't know where they're at, or they get hurt and we don't know where they're at. If that device can be tracked right from my palm essentially as a GPS device, we can walk right to them. Safety-wise, that's huge for us.***
>
> – MICHAEL ZOLLARS
> Lieutenant, Spokane Valley P.D.

VOICE AND DATA ON ONE DEVICE
FASTER DECISION MAKING, BETTER OUTCOMES

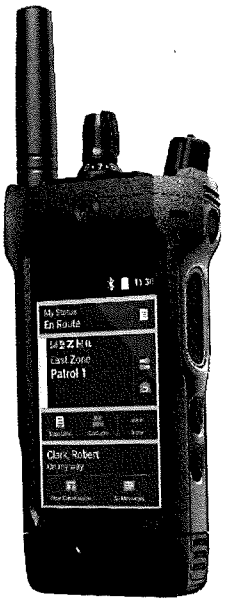
The APX NEXT combines voice and data capabilities on a single, rugged and easy-to-use device, preserving the lifeline between first responders, and improving their link to the command center with high-speed data capabilities for improved connectivity and real-time operational insight.

ViQi Virtual Assistant

Officers can run routine database queries autonomously. Dispatchers can focus on responding to the most critical situations. And the intelligence that keeps first responders safe is moved to the field faster than ever.

SmartProgramming

Your radios should be in the field, not in the shop. SmartProgramming enables you to update your APX radios with zero touch. Encryption keys and software patches can be automatically pushed via broadband LTE.



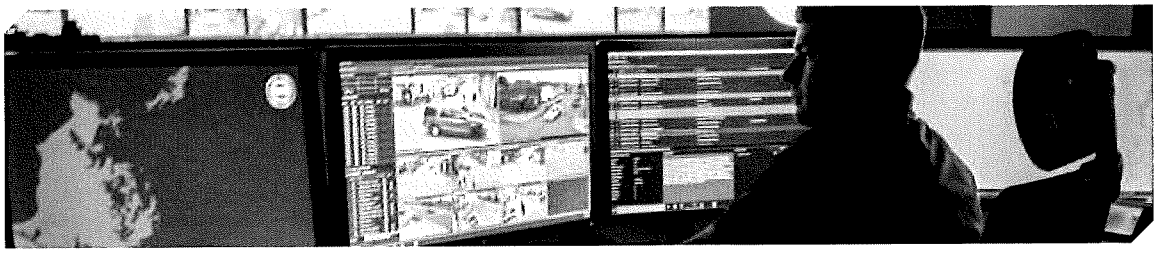
SmartLocate

Location updates every few seconds, so you always know where your team is, while freeing capacity on your 800 MHz system for other uses. Broadband LTE connectivity radically improves location refresh rates and expands the number of devices that can be tracked simultaneously.

SmartConnect

Stay connected to your P25 system, even outside of 800 MHz coverage. SmartConnect maintains your P25 voice and data communications by automatically switching between P25 and broadband.

Users can see their exact location - and the location of other units in the area - on mobile or portable devices, with push-to-talk connectivity over LTE networks, and easy access to remote information - such as suspect and license plate data. This will result in better communication, highly informed decision making, and lightning-fast operational agility - with less equipment to manage and more time to focus on mission critical activities.



PREMIERONE

PremierOne CAD software allows dispatchers to provide officers with complete data on every situation including the incoming call, related records and responder location and status. With access to all critical information, dispatchers can help first responders achieve a safer and more prepared response based on precise data that is specific to your agency's workflow.

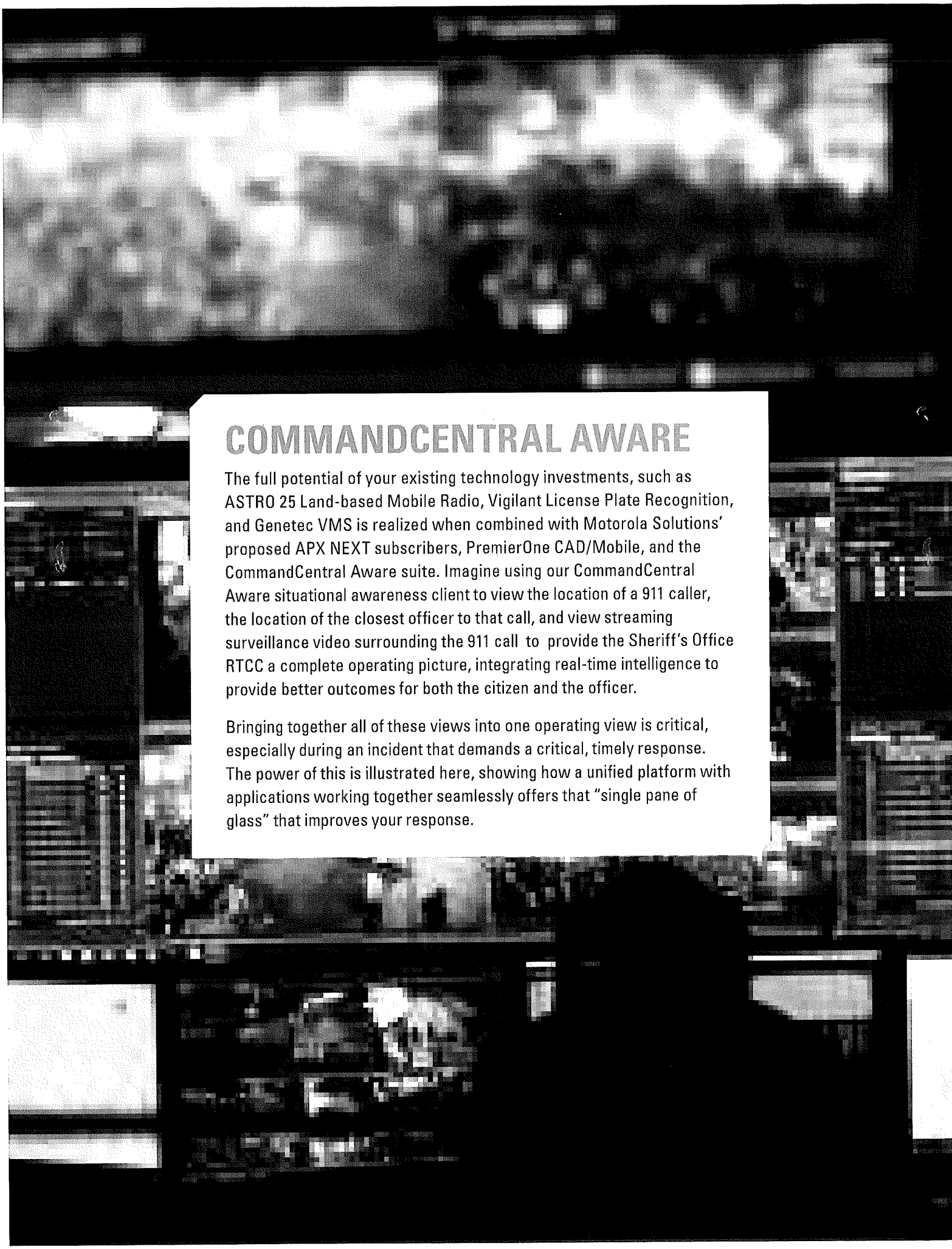
Also, PremierOne CAD/Mobile fully extends command center information to the vehicle – location, history, hazard data, video feeds, and building plans, for enhanced real time decisions. In summary, PremierOne CAD software helps improve your team's response times, efficiently allocate resources and better inform first responders through greater information gathering and situational awareness.

- MAXIMIZE COLLABORATION AND EFFECTIVENESS – Optimize interoperability to keep everyone connected in real time. Increased collaboration means faster and better responses for the citizens of St. Johns County.
- KEEP OFFICERS AND CITIZENS SAFE – Maintain situational awareness as incidents escalate, with real time response location, status information, and alerts.
- INCREASE PRODUCTIVITY – PremierOne's unified workflows create new efficiencies, allowing officers to spend less time writing reports and more time on the street.
- LEVERAGE EXISTING INVESTMENTS – In June 2019, St. Johns County BOCC approved the purchase of Motorola's PremierOne CAD system. With our proposed solution of adding the sheriff's office to the existing county PremiereOne CAD, both agencies will have seamless collaboration, improving the safety of The County's citizens and its first responders.

PREMIERONE RECORDS AND RECORDS MOBILE

Whether officers need to create reports while in the field or personnel needs help organizing and sharing records data, PremierOne Records provides complete integration across the suite of applications. PremierOne Records and its included 40 plus modules are a robust records management system that accurately captures and secures all records data into a single repository for advanced information sharing, powerful efficiencies and security.

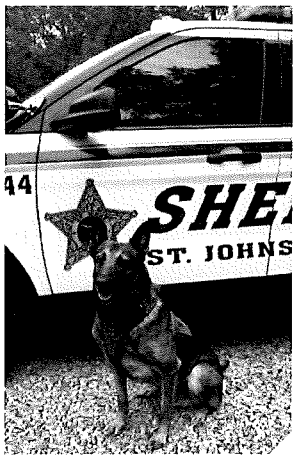
- PremierOne Records also gives every agency the power to change and add fields to every form and report without vender involvement, utilizing our Advanced Configuration Tool.
- Create entirely new modules with PremierOne Records and have those fields and modules searchable.



COMMANDCENTRAL AWARE

The full potential of your existing technology investments, such as ASTRO 25 Land-based Mobile Radio, Vigilant License Plate Recognition, and Genetec VMS is realized when combined with Motorola Solutions' proposed APX NEXT subscribers, PremierOne CAD/Mobile, and the CommandCentral Aware suite. Imagine using our CommandCentral Aware situational awareness client to view the location of a 911 caller, the location of the closest officer to that call, and view streaming surveillance video surrounding the 911 call to provide the Sheriff's Office RTCC a complete operating picture, integrating real-time intelligence to provide better outcomes for both the citizen and the officer.

Bringing together all of these views into one operating view is critical, especially during an incident that demands a critical, timely response. The power of this is illustrated here, showing how a unified platform with applications working together seamlessly offers that "single pane of glass" that improves your response.



Every day, our public safety customers rely on effortless and reliable communications to keep their communities safe. They call it their lifeline. At Motorola Solutions, we not only build that lifeline – with mission-critical services, software, video, and analytics, backed by secure, resilient land mobile radio communications – we advance it every day through our commitment to innovation.

Our drive for continuous innovation and partnership with St. Johns County Sheriff's Office enables you to be ready – in the day-to-day moments, and in the moments that matter most.

MOTOROLA SOLUTIONS

Section 1

System Description

State-of-the-Art Technology for a Safe and Resilient Community

September 12, 2022

St. Johns County, FL

Table of Contents

Section 1

System Description

1.1 APX Radios and Features

1.1.1 Overview

APX NEXT and APX NEXT XE are Motorola Solutions' next-generation P25 platforms purpose-built for first responders to access and act on information while maintaining their focus in critical situations. With natural and accessible touch interface, best-in-class audio optimized for high-noise environments, and extended coverage through broadband connectivity, APX NEXT and APX NEXT XE deliver actionable intelligence to the point of engagement for personnel to stay connected and in control wherever the mission takes them. In addition, APX NEXT XE delivers all of this in a form factor designed for extreme environments.

Figure 1-1:APX NEXT Radios

Equipped with broadband, LTE, Wi-Fi, Bluetooth 5.0, and GPS capabilities, APX NEXT brings future-ready applications, services, and best-in-class connectivity to the field and control room. The APX NEXT platform's cloud-based provisioning system will allow your agency to quickly procure, provision, and update the APX NEXT fleet, reducing the downtime needed to get devices into the field and saving your support staff valuable time.

Key benefits and advanced capabilities of the APX NEXT device include the following:

- SmartTouch Experience – Easier operation with a redefined touch UI, centered around a new 3.6-inch impact resistant touch display and shallow menu hierarchy that offer more information at a glance and quicker engagement with critical applications. This cleaner and more intuitive visual layout increases the usability of the APX NEXT radio and helps your users find the information they need without pause or distraction.
- Ruggedized, Ergonomic Design – Increased personnel safety and efficiency with an improved T-Grip ergonomic design, full-color top display, and tactile knobs for efficient use in emergency situations. Patented touch technology enables for reliable gloved use, while also making the screen immune to false actuations from water, snow, ice, or debris. The APX Next device meets the same MIL standards for ruggedization achieved by our APX platform radios.
- Interoperability – Supports all public safety frequency bands (7/800 MHz, VHF, UHF) for full interoperability across radio systems with minimal intervention by the radio user.
- Easy Fleet Management – Easier and quicker radio provisioning, remote updates, and streamlined management for support staff, delivering greater awareness of your APX NEXT fleet. Using Motorola Solutions' cloud-based RadioCentral (RC) programming, APX NEXT supports faster provisioning and deployment to get devices in the hands of responders and out into the field.

Across all aspects of the radio experience — deployment, operation, maintenance, and evolution — APX NEXT brings critical advancements to usability and performance. This platform brings streamlined interfaces, accelerated workflows, and mission-critical reliability to your agency's operation, while the focus that responders, dispatchers, and technicians need to stay safe and effective is protected.

1.1.2 Evolving with Application Services

If proposed, a host of application services will enhance the APX NEXT device's capabilities in the following ways:

- Quick access to immediate, actionable intelligence via intuitive voice control and ViQi—a virtual partner that can run tags and provide detailed information through voice.
- Better coverage through automatic switching between LMR and broadband connectivity via SmartConnect.
- Accurate location data over a broadband network for more informed decision making via SmartLocate.
- Immediate software and security updates in the field using high-speed bandwidth and extended coverage of LTE networks via SmartProgramming.
- Precise and accessible location information for field users on a modernized map interface via SmartMapping.
- Seamless and discrete multimedia communications over a broadband connection via SmartMessaging.

1.1.3 Managing and Provisioning Devices

APX NEXT delivers greater awareness and faster management of radio fleets with optimized provisioning, networking, and monitoring tools that transform accurate data into smarter action. These features enable dispatchers and network managers to make more informed operational decisions, keep radios in the field, and, above all, protect first responders' focus and safety.

Device Management Services (DMS) packages provide programming, management, and maintenance services to maximize the effectiveness of this APX NEXT solution, while reducing maintenance risk, workload, and total cost of ownership. The DMS packages are separated into tiers designed for a range of customer needs, whether the solution is self-maintained or managed by Motorola Solutions.

Using Motorola Solutions' cloud-based RadioCentral (RC) programming, APX NEXT supports faster provisioning and deployment to get devices in the hands of responders and out into the field. Parameters such as talk groups, interface options, and security keys can be programmed remotely within minutes. Access to RadioCentral is provided through the Device Management Service package.

Figure 1-2 below illustrates the expedited RC provisioning process of APX NEXT.

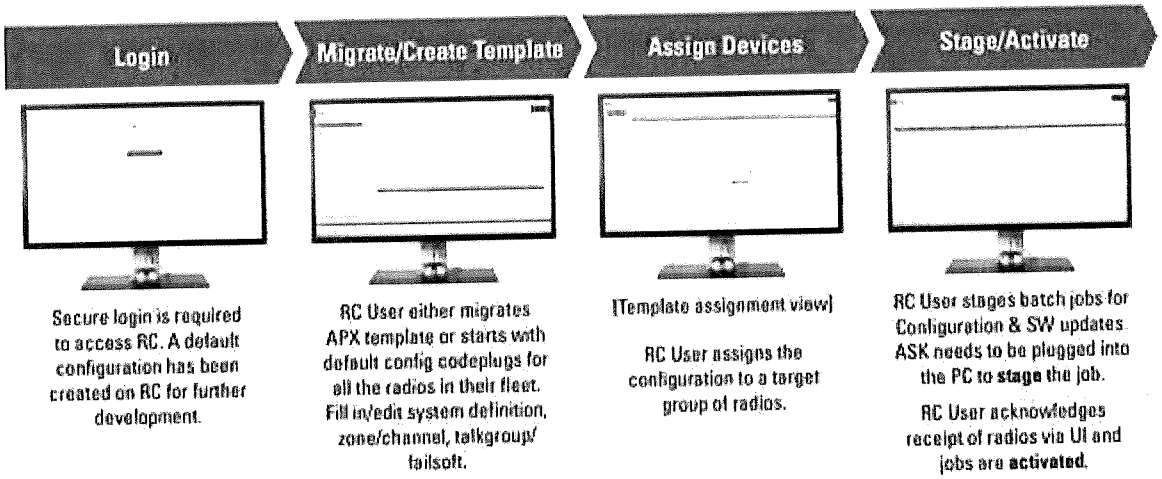


Figure 1-2: APX NEXT Provisioning Process via RadioCentral

The APX NEXT out-of-the-box experience is streamlined with a few simple steps. Users will power on the device and view a boot-up animation with startup. Status bar icons on the front display indicate when a connection is made and an update download is initiated. If the APX NEXT device is being started for the first time, a "peek-in" device management notification will indicate that the default configuration is detected. When the update download is complete, the device reboots and installs the update. When the install is complete, the device goes back to the full home screen and notifies the user that the update is complete. For Encryption and Authentication users, a KVL needs to be connected to the radio for those services. From power on to provisioning completion takes less than a minute.

1.1.4 Evolving with Updates and Upgrades

APX NEXT is a future-ready platform that will evolve alongside users through updates and upgrades, delivering expanded mission-critical capabilities while keeping personnel in the field where they are needed. To this end, APX NEXT eliminates the extended downtime and shop visits often associated with device upgrades; now, software patches can be automatically installed regardless of geographic location over a broadband connection, or, if proposed, immediately pushed to the field over LTE with Motorola Solutions' SmartProgramming service.

This streamlined process eliminates bottlenecks in the upgrade process and delivers important new features into users' hands. Firmware upgrades will also fit more seamlessly into workflows to avoid unnecessary disruptions. Figure 1-3 below illustrates how feature updates are easily deployed to the entire radio fleet.

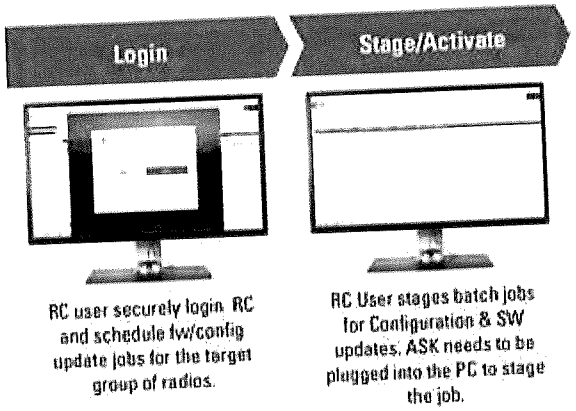


Figure 1-3: Typical Firmware and Configuration Update Process via RadioCentral

If a situation occurs where users do not have the time for an update, those updates can be delayed through a prompt until the next power cycle. This puts personnel directly in control of when updates work best for responders, especially in the chaotic environment of public safety. A snapshot of the APX NEXT device with "Install Update" prompt is shown below.

Figure 1-4: APX NEXT In-Field Update on the Device

1.1.5 Providing Insight

SmartInsight services provide an end-to-end view into your agency's APX NEXT device usage. From 24/7 monitoring and data collection to actions pertaining to fleet management, SmartInsight helps administrators collect, analyze, report, and act on diagnostic information to optimize your APX NEXT fleet's performance. The application is easy-to-view, with accessible interactive dashboards to gain more visibility into the fleet's health status.

SmartInsight delivers the following capabilities to enhance APX NEXT operations:

- Monitor various device parameters like signal strength, device usage, and inventory data.
- Store collected information securely in the cloud, where data exploration, cleansing, and correlation is performed to extract descriptive, predictive, and prescriptive insights for device management.
- Use analytics to take corrective actions and identify potential issues before they occur.

1.1.6 Securing Communications

APX NEXT uses Motorola Solutions' hardened End-to-End security to protect communications and allow only authorized units in the system to listen to transmissions. End-to-End security provides seamless protection from the device and data in transit to the cloud and the LMR system.

This solution ensures each component in the system is designed and validated against ongoing threat assessments to ensure vulnerabilities are detected and remedied, while potential new vulnerabilities will be addressed with seamless security updates. This offers transparent, real-time protection and keeps critical information and infrastructure safe.

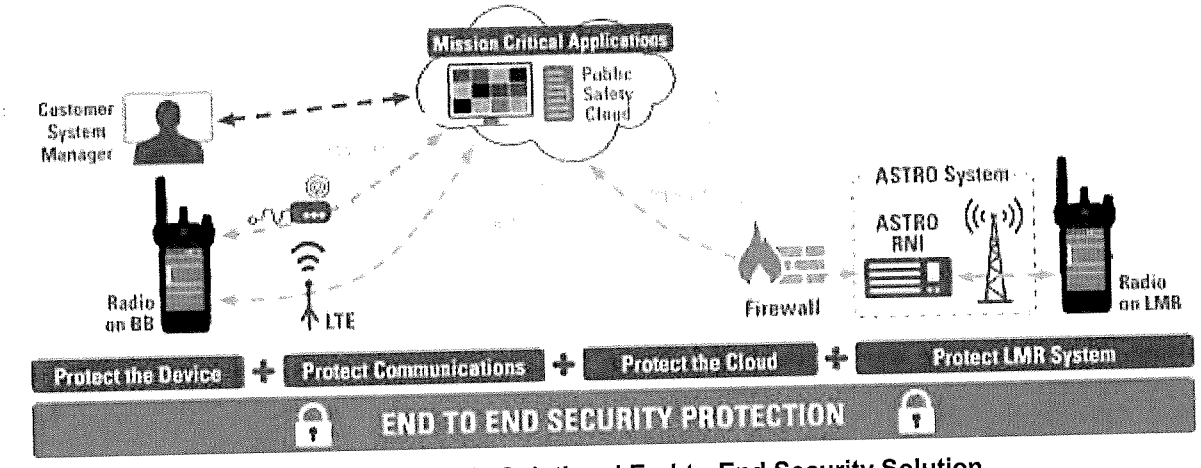


Figure 1-5: Motorola Solutions' End-to-End Security Solution

1.1.7 ViQi Virtual Partner Application Service (Future)

Maintaining situational awareness and first responder safety through natural operation is integral to the APX NEXT radio. This outcome is achieved through ViQi™ Virtual Partner—a cloud-based service that provides vital public safety information via voice. With a single button press and simple audio prompt, your personnel can use natural language to run a license plate or driver's license, and search for vehicles with matching vehicle identification numbers straight from the field without disruption.

Virtual Partner leverages artificial intelligence capabilities to interpret voice queries and quickly deliver query results in an audible format. This empowers field personnel to submit queries with the radio without the risk of losing situational awareness while typing a manual query. The automated nature of the solution also allows officers to obtain critical information faster than relaying the query to dispatchers. The APX NEXT radio will leverage either LMR or supported broadband networks to send queries and return responses.

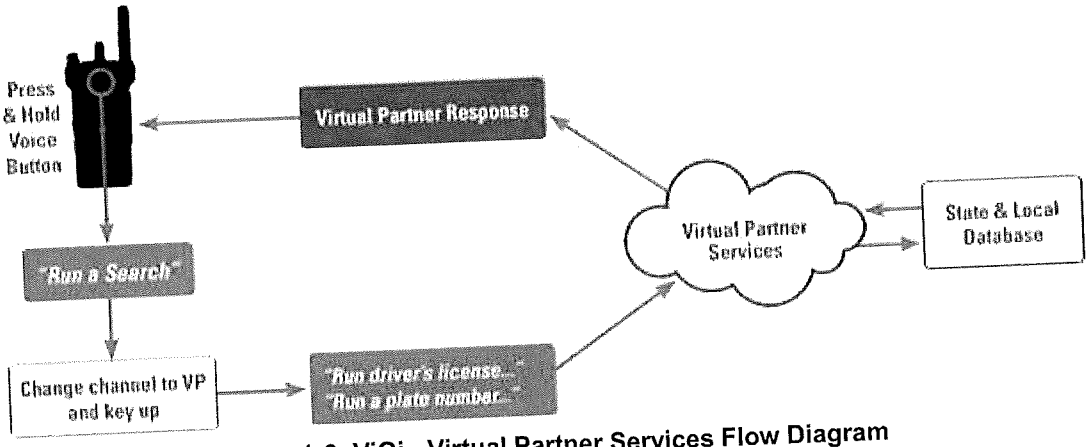


Figure 1-6: ViQi - Virtual Partner Services Flow Diagram

The Virtual Partner Application Service is proposed as a subscription-based model to optimize budget and scale to meet evolving needs.

1.1.8 SmartConnect Application Service

First responders need to know that they are covered and supported with critical intelligence no matter where the mission takes them. Leveraging APX NEXT and supported devices, SmartConnect keeps users connected and maintains critical LMR features through a broadband connection. By seamlessly switching between P25 LMR and LTE cellular networks, SmartConnect extends reliable PTT communications as radio users roam onto supported broadband networks. Authentication, status, talkgroups, and encryption are all preserved automatically, without interruptions or resets to ensure that end users continue to have access to the critical features they need in emergency situations.

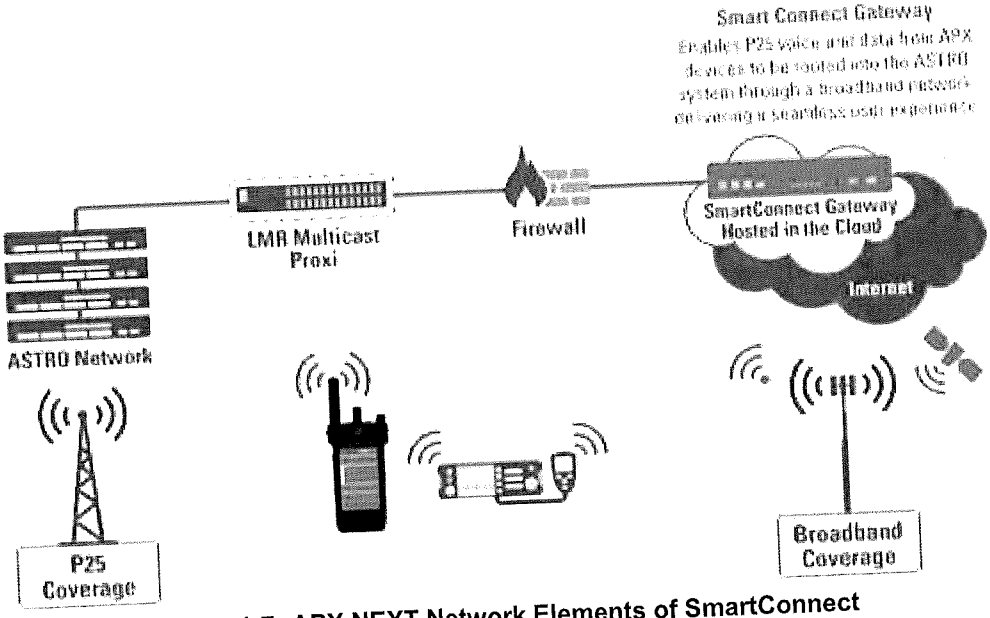


Figure 1-7: APX NEXT Network Elements of SmartConnect

SmartConnect allows users to retain most P25 radio features when out of range of LMR, including the following:

- Agency Groups.
- Dynamic Regrouping.
- Call Alert.
- Emergency Call & Alarm.
- FDMA/TDMA to/from LMR System.
- Group Call Clear/Encrypted.
- Group Regrouping.
- Multigroup.
- PTT ID.
- Priority Monitor Scan.
- Radio Authentication.
- Radio Check.
- Radio Inhibit/Uninhibit.
- Radio Interrupt/Console Takeover.
- Status Update.
- ViQi Virtual Partner via LMR network.

The SmartConnect Application Service is proposed as a subscription-based model to optimize budget and scale to meet evolving needs.

1.1.9 SmartLocate with Command Central Aware

SmartLocate is an application service provided by Motorola Solutions for the APX NEXT device in North America. SmartLocate sends subscriber GPS location data from APX NEXT devices to CommandCentral Aware via a commercial LTE network. Customers are able to monitor the location of APX NEXT devices on the CommandCentral Aware client.

No matter where the mission takes personnel in the field, the APX NEXT SmartLocate feature provides dispatchers with accurate location data over a broadband network. By using the broadband network and CommandCentral Aware capabilities, SmartLocate can send faster, more accurate GPS coordinate updates from the field to Aware clients. Broadband also increases the frequency of location reporting beyond an LMR system, improving location accuracy and allowing for a higher number of users without LMR infrastructure capacity limitations. This location information is used to create an accurate operating picture of any situation.

CommandCentral Aware's consolidated, map-based, operating picture enables enhanced information sharing and informed real time decision-making. Aware's cloud-based platform enables agencies to take advantage of new capabilities as they are developed, without an intrusive upgrade experience. Updates and new features are deployed every few weeks, and users automatically get new capabilities the next time they log in. Cloud deployments also reduce the operational impact of faults and outages. This frees your staff to focus on strategic initiatives, instead of time-consuming tactical efforts, and drives greater value for public safety.

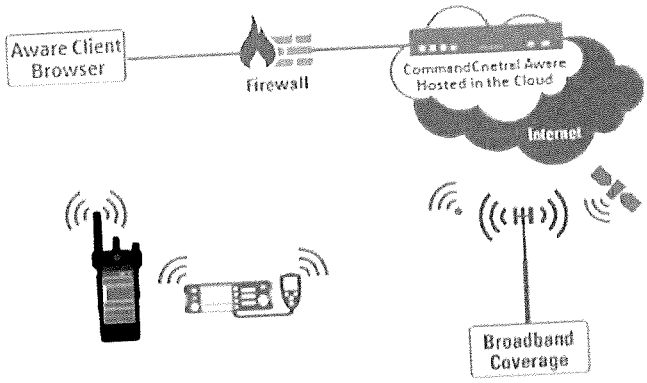


Figure 1-8: SmartLocate Diagram

SmartLocate operation requires the following:

- APX NEXT subscriber device(s).
- SmartLocate subscription.
- Device Management Subscription.
- CommandCentral Aware subscription.
- APX NEXT devices must be powered up and in a supported LTE network coverage area during SmartLocate operation.

1.1.10 SmartMapping Application Service

The SmartMapping application provides precise and accessible location information for field users on APX NEXT's modernized map interface, improving situational awareness and informing response. Users can see their own location and the location/status of other officers at a glance and immediately tap to communicate with these personnel. SmartMapping streamlines engagement by providing access to the application directly from the APX NEXT home screen to best support users wherever the mission takes them.

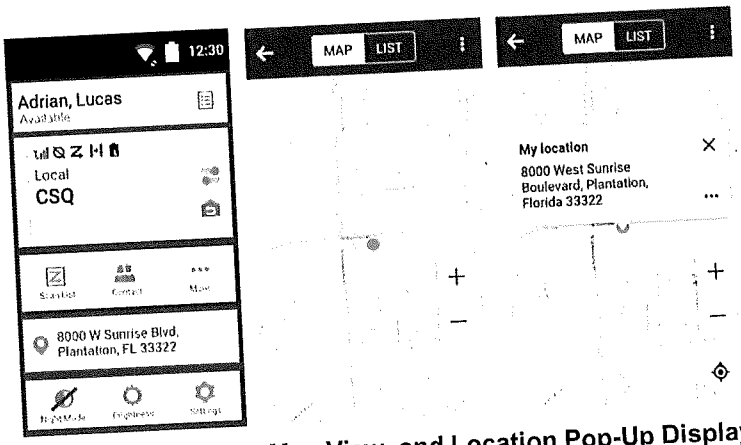


Figure 1-9: SmartMapping Widget, Map View, and Location Pop-Up Display (Left to Right)

SmartMapping also provides the following capabilities for APX NEXT users:

- Search for specific agency users to communicate with by using accessible, on-screen navigation and search tools.
- Select map layers to get a different view of an area, including Street View, Terrain, or Satellite Image.
- Adapt to changing agency needs as new integrations and capabilities are introduced into the SmartMapping application.

1.1.11 SmartProgramming Application Service

Leveraging Device Managed Services (DMS) and RadioCentral provisioning capabilities, the SmartProgramming application allows radios to be updated anywhere within an agency's local LTE network coverage area. APX NEXT devices no longer need to be tied to a computer via USB cable, limited to Wi-Fi network coverage, or gated by Land Mobile Radio (LMR) bandwidth. SmartProgramming allows the APX NEXT device to take advantage of LTE broadband data speeds to pull programming jobs from RadioCentral devices in minutes.

The SmartProgramming Application Service is proposed as a subscription-based model to optimize budget and scale to meet evolving needs.

1.2 PremierOne CAD and Mobile System Description

1.2.1 System Overview

Motorola Solutions is pleased to present the following system for the St. Johns County Sheriff's Office, FL (hereinafter referred to as the "Customer"). Our system is based on our interpretation of the requirements derived from our discussions with you.

Motorola Solutions' offering consists of additional server hardware, server networking hardware, system software, PremierOne application and client software, interfaces and services (as stated in the Statement of Work) for the add-on of the Customer's agency to the existing St. Johns County Fire Rescue's ("System Owner") PremierOne CAD system (Version - 4.5.3.188 (CU3b).

1.2.1.1 Participating Agencies

The designated agencies participating in the system are:

- St. Johns County Fire Rescue (Hosting Agency/System Owner).
- St. Johns County Sherriff's Office (Add-on Agency).

1.2.1.2 Basis for System Sizing

Motorola Solutions uses Call for Service (CFS) and client quantities as the parameters to establish the tiers of infrastructure sizing. Based on the counts provided by the Customer, the system has been sized to add one additional host server to the System Owner's primary and secondary sites and should not exceed the recommended Calls for Service and Clients as listed below:

- Up to 2 Million CAD Calls for Service per year.
- Up to 250 PremierOne CAD concurrent clients.
- Up to 1,000 PremierOne Mobile concurrent clients.
- Five (5) years of PremierOne CAD data retention (2 years of live online data and 3 years of archived data).

The following applications, system components and services are included in this system:

1.2.1.3 Application Software and System Components

This System is comprised of the following component and Subsystem elements:

CAD Subsystem

- System Owner's PremierOne CAD version 4.5.3.188 (CU3b).
  - PremierOne Mobile.
  - PremierOne for Android/iOS.

CommandCentral Components:

- CommandCentral Aware Plus for 10 Named user Licenses for five (5) year subscription.

System Components

- Interfaces.
- Legacy CAD Data to PremierOne CAD Incident Import.

The following Figure 1-10 represents a logical illustration of the system components.

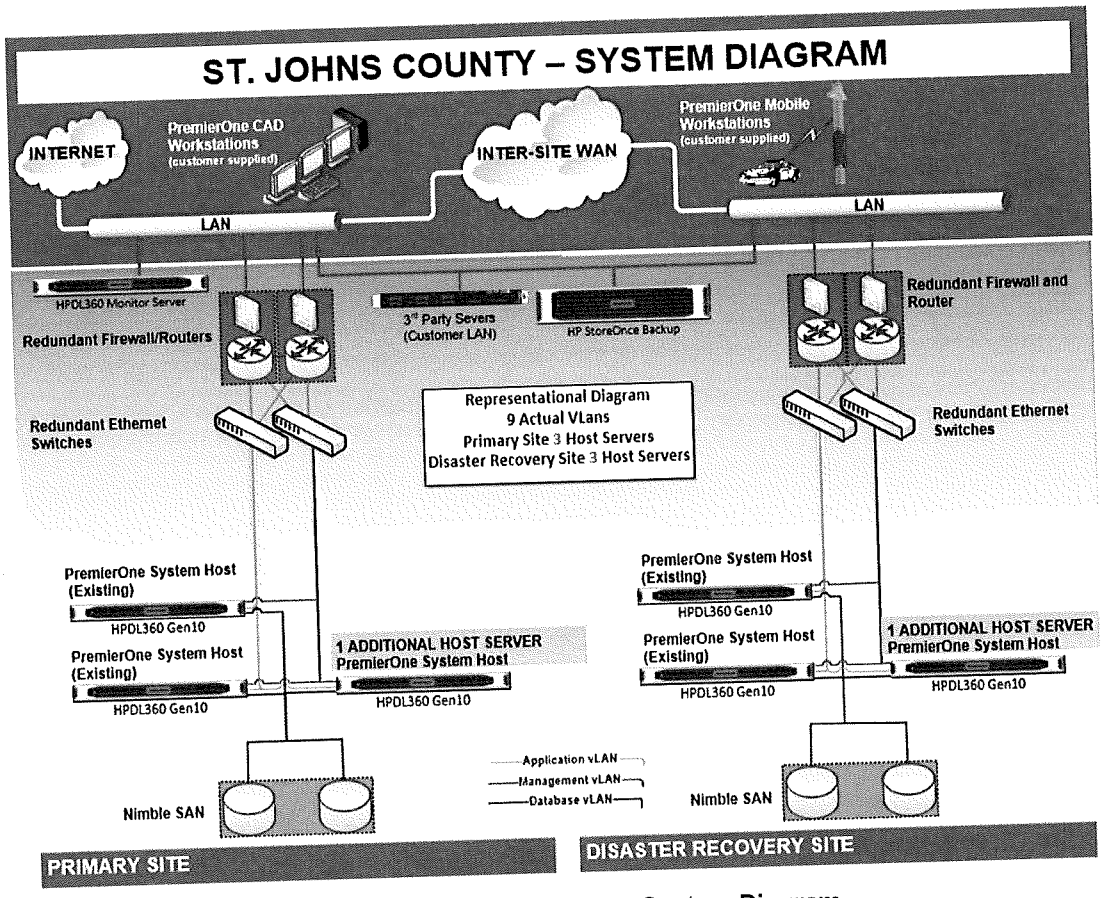


Figure 1-10: Representative System Diagram

1.2.1.4 System Application Client Software Licensing

The following Table 1-1 summarizes the number of PremierOne client application software licenses for all agencies listed in Participating Agencies.

Table 1-1: System Client Licensing

System Client Licenses	Quantity	Type
PremierOne CAD Dispatch with Mapping	18	Per Seat
PremierOne Mobile (Windows)	400	Per Seat
PremierOne Mobile (iOS or Android)	12	Per Seat
CommandCentral Aware	1	Subscription

1.2.1.5 System Interfaces

Table 1-2 below lists the interfaces included in our system. A description of each interface listed in the table below has been provided in Attachment A. Any requests for change to the Interface Description following contract is subject to review and consideration through the change control mechanism of the contract.

Table 1-2: System Interfaces

Interface Name	Interface Description	DR Y/N?
CTS America SmartCop RMS	CFS Fire and ePCR Records Data Feed	Y
FUSUS (RTCC)	CFS Fire and ePCR Records Data Feed	Y
PMAM – CAD Alarm Interface	PMAN – CAD Alarm Interface	Y
PageNet	TAP Notification - CAD Notification Interface	Y
RapidSOS	Integration	Y
State Query	External Query – Suite Interface	

1.2.1.6 CommandCentral Interfaces

CommandCentral Aware Table 1-3 provides a list of the specific interfaces included in this solution, an indication of data direction, and the point of installation.

Data Direction

- **Outbound (O)** – Motorola Solutions system will send data to an external receiver.
- **Inbound (I)** – Motorola Solutions system will receive data from an external source.
- **Bi-directional (B)** – Motorola Solutions system will send data to an external receiver and receive data from an external source.

Installation Point

- Primary System (**P**).
- Client (**C**).

Interface technical information, inclusive of data elements, will be provided prior to contract.

Table 1-3: System Interfaces

Interface Name	Data Direction	Installation Point
ShotSpotter Gunshot	I	P
Genetec ALPR	I	P
Avigilon	I	P
Vigilant		

CommandCentral interfaces are dependent on the functionality made available to Motorola Solutions by Customer's third-party system. Customer is responsible for providing connectivity to the third-party system via the SDK, API, or other Motorola Solutions-approved access. Customer is also responsible

for providing access to third-party systems such as support agreement support as this might be required to investigate, test, and complete the system integration.

Genetec requires a specific license to be purchased (part number GSC-1SDK-Motorola-RTVI) to connect CommandCentral Aware and Genetec systems. Two Cloud Anchor Server licenses are required (one for each workstation viewing Genetec video). Customer will need to purchase these licenses and provide to Motorola Solutions.

1.2.2 Application Descriptions

The following sections provide brief descriptions of PremierOne CAD and Mobile, and CommandCentral Aware applications.

The system uses Commercially Off-the-Shelf (COTS) products therefore software development to the application framework is not provided.

1.2.2.1 PremierOne CAD

Motorola Solutions has designed PremierOne CAD to be the central convergence point for communications from multiple sources and systems, mission-critical information and resource management.

The user interface offers quick access to information via a location-based, Esri standard GIS map. Users perform commands and functions using a mouse, command lines, function keys, shortcuts, or user definable right click menus. The GPS-aided resource management tool displays the location and identity of GPS equipped vehicles or devices enabling a coordinated response while further supporting officer safety.

In PremierOne CAD, ARL, if purchased, could be used in recommendations to track the location of emergency vehicles to determine their present location when requiring units to respond to an incident. By adding ARL recommendations to PremierOne CAD, PremierOne CAD can make recommendations based on the actual location of units rather than recommending units solely based on jurisdictional assignment.

PremierOne supports Direct GPS Connection where location information is sent directly to PremierOne without the use of the PremierOne Mobile client application. Direct GPS Connection requires that device location be reported to PremierOne using Trimble ASCII Interface Protocol (TAIP) with a unique identifier over User Datagram Protocol (UDP).

Users can create incidents from public telephone calls, from information received from an officer or from another public safety agency, or through an alarm interface. Once the user enters basic details of the incident into the system, users may dispatch field personnel to handle the incident. Users may update incidents with additional details such as information about the handling of the incident. Once the user has completed the incident in an appropriate fashion, the user then can close the incident.

Field personnel may use PremierOne CAD to retrieve details about incidents or to make incident updates. Additionally, supervisory personnel may use the PremierOne CAD to monitor the operations of the communications center, the handling of incidents and field unit statistics.

PremierOne CAD functions as a standalone product but also seamlessly integrates with Motorola Solutions' PremierOne Mobile and Records application. PremierOne CAD may also be integrated with other Motorola Solutions and third-party systems.

Users that can benefit from accessing PremierOne CAD and Mobile include but are not limited to Dispatchers, PSAP Supervisors, Patrol Officers and Call Takers.

1.2.2.2 PremierOne CAD Concepts

User Input

Users may operate PremierOne CAD either with or without a mouse. While all commands and actions within the application can be accessed with the mouse, users also may drive PremierOne CAD almost exclusively from the keyboard. A few PremierOne CAD functions, such as selecting units from a map, must be performed with a mouse.

Work and Status Monitors

Users perform the majority of actions within PremierOne CAD's work monitor. Status monitors present summary information about incidents or units. A user may have one or more status monitor windows available at the workstation.

Security and Roles

PremierOne CAD recognizes authorized users and provide access to individually authorized functions at the time of sign-on. To facilitate these responsibilities, access rights and permissions are associated with the various functions available within PremierOne CAD. A role is a set of specified privileges, which provide access to data, commands, forms, devices, and functions. Each user and device is assigned to one or more of the default of Customer created roles.

Units, Incidents and Dispatching

A unit within PremierOne CAD represents the resources, which are dispatched or monitored by the communications center personnel. All units in the system are identified with a unit id, which is typically the radio call sign for the unit. Users can initiate incidents from the command line or from the incident initiation form. The system provides a user with four methods to begin the incident dispatching process. These four methods include:

- Dispatch incident function key.
- Incident dispatch command.
- Dispatch form.
- Drag and drop feature within status monitors and map.

Incident Management

In addition to initiating and dispatching incidents, users can manage existing incidents through the various incident management features of PremierOne CAD:

- Updating existing incident information.
- Associating incidents.
- Disassociating incidents.
- Cloning incidents.
- Closing incidents.
- Reopening incidents.
- Displaying a summary list of incidents.
- Searching for incidents.

Unit Management

Users have the ability to monitor and maintain the current activities for each unit through the various unit management features:

- View and update unit assignment data.
- Make unit status changes.
- Manipulate a unit's call stack.
- Transfer units.
- View a unit's history.
- Move units from one station or area to another station or area.
- View the current activities for a unit.
- Assign crews.
- Clear units from an incident.
- Manipulate units that are assigned to incidents.
- Move resources to cover depleted stations or areas.
- PremierOne CAD can alter a unit's capabilities based on the personnel assigned to that unit.

Federal, State and Local Queries

PremierOne allows users to submit requests for information to external databases. These external queries can involve local agencies, as well as state and federal agencies. External databases all have their own data formats and respond to submitted queries with one or more responses.

Maps

PremierOne mapping utilizes products from Environmental Systems Research Institute (Esri) for geo-processing. The display of maps is an integrated component within PremierOne. The map may be configured to automatically display when the user signs on to the workstation. A number of commands and functions allow the user to manipulate the map and make updates in response to user actions. The map may be configured to display an icon at this location to assist the call taker in determining the location at which an emergency response is required. The system also attempts to find the nearest address/common place to the caller coordinates.

Mail & Messaging Services

The mail and messaging functionalities of PremierOne CAD allow users to exchange and distribute electronic mail and messages within the dispatch center and to units equipped with MDTs.

1.2.2.3 PremierOne Mobile with Mobile Mapping

PremierOne Mobile provides public safety personnel the ability to assess and prepare for a situation while enroute to the scene. Users access information via screen configurations that provides navigation throughout the PremierOne Mobile application.

Table 1-4: PremierOne Mobile Mapping Capabilities

PremierOne Mobile - Available Clients:	Window	Android	iOS
Operating System	Windows 8.1+	Android 8.0+	iOS 10 - 13
Cloud Enabled	•	•	•

MOTOROLA SOLUTIONS

PremierOne Mobile - Available Clients:	Window	Android	iOS
Silent Dispatch	•	•	•
Incident & Unit Management	•	•	•
Real-Time Status Monitors	7	5	5
Field Initiation for Traffic Stops & Other Incidents	•	•	•
Database Querying	•	•	•
BOLOs	•	•	Query Only
Responder and Unit Location Tracking	•	•	•
Premise & Hazard Details with Images	•	•	•
Geofencing with Entry & Exit Alerts	•	•	•
4G & LTE Network Capability	•	•	•
CJIS Security Support with FIPS 140-2 Encryption & Auditing	•	•	•
Barcode Scan	•	•	•
Voice Entry for Comments	•	•	•
Actionable URL in Comments	•	•	•
Messaging	•	•	•
Advanced Mapping, BOLOs, Premise & Hazards	•	•	•
Advanced Configurations	•	•	•

The integrated map provides the user the ability to display call location, drive directions, premise hazards and the location of other units. PremierOne Mobile leverages the same common map platform used in PremierOne CAD, which is managed and provisioned from a centralized location and deployed to all systems remotely.

PremierOne Mobile obtains location information from a collocated GPS receiver. The PremierOne Mobile Windows Client supports either the Trimble ASCII Interface Protocol (TAIP) or National Marine Electronics Association (NMEA) standard. The PremierOne Mobile client application can send its location to PremierOne CAD via a cellular data modem. The vehicle location information is used by PremierOne CAD to support location dependent features including: Mapping, Track-It, Follow-It, and Recommendations.

1.2.2.4 CommandCentral Aware

Motorola Solutions' CommandCentral Aware solution combines disparate systems and data into an accessible interface. This single interface offers command centers a complete operating picture to support field personnel in real time. CommandCentral Aware unifies data from mapping, correlated event monitoring, analytics, and communications. This interface streamlines public safety workflows and viewpoints, enabling users to access and act on critical information.

The agency can increase the value of current investments by connecting CommandCentral Aware to other software platforms. These integrations include Computer Aided Dispatch (CAD) systems, Call Handling, Land Mobile Radio (LMR), or Video Management Systems (VMS). Users can communicate with confidence, knowing their information is hosted in the highly secure Microsoft Azure cloud.

Users that can benefit from accessing CommandCentral Aware include but are not limited to Dispatchers, PSAP Supervisors, Real Time Crime Analysts as well as Investigators.

CommandCentral Aware provides location and alert capabilities to improve public safety response, described in the sections below.

Mapping

CommandCentral Aware features a unified interface to display locations and alerts. Users can view all location-based data on the map display to enhance decision making. CommandCentral Aware Mapping features also include the following:

- Event Monitors – View device status and location, CAD incidents, open-source data alerts, and sensors on a map. This map can consist of Esri online, Esri server, or static map layers. This map can be modified with other data layers.
- Data Layer Panel – Show or hide data layers to refine the map view.
- Event Information Display – View details associated with each icon on the map.
- Historical Map – View a 90-day lookback of radio locations, CAD incidents, service requests, or emergencies. An export tool extracts the recreated timeline to KML format to view in Google Earth or ESRI ArcGIS Pro. If the camera (and its relative VMS) has the ability to play recorded footage, the recorded footage of the selected time frame can be played in Aware's Video Module directly from the Historical Map.
- Breadcrumbing – Track individual APX user radios. Tracking begins at the time the action is toggled on. Devices can provide up to the last 30 minutes of live movement.

Geographic Information System (GIS) Data Set

CommandCentral Aware integrates with hosted GIS data sets from Esri ArcGIS Server or ArcGIS online. The geospatial information contained within these data sets are core to the intelligent map display. This enhances workflow details driven by geography and the metadata contained within these data sets.

Esri's powerful geospatial engine within CommandCentral Aware is used to automatically invoke spatial queries, including nearby items and geographic boundaries. This geospatial processing enables intelligence-driven analysis in order to focus on the concentrated area of concern and orientate those responding.

Data sets help users to:

- Refine displayed data based on the geographic area defined per user. Data includes area, beat, sector, precinct, zone, or quadrant.
- Find nearby entities by predefined distance. Parameters include closest camera while in route, closest cameras to an event - CAD, gunshot detection, alert.
- Determine road blockages caused by traffic jams, flooded roadways, or other obstacles.

Weather Integration

CommandCentral Aware includes integration with Weather services. This integration provides customized weather-driven services. Services include site-specific forecasts, severe-weather warnings, historical data, and custom analytics. Weather services also provides the following data:

- Location key for the desired location.
- Forecast information for a specific location.
- Current Conditions data for a specific location.
- Daily index values for a specific location. Index availability varies by location.
- Radar and satellite images.

Rules Engine

The Command Central Aware rules engine allows users to create rule-sets to trigger actions based on event types. For example, users can highlight rows in the Event Monitor and customize sound alerts for critical incidents. These visual and audio triggers reduce the number of steps needed to support an incident.

Floor Plan Integration

CommandCentral Aware allows the ability to view building floor plans in the Map Module enabling users to see detailed building levels, switch between floors, and look for specific rooms or cameras on each floor. Clicking the map opens a floor plan widget at the bottom of the window where users can change the view between floors in a building. The Indoor Cameras Tool allows users to place cameras on the building floor it is located on, providing more granularity in locations where cameras are installed on multiple floors. Floor plan files must be in AutoCAD DXF format to be supported by CommandCentral Aware. There are twenty five (25) floors included with CommandCentral Aware. Each additional floor will incur an additional cost.

1.2.3 CommandCentral Aware Integrations

CommandCentral Aware can integrate with various tools and solutions, described in the sections below.

APX Radios Location on Push-to-Talk or Location-on-Receive (TDMA)

CommandCentral Aware provides the location of users from GPS-enabled LMR (ASTRO 25 radios) and broadband devices (LTE/Wi-Fi-enabled smartphones, tablets, and modems). When a user presses the PTT, Emergency Button, Man-Down, or On-Demand buttons (or Stale Location or Not Reporting indications activate), CommandCentral Aware pinpoints the location. With each PTT press, CommandCentral Aware updates, delivers, and ingests device location data. This keeps command center personnel informed during critical incidents and allows dispatch to make more informed decisions. A user can be affiliated with multiple devices (both broadband and LMR). Multiple users and their devices can be affiliated with a unit.

Location on PTT increases location accuracy even when the radio system is congested with voice traffic. Location on PTT can be sent over the voice channel, in addition to cadence, distance, or manual updates already being sent over the data channel. Once location data is received by the Packet Data Gateway (PDG) at the ASTRO 25 master site, it is forwarded to the application via CloudConnect OR Intelligent Middleware (IMW). The CommandCentral Aware application then allows dispatchers to view the location of any APX radio in near real-time to accelerate response.

An APX radio in a group or emergency call sends its current GPS location over the voice channel during each transmission. Location data is embedded directly in the voice stream and sent continuously without impacting voice quality. Radios with Location on PTT can be configured to send their location after each PTT during group calls and during emergency calls.

Vigilant License Plate Recognition (LPR) Integration

CommandCentral Aware integrates with the Vigilant LEARN solution, which enables search and analysis of Vigilant LPR detections within the Aware Map Module. When a license plate detection displays in real-time on the Aware map, the license plate can be searched directly from the CommandCentral Aware interface enabling you to see previous historical detections (time, date, location) and additional details associated with the license plate. With an existing Vigilant LEARN subscription, users can analyze and research the LPR hit for more information and research the plate from the LEARN database.

Avigilon Control Center (ACC) & Video Analytics

The Avigilon Control Center (ACC) uses self-learning analytics to provide effective monitoring and proactive, real-time response for security personnel. ACC combines an intuitive interface with advanced artificial intelligence (AI) search technology for a full-featured integration with CommandCentral Aware. Avigilon offers analytics embedded in Avigilon cameras up to 5K (16 MP) resolution.

This ACC integration includes the following:

- **Advanced Pattern-Based Analytics** – Avigilon advanced video pattern detection technology accurately recognizes the movements of people and vehicles while ignoring motion not relevant to a scene. The system's self-learning ability reduces false positives and helps make alerts more meaningful.
- **Teach-by-Example Technology** – Avigilon teach-by-example object classifier technology allows users to provide feedback about the accuracy of alarm events generated by Avigilon devices. Rather than decreasing analytics sensitivity to reduce false alarms, the feedback trains devices to improve the accuracy of the analytics used to determine which alarms are real and which are false. This impacts a low false-positive alarm rate. Over time, the system learns the scene and is able to prioritize important events based on user feedback. This increases sensitivity to conditions that are of concern while reducing false alarms to keep the focus on what matters.
- **Avigilon Video Analytics Alerts Integration** – Avigilon ACC allow video analytics to send alerts to CommandCentral Aware. These analytics include object detection, motion detection, path crossed, and directional pattern changes.

The ACC rules engine enables users to selectively apply analytics-based events as alarms and rule triggers. These rules offer immediate notifications for suspicious activities to help CommandCentral Aware users monitor and respond more efficiently.

Avigilon to CommandCentral Aware integrates the results of the rules engine combined with video from the Avigilon VMS. The targeted video feed is displayed in response to user interaction and pre-defined scenarios based on a customizable rule set. Users can configure specific categories of events, such as CAD incidents, LPR alarms, or other alert reporting systems integrated into CommandCentral Aware, in relation to analytics to trigger video feeds. These real-time events and forensic capabilities detect and notify scene changes, missing objects, and rules violations. In addition to the live video and analytics, the connector supplies operator's video display tools that control pan, tilt, zoom (PTZ) cameras, and playback of recorded video.

The following is a complete list of Avigilon Control Center (ACC) video analytics features for object detection and classification for live or forensic events that enhance the common operating picture and situational awareness capabilities of CommandCentral Aware.

Table 1-5: Avigilon Control Center Video Analytics

Avigilon Analytics Rules for ACC	Analytics Rules Description (Objects are Classified as Person or Vehicle)
Objects in Area	The event is triggered when the selected object type moves into a specified region of interest.
Object Loitering	The event is triggered when the selected object type stays within a specified region of interest for an extended amount of time which is configured.
Objects Crossing Beam	The event is triggered when an Object or a specified number of Objects have crossed the directional beam that has been configured over the camera's field of view. The beam can be unidirectional or bidirectional.
Object Appears of Enters Area	The event is triggered by each object that enters the specified region of interest.
Object Not Present in Area	The event is triggered when no objects are present in the specified region of interest.
Objects Enter Area	The event is triggered when the specified number of objects have entered the specified region of interest.
Objects Leave Area	The event is triggered when the specified number of objects has left a specified region of interest region of interest.
Object Stops In Area	The event is triggered when an object in a specified region of interest stops moving for the specified threshold time.
Direction violated	The event is triggered when an object moves in the prohibited direction of travel.
Camera tampering	The event is triggered due to sudden scene changes.
License Plate Recognition Analytics	New license plate recognition analytics engine with highly-accurate license plate capture, identification, and search for fast event response. Use watch lists to create alerts and actions when a license plate match is detected.

1.2.4 Service Solutions

The following sections provide brief descriptions of service solutions delivered as part of the PremierOne offering.

1.2.4.1 Legacy Data Access or Data Migration

It is a very common desire for agencies when migrating to new systems to preserve and utilize the data contained in the legacy systems There are two types of data will be accessed or migrated and each type will be treated differently.

The first type of data is configuration data. This consists of code tables and other lists from the existing CAD system. This would include data such as unit identifiers, incident types, personnel information. These data types may either be imported into PremierOne system or manually entered during the provisioning process. For those tables to which data can be imported, the common process is for the Motorola Solutions team to provide spreadsheets to the Customer personnel. Customer personnel will

export the data from the existing system, transform it as needed to match the provided spreadsheets and import it into the PremierOne system using the built-in import functionality. Data that will be manually entered during the provisioning process is gathered by the Customer and recorded on provisioning worksheets.

The second type of data is historical data. This consists of the transactional data that is a record of events / incidences that were recorded in the existing CAD system. This would include data such as incident information, unit history information, messaging information.

Below are the strategies being offered to accommodate access to this historical data.

Legacy Data Access - Data Warehouse

This data will be extracted from the existing CAD system by the Customer and be incorporated in to a SQL data warehouse supplied by Customer that can be accessed via standard SQL tools. The Customer can then develop queries and format the returns in PremierOne.

The legacy databases must be stored in Customer supplied relational databases (hardware and software) external to the PremierOne system and Motorola Solutions must be able to link directly to the legacy databases from MS SQL Server.

Legacy CAD Data to PremierOne CAD Incident Import (60-days)

Motorola Solutions will convert and extract specific data that exists in the Customer legacy CAD system and then import to the CAD system. While Motorola Solutions is responsible for converting the specified data, it is critical that the Customer assign a knowledgeable resource to this activity that will remain engaged throughout the migration process.

The legacy databases must be in a Customer supplied Microsoft SQL Server databases (hardware and software) external to the system and Motorola Solutions must be able to link directly to the legacy databases from Microsoft SQL Server.

The legacy databases must be stored in Customer supplied Microsoft SQL Server databases external to the system and Motorola Solutions must be able to link directly to the legacy databases from Microsoft SQL Server.

Motorola Solutions will migrate 60-days of legacy data.

Motorola Solutions does not provide any data clean up or manipulation of the provided data and conducts a single, one time, bulk load of legacy data. The Customer should conduct a comprehensive analysis of the data in the legacy systems to identify duplicate data/records, lost data, orphaned records, or records that have not been linked properly and resolve those issues prior to extracting the data to be converted.

The following are types of data being imported:

- Location.
- Call Type.
- Disposition.
- Comments.
- Units Involved.
- Agencies Involved.

- People Involved.
- Vehicles Involved.

Imported incidents will have the following characteristics:

- Imported incidents will be created and then "closed".
- Imported incidents cannot be re-opened or cloned.

Imported incidents older than aging threshold set in PremierOne will be moved to PremierOne CAD's RDW and then purged from production.

1.2.5 Third Party Integrations

1.2.5.1 RapidSOS Integration

PremierOne Integrates RapidSOS features into PremierOne CAD. This integration allows for immediate call location, responses to moving callers and access to additional more detailed information about the caller.

Locate Callers Immediately

Improve response time and call location accuracy by accessing a reliable caller device based hybrid (DBH) location in as little as three seconds of taking a call from within PremierOne CAD.

Respond to Moving Callers

See a faster and more reliable location even if the caller is moving with integration between PremierOne CAD and RapidSOS. This robust technology provides accurate location to three seconds every time the call taker re-bids the caller location.

More Detailed Information

Arm you call takers and responders with faster more detailed caller information before questioning has even started. With this streamlined technology, caller data is provided by multiple resources, aggregated by RapidSOS, which PremierOne CAD then queries and delivers to the call taker.

1.2.6 System Platform and Components to be Added to System Owners Existing System

This section discusses the hardware, operating system, and system software of the system to be added on premise at the System Owner's Data Center Facility. Quantities of hardware are provided in the Equipment List.

The addition of the Customer's agency to the System Owner's existing PremierOne CAD system will require one (1) additional Host server for each site (Primary and DR).

Note: It is the responsibility of the Customer to provide any specialized hardware and installation to ensure compliance with any Local, State or Federal natural disaster safety regulations.

1.2.6.1 PremierOne System Servers

The system hardware is comprised of Hewlett Packard Enterprise (HPe) servers as physical hosts.

Host servers are HPe DL360c Gen10 servers configured with the following components:

- Dual 12-Core Intel® Xeon® Gold 6146 processor, running at 3.2 GHz, with a 25 MB L3 Cache.
- Each server also contains direct attached storage in the form of two 8 GB micro SD hard drives with Smart Array controllers in a RAID configuration.
- Four (4) - 10 Gigabit network ports.
- Each server is configured with 384 GB RAM.

1.2.6.2 PremierOne System On-Premise Storage and Backup

The system's Backup and Recovery subsystem includes online storage and a means to back up the system offline through Nimble Storage and HPe StoreOnce disk arrays. Our system design provides storage area arrays that are utilized by the host servers for storage and for online backups with near real-time data recovery.

Nimble Storage Expansion

The Nimble Storage on the System Owner's existing system will require an expansion from 11TB to 42TB.

The Nimble Storage HF Series SAN provides 42 TB of RAW storage. This storage consists of twenty-one (21) 2 TB HDD along with three 1920 GB SSD (5.8 TB flash) iSCSI connected drives.

1.2.6.3 PremierOne Network and Management Components

Switch Replacement (Arista Networks Data Center Switches)

The EOS modular operating system supports intelligent Layer 2 switching, Layer 3 IPv4/IPv6 routing, as well as role-based policy capabilities.

The Arista 7050TX-48 is a data-center grade 32-port 10Gb Ethernet switch with 40Gb uplink. The switch comes with power supply and fan redundancy. The switches and their design were chosen to provide system availability and redundancy.

The Arista 7010TX-48 is a 48 port 10/100/1000 MB Ethernet switch. This switch is included to provide connectivity for management activities in a subnet outside of those for core functionality

1.2.7 System Architecture

The system is designed on the principles of Service Oriented Architecture (SOA) allowing separation of servers and services to modular components. The system can be expanded through the allocation of additional physical or logical resources as needs grow. In addition, site-to-site replication creating a multi-site architecture.

The system is deployed with a single production environment incorporating the high availability components and interfaces presented in this system. The production environment incorporates the high availability components and reconfigured interfaces presented in this system.

The system is architected around a virtualized server configuration and supports VMware vSphere 6.5 (or later) for the hypervisor. Server virtualization provides application isolation providing the ability to isolate specific services for ease of diagnostics and hardware resource management.

1.2.7.1 PremierOne High Availability Architecture

PremierOne is also architected to have no single point of failure. Its software design is redundant, as database replication occurs across multiple servers. The system is built on industry standard components from Microsoft .NET architecture using Microsoft Windows and Microsoft SQL Server and other vendors.

The combined software, hardware and IT network architecture is designed to provide an integrated high-availability system at each site. Redundant software and hardware components are the basis of the high-availability system design. Redundant network paths are used throughout the system configuration.

Multiple application servers support the application service layer and utilize load balancing to manage the load across the servers. RAID storage configurations provide redundancy and recovery within the storage components, and dual power supplies and circuits are used to ensure power redundancy.

Application, database and Application Delivery Controllers (ADC) failovers operate independent of one another within PremierOne. This means the failure of one component does not require the other components to failover.

PremierOne's active monitoring identifies problems and failures before they occur. For example, low disk space or high processor utilization will trigger an alert to be sent, to notify the recipient of a possible problems or future failure before it affects the system. In the event of a service or component failure, PremierOne will stop using the failed service or component instance and automatically shift over to the secondary service or component instance without impacting operations.

The following depicts the fault tolerant components of the system.

Table 1-6: Fault Tolerant Software Components

Component
• Multiple F5 ADCs to provide load balanced network traffic to the application services. • PremierOne monitors active services and restarts them as necessary. • In the case of a server failure, the node is disabled transferring the load to the remaining nodes in the cluster.
Replicated databases on different servers. Servers are replicated in a cluster set. • SQL Server AlwaysOn provides redundancy and automatic failover. • In case of a database server failure, there is no user intervention required. Secondary database becomes the active database without administrator intervention and continues processing transactions within the data center.
Fault tolerant networking components throughout the entire stack, the use of Link Aggregation Groups between network nodes and multipath configuration such that no single cable, port or device can interrupt system operation.
PremierOne System Manager monitoring: • CAD application. • Records application. • Application Delivery Controller cluster. • Database status. • Disk space. • Windows Performance Counters.

The backup service (backup library and backup software), the Report Data Warehouse (ad hoc reporting services), and the Test/Training environments are not designed to meet the same high availability requirements as the production application and database servers. Reporting services and test/training environment(s) are not considered critical and therefore are not redundant in the configuration.

CommandCentral Jail is not included in the monitored status, but will have backup replication on the Disaster Recovery site.

High availability is independent of a geographically redundant secondary disaster recovery system.

The system design also provides a single limited use environment that can be used as a test or training environment. The single limited environment does not include the interfaces configured for use in the production environment.

Environment Summary

- One (1) Production Environment on both Primary and Disaster Recovery sites.
- One (1) Limited Use for Test or Training on both Primary and Disaster Recovery sites.
- One (1) Additional Reporting Data Warehouse (RDW) for PremierOne CAD.

1.2.7.2 Microsoft Active Directory Service (On-Premise)

The system provides directory services to support the secure management and operations of system through an isolated Microsoft Active Directory (AD) environment. The servers provided with the system contain computer accounts in this AD tree. Service and Administrator user accounts and groups will be setup in the isolated Active Directory with the appropriate group memberships set.

In order to facilitate ease of user account management, the system can use the Customer's AD environment for authentication. Once the user account is built in the system provisioning, it can then use LDAP to query the Customer's environment for the account authentication. By using this configuration, the Customer can enforce password policy, retention, and complexity requirements across the enterprise with a user having a singular identity.

Motorola Solutions will provide a one-way forest trust from the system local domain to the Customer's Active Directory environment. The trust provides users with Domain Administrator privileges on the Customer's AD instance to access and administer the system environment while preserving authentication and logon information. Motorola Solutions recommends that this trust be non-transitive in nature. Motorola Solutions does not recommend a two-way trust, as none of the system service accounts need authentication or resources on the Customer's network.

The system's Active Directory schema is for servers and services. Active Directory user authentication (if desired) will be against the Customer's Active Directory schema.

Name Resolution

The system provides host name resolution through an Active Directory Integrated Domain Name Service (DNS). In order for computers residing outside of the system's network to communicate with the system, the Customer must configure their DNS servers to forward their computer's name resolution requests to system's DNS servers. This will allow devices on the Customer network to find systems within the system's environment.

For tighter integration, the Customer, working with Motorola Solutions, must configure their DNS servers to allow name resolution requests from within their networks to be processed.

1.2.7.3 Common Services

Common Services provides system administrators the flexibility to manage internal services throughout the platform from a single point. The system's Common Services include GIS, System Security, Reporting, and the system tools for provisioning.

Geographic Information System (GIS)

Geo-spatial data is uploaded to the system through tools implemented within Esri ArcGIS. Address validation data is maintained in redundant Microsoft SQL Server geodatabases that store locations and boundaries both spatially and in optimized search tables. Esri ArcGIS Servers provide routing and ETA calculations using the Network Analyst extension. Client maps are displayed using Esri ArcGIS Engine.

- The system uses GIS for display, location validation, and unit recommendation. The system's tools made available for ArcTool box, provides the ability to load local data manually or through an automated model.
- The system's Response Boundary Data Import Tool imports and aggregates boundaries in multiple layers into a single spatial table within the geodatabase for support of multi-agency / multi-jurisdictional scenarios. GIS data is a required key component of a system deployment. GIS provides the mechanism for location validation and recommendation for response.
- A system conformant and geographically accurate GIS data is required for the proper operation of the system. It is the Customer's responsibility to provide a complete and accurate GIS data that conforms to the PremierOne GIS Data Requirements. Each agency being added to the system must have their geographic coverage included in the geodatabase imported into the system.
- The use of remote and/or Esri Online services is not supported. Motorola Solutions is not responsible for map availability or any degradation of client performance caused by the use of third party hosted internet map services as these services are outside the domain of the system infrastructure and are not managed by Motorola Solutions. The system is a mission critical application that must control the import/access of the GIS data.

System Security

The system is deployed within its own Microsoft Active Directory (AD) domain in its own local area network. Active Directory Domain Controllers authenticate and authorize users to perform actions within the domain making sure authorized users have appropriate access to data and services. The system user provisioning environment can be setup to query your AD environment (using LDAP) allowing for a single point of user and password management across all applications.

The system network contains multiple virtual local area networks that are used to secure and segment traffic for purposes of user access as well as data storage and replication. System architecture resides behind dual redundant firewalls to protect the system network from unauthorized intrusion and security threats. These firewalls are provisioned in a high availability configuration so if either of the two fails, traffic and security will remain intact across the other.

Query Services

PremierOne allows users to submit requests for information to external databases. These external queries can involve local agencies, as well as state and federal agencies. External databases all have

their own data formats and respond to submitted queries with one or more responses. These queries can be made available to all PremierOne applications.

PremierOne also allows the customer to build queries against a local database during query provisioning. If a query is configured for submission to both a state interface and a local database, state queries will continue to be passed to the existing CommSys interface, while the local database query will run through the custom XML (in a Motorola Solutions template) provided by the customer.

Microsoft Reporting Services

PremierOne uses Microsoft SQL Server 2017 Reporting Services (SSRS) for reporting purposes. SQL Server 2017 Reporting Services is a server-based reporting platform that is used to create and manage tabular, matrix, graphical, dashboards, and free form reports that contain data from relational and multidimensional data sources. The reports can be viewed and managed via a browser.

1.2.8 Customer Provided Workstation Specifications

Workstation specifications are representative of workstations used in the testing of the latest release of system software and do not take into account any other applications.

Future releases of the system may dictate changes to the workstation specifications. Each agency should consider their own technology replacement lifecycles and policies for specific purchase decisions.

1.2.8.1 PremierOne CAD Minimum Recommended Specifications

Table 1-7: PremierOne CAD Workstation Minimum Recommended Specifications

Component	Description
Processor	3.5 GHz Processor Intel® Xeon® (E5-1620 v4 or similar).
RAM Memory	16 GB or more of memory. (Although not needed for the PremierOne client, inclusion of additional memory (example, 16GB) in new workstation purchases is common for future capacity.)
Available Disk Space	20 GB available disk space; solid state drive (SSD) required for optimal performance.
Operating System	Windows 10 Professional higher (64-bit recommended).
Network Interface Card	100 Mb or faster (Gigabit recommended) Ethernet network adapter. - Note that network latency will impact system performance.
Display	Three (3) – 1024 x 768+ pixel, 16+ bit color displays.
Keyboard	QWERTY Keyboard with 12 function keys.
Graphics Adaptor	Graphics adapter with at least 512 MB RAM per monitor, 24-bit capable graphics accelerator, OpenGL v2.0 runtime or higher. Latest available drivers. Shader Model 3.0 or higher is recommended.
Network Bandwidth	2 Mbps network bandwidth (to server) with 20 ms or less round-trip latency
Additional Software Applications	Adobe PDF reader (for help files). SQL Server Express 2017 CU level supporting TLS 1.2 is required. ArcGIS Engine 10.6.1 (included with PremierOne CAD client software). Microsoft .NET Framework v4.8.

1.2.8.2 PremierOne Mobile Workstation Minimum Recommended Specifications

Table 1-8: PremierOne Mobile Workstation Minimum Recommended Specifications

Component	Description
Device	Modern "business grade" or "ruggedized" Windows notebook.
Processor	Multi-core processor (i5 or higher, 4-thread, 2.6 GHz +), Intel® Core™ or newer Intel® Series.
RAM Memory	16 GB or more RAM (4 GB must be available for PremierOne Mobile).
Available Disk Space	20 GB or more available disk space; SSD (Solid State Drive) recommended.
Operating System	Windows 10 Professional or higher (64-bit recommended).
Network Interface Card	Wireless communications minimum 3G network, 4G/5G network recommended.
Display	1024 x 768+ pixel resolution display minimum, 16+ bit color display, 11.6" or larger display. Usage on devices with alternative resolutions and smaller screens should be tested and screen settings optimized. Example: On a 10.1" WUXGA screen, use a resolution of 1280 x 800 and a font size of 125%.
Keyboard	Standard QWERTY keyboard and Touchpad / Point Stick (or equivalent mouse device). Touchscreen Optional.
Graphics Adaptor	Discrete graphics card with at least 256 MB of RAMs.
Additional Software Applications	Adobe PDF reader (for help files). SQL Server Express 2017 CU level supporting TLS 1.2 is required. Microsoft .NET Framework v4.8.
Additional Software Applications for PremierOne Mobile Mapping	ArcGIS Engine 10.6.1 for Classic Map. Microsoft Visual C++ Redistributable for Visual Studio 2017.

1.2.8.3 CommandCentral Aware Hardware Recommended Specifications

Table 1-9: Cloud Anchor Server Installation Requirements

Description
One (1) rack unit per Cloud Anchor server.
Two (2) circuits to distribute power to the server rack (dual power supplies).
UPS (Uninterruptible Power Supply) at the site where the Cloud Anchor server and CommandCentral Aware workstations will be installed.
Access to the Internet.

Table 1-10: CommandCentral Aware Recommended Workstation Specifications

Component	Description
Processor	Intel Xeon 6136 @3.0 GHz (12 cores).
RAM Memory	32 GB or more memory.

Component	Description
Drive	One NVMe 512G SSD.
Operating System	Windows 10 Professional.
Network Interface Card	1 Gb port.
Graphics Card	NVIDIA Quadro P2000.
Display	Narrow Bezel IPS Display, 2560x1440 resolution.
Monitor	27-inch monitor or larger.

1.2.8.4 Technical Considerations and Design Requirements

The hardware and licensing identified in this system may be subject to change. As technology continues to advance, Motorola Solutions may take advantage of new and different offerings for the betterment of the Customer. Any changes will be reviewed with the Customer.

Customer Responsibilities:

- Supply Windows Server Client Access Licenses (CALs) for all system client devices accessing CAD and CAD Mobile.
- Supply Mobile Device Management (MDM) software for Mobile devices, as desired by the Customer.
- Provide advanced authentication for Mobile/Handheld device connectivity if required.
- Provide a network diagram depicting all the devices, device types, and interfaces that the system will connect to and through, including, but not limited to all blocked ports, hubs, switches, routers, firewalls, and any other network equipment.
- Provide IP addresses on the Customer's network for the system servers and third-party application servers. All server names and IP addresses behind Motorola Solutions' Firewalls cannot be changed.
- Provide external interface connection demarcation points at locations agreed to by Motorola Solutions. These locations shall normally be adjacent to the PremierOne equipment rack.
- Provide access, administrative or otherwise, to appropriate systems, locations, information, tools, and equipment to ensure proper connectivity, installation, operations, and maintenance of the system.
- Provide 24-hour access to a secured two-way Internet connection to the system firewalls for the purposes of deployment, maintenance and monitoring.
- Provide for outbound Internet connectivity initialized by system Servers.
- Motorola Solutions' delivery model is reliant upon our ability to perform some tasks remotely, which requires secure, remote broadband access for remote deployment, monitoring and support of the system. Customer-provided high-speed internet access with a minimum bandwidth of 10 Mbps is required at the time of project kickoff and must remain available to Motorola Solutions throughout warranty and support periods to accommodate remote support of the system. In the event that dedicated links are required, a minimum of 7.5 Mbps upload and download access is required. It is the Customer's responsibility to ensure that the aforementioned capacity is available. In the event remote broadband access is not available to Motorola Solutions, preventing us from delivering the contracted service remotely, Motorola

Solutions will provide service on-site at additional cost. The additional cost will be presented to the Customer via the change provision of the contract prior to the delivery of the on-site service.

- Provide, install maintain and service any software as required for anti-viral, anti-malware protection on the system. If the software requires connectivity to a central server for maintenance and updates, the connectivity including ports and access needs to be provided.
- If Customer is going to build their own local queries; the data must exist in databases that can be accessed via standard Microsoft SQL tools. The Customer must also understand the database schema so the table relations can be understood. As applicable, the Customer should also conduct a comprehensive analysis of the data to identify duplicate data/records, lost data, orphaned records, or records that have not been linked properly.

1.2.8.5 CJIS and Compliance

At Motorola Solutions we believe compliance is a team effort. As our customers' partner in compliance, we are committed to employing privacy and security protocols that enable our customers to comply with the most stringent legal and regulatory requirements. In addition, we build on a strong foundation with an architecture (both Azure and on premise) designed and managed to meet a broad set of international compliance standards, as well as region-specific and industry-specific standards.

System services are designed to use FIPS certified technologies to protect data at rest and in transit. PremierOne services utilize FIPS compliant Transport Layer Security (TLS) 1.2 protocol with AES 256-bit message encryption to establish secure communication with PremierOne Records and Records Mobile Clients.

Motorola Solutions employs rigorous third-party audits to verify its adherence to security controls and standards. To demonstrate Motorola Solutions safeguarding of customer data, comprehensive third party audits of primary Software Enterprise development and support operations have been completed and those operations have achieved ISO/IEC 27001:2013 (information security management systems) certification and AICPA SOC2 Type 2 reports will be available in early 2021. ISO/IEC 27017:2015 (information security controls for cloud services), ISO/IEC 27018:2019 (protection of personal information in public clouds) and ISO/IEC 27701:2019 (privacy information management) will be available in mid-2021. Supplemental SOC2 Type 2 reports and ISO/IEC 27001:2013 certifications for the development and support operations at satellite locations have been completed.

Motorola Solutions understands our customers' critical need to safeguard the lifecycle of Criminal Justice Information. To support that need, Motorola Solutions designs its products and services to support compliance with the FBI's Criminal Justice Information Services (CJIS) Security Policy and we commit to the terms of the CJIS Security Addendum. With a dedicated team of CJIS compliance professionals, we assist our customers' through administering and coordinating CJIS compliant personnel credentialing, providing documentation assistance in connection with CJIS audits and advising on how to configure and implement our solutions in a manner consistent with the CJIS Security Policy.

1.3 Records

1.3.1 System Overview

Motorola Solutions is pleased to present the following system for the St. Johns County Sheriff's Office, FL (hereinafter referred to as the "Customer"). Our system is based on our interpretation of the requirements derived from our discussions with you.

Motorola Solutions' offering consists of additional server hardware, server networking hardware, system software, PremierOne application and client software, interfaces and services (as stated in the Statement of Work) for the add-on of PremierOne Records and Records Mobile for the Customer's agency to the existing St. Johns County Fire Rescue ("System Owner") system.

1.3.1.1 Participating Agencies

The designated agencies participating in the system are:

- St. Johns County Fire Rescue (Hosting Agency/System Owner).
- St. Johns County Sherriff's Office (Add-on Agency).

1.3.1.2 Basis for System Sizing

Motorola Solutions uses Call for Service (CFS) and client quantities as the parameters to establish the tiers of infrastructure sizing. Based on the counts provided by the Customer, the system has been sized to add one (1) additional host server to the System Owner's primary and secondary sites and should not exceed the recommended Calls for Service and Clients as listed below:

- Up to 2 Million CAD Calls for Service per year.
- Up to 250 PremierOne CAD concurrent clients.
- Up to 1,000 PremierOne Mobile concurrent clients.

1.3.1.3 Application Software and System Components

This System is comprised of the following component and Subsystem elements:

Records Subsystem

- PremierOne Records version 4.6.X with IBR (FIBR) submission only.
  - PremierOne Records supports the submission of:
    - Crash February 2011.
    - Citations November 11, 2012.
    - Florida UCR June 2008.
    - Human Trafficking and Cargo Theft Reporting (2-17-2015).
    - Hate Crime Report Form (MAR2015).
    - FL IBR/UOF/UAA IEPD 1.2 Errata Revision 1.
- PremierOne Mobile Records.

- PremierOne Records Convert-on-Demand Tool.
- PremierOne Property and Evidence.

System Components

- Interfaces.

The following Figure 1-11 represents a logical illustration of the Records system components.

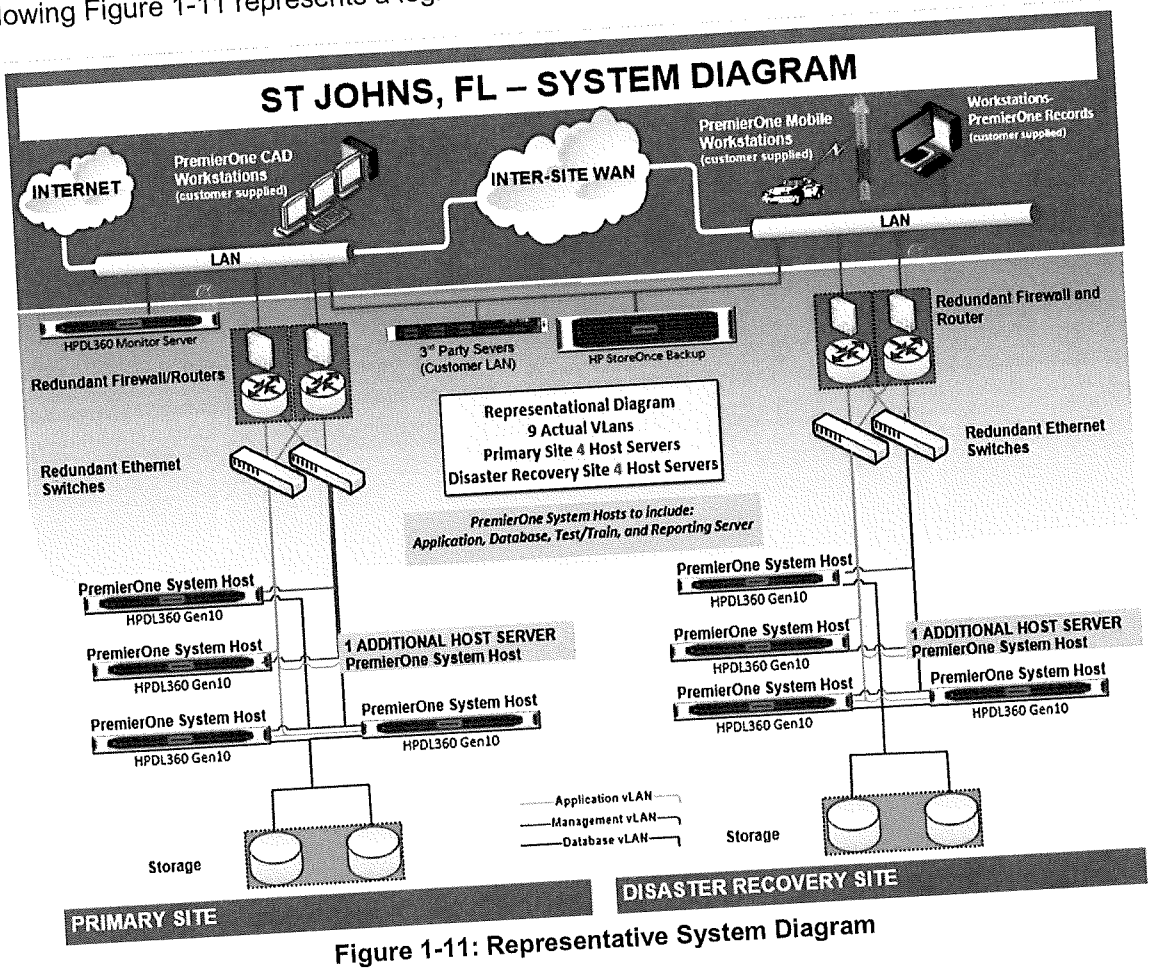


Figure 1-11: Representative System Diagram

1.3.1.4 System Application Client Software Licensing

The following Table 1-11 summarizes the number of PremierOne client application software licenses for all agencies listed in Participating Agencies.

Table 1-11: System Client Licensing

System Client Licenses	Quantity	Type
PremierOne Records	12	Per Seat
PremierOne Records Mobile	150	Per Seat

1.3.1.5 System Interfaces

Table 1-12 below lists the interfaces included in our system. A description of each interface listed in the table below has been provided in Attachment A. Any requests for change to the Interface Description following contract is subject to review and consideration through the change control mechanism of the contract.

Table 1-12: System Interfaces

Interface Name	Interface Description	DR Y/N?
LiveScan (DataWorks Plus)	DataWorks Plus – LiveScan Bidirectional Interface	Y
FileOnQ	EvidenceOnQ (FireOnQ) – Property and Evidence Outbound Interface	Y
State Query	External Query – Suite Interface	Y

1.3.2 Application Descriptions

The following sections provide brief descriptions of PremierOne Records application. PremierOne uses Commercially Off-the-Shelf (COTS) products therefore software development to the application framework is not provided.

1.3.2.1 PremierOne Records

PremierOne Records is Motorola Solutions' next generation law enforcement records management system, based on over 30 years of industry RMS experience, PremierOne Records was designed from the ground up with the current and future needs of public safety agencies in mind. A fundamental goal of PremierOne Records is to provide the greatest level of flexibility. Working with the Advanced Configuration Tool of PremierOne Records allows agencies to add and hide fields, change field labels, make fields required, alter output format, and determine the information that is made available to users and roles.

Users that can benefit from accessing PremierOne Records include but are not limited to Patrol Officers, Records Specialists, Records Supervisors, Retention Specialists, Detectives and Investigators.

1.3.2.2 PremierOne Records Concepts

Records Clients

PremierOne Records provides the same functionality, fields, data, and security to both the officer in the field using a Records Mobile Client and the records bureau user accessing the system through a LAN-connected desktop computer.

- Standard Client – Used for workstations which are connected to the network, such as those on a LAN or WLAN. This self-updating client can be launched from a web browser and can be run without a local installation, thus reducing installation and maintenance costs.
- Records Mobile Client – Used in situations where network connectivity is not assured or nonexistent, such as with mobile units on a wireless network for field based reporting (FBR). Over the wire update and caching services assure that all clients are kept up to date with application updates, changes to forms, code tables, etc., reducing maintenance costs.

Navigation

PremierOne Records was designed with a physical law records department in mind. Users can find information in PremierOne Records in the same areas where you would expect to find them physically in your department. PremierOne Records provides easy and quick access throughout the application. Users can navigate using familiar point-and-click access to modules, similar to a browser. As with a browser, forward and back keys are provided as well as the ability to open additional tabs, allowing multiple modules to be open at a time.

Records Command Line

A command line window can be opened using a hotkey that allows authorized users to perform typical actions such as add, edit and navigation functions without using the mouse. The command line auto-fills both commands and parameters requiring just a few keystrokes to create a new record or access any record in the system. The Records command line window can be displayed even with the other PremierOne Records windows minimized giving the user a cleaner more efficient client. This is especially important for Records Bureau or other data entry users as the can create or edit records much faster, with fewer keystrokes and mouse clicks. This feature is also available in the Records Mobile client allowing patrol officers and other Mobile users to quickly create records without using a mouse. For paper-based agencies that print and use paper copies of records, the command line can be combined with a low cost bar code scanner to greatly improve efficiencies. A bar code can be printed at the bottom of each document that when scanned immediately retrieves the record with no other user intervention. This feature is especially beneficial for document approval or other manual or automated workflow processing.

Motorola Solutions Documents

Users perform the majority of data entry within Motorola Solutions Documents, a forms tool based on patented technology. This technology leverages decades of experience with law enforcement records management systems and is designed to improve data entry efficiency, accuracy and reduce the learning curve for new user. Specially designed functionality such as tabs, search while you type, and 'To do' items are all designed to reduce the effort required to fully document each event.

- **Tabs:** To facilitate data entry, tabs combine like data types such as victim, offense, or property. Within each data type, a user may enter as many of that data type as necessary.
- **Required Fields:** Within any document in PremierOne Records, some fields will be required to be filled in before the document can be saved to the database. Required information helps to preserve the integrity of the document as a whole to make it a valid document. Fields may be required based on business rules established by an agency or because the agency requires data to be collected for reporting purposes. The system may also require certain data fields be completed to assure accurate and complete IBR submissions.
- **Single select code Fields:** Single select code tables allow users to enter only those codes that have been created for a given field.
- **Search while you type:** This functionality displays only the entries in a list that match the text that you type. Search-as-you-type considers all the words in a phrase, not just the first word at the beginning of the phrase.
- **Multi-select Code Tables:** As with single select code tables, multi-select code tables only allow for the acceptable range of data values to be entered.
- **Pull Forward:** You can use Pull Forward to search for and find existing data, and then pull that data into Motorola Solutions Document.

- **To Do List:** Motorola Solutions Documents also check to ensure all required fields have been filled out and are valid. If you omit a required field or have incorrect information, an error message will appear in the Help window of the document. These error messages, or the to-do list, are hyperlinks. They bring the cursor directly to the field that requires attention when the form you are currently working in. Documents that are not complete may be saved as a draft, but the data is not present in the database directly.
- **Only display necessary fields:** This feature of Motorola Solutions Documents only displays those fields necessary to complete the document. When a user enters data that then requires further information, fields for entering the additional data become available. Until those fields are needed, they remain hidden.
- **Photos:** Drag and drop Motorola Solutions Document windows also support drag-and-drop functionality for images.
- **Auto save:** PremierOne Records can be configured to automatically backup or save a document prior to document submission. The document is saved in draft form until it has been submitted.
- **Document Locking:** A locking message displays if another user tries to access a document that is open and locked. Document locks expire when the opened document is closed, or after a configured time (default is 12 hours), whichever comes first. Other users attempting to open a locked document will get a read-only version of the document that displays the document lock message in the lower right corner. Users cannot make edits to the read-only document.
- **Searching:** Free text searching in PremierOne Records provides default basic search and field display functionality as well as advanced search functionality for custom search. Agencies can specify and configure which module data fields are available for searching. Additionally, PremierOne Records has a free text and advanced free text search capability, which functions similarly to web text searches; Users can enter a word or phrase in the free text search field and search across the entire data store for records that match the text or phrase.

1.3.3 Service Solutions

The following sections provide brief descriptions of service solutions delivered as part of the PremierOne offering.

1.3.3.1 Intelligent Data Discovery Services (IDD) for Records

Records IDD Services include instruction in the use of advanced SQL Server Reporting Services (SSRS) features, which will allow for the connection, extraction, and display of data from Records in tailored and customized dashboards.

IDD's use of Microsoft's SSRS employs the data to generate and securely share online dashboards and reports, initiate searches and mine data. The IDD services for Records include the following dashboards:

- Three (3) Tailored Standard Dashboards:
  - Master Index Search Dashboard.
  - Records CompStat Dashboard.
  - Records Major Crimes Dashboard.

- Two (2) Customer Defined Dashboards (built during IDD Training and limited to data existing in the system Records dataset).
- Two (2) days of consultative services pertaining to reports and dashboards for Records.
- Three (3) days of Records Intelligent Data Discovery (IDD) Training (*Additional dashboards are built during the training class).

A single copy of each of the Standard IDD dashboards will be tailored per the provisioning of the P Records system, and delivered to the site. Records IDD is limited to data existing in the system records dataset. Microsoft's SSRS is a reporting and report distribution application. A map view of the data, such as location of Incidents, may be produced as part of the report output, but, with no interactive mapping ability. Total system capacity for IDD is dependent upon the total number of concurrent reports being requested from the Records reporting data warehouse server. Final system capacity is dependent upon final design and report types being generated on a concurrent basis.

1.3.3.2 Legacy Data Access or Data Migration

It is a very common desire for agencies when migrating to new systems to preserve and utilize the data contained in the legacy systems There are two types of data will be accessed or migrated and each type will be treated differently.

The first type of data is configuration data. This consists of code tables and other lists from the existing RMS system. This would include data such as unit identifiers, incident types, personnel information. These data types may either be imported into PremierOne system or manually entered during the provisioning process. For those tables to which data can be imported, the common process is for the Motorola Solutions team to provide spreadsheets to the Customer personnel. Customer personnel will export the data from the existing system, transform it as needed to match the provided spreadsheets and import it into the PremierOne system using the built-in import functionality. Data that will be manually entered during the provisioning process is gathered by the Customer and recorded on provisioning worksheets.

The second type of data is historical data. This consists of the transactional data that is a record of events / incidences that were recorded in the existing RMS system. This would include data such as incident information, unit history information, messaging information.

Below are the strategies being offered to accommodate access to this historical data.

1.3.3.3 Legacy Data Access - Data Warehouse

This data will be extracted from the existing RMS system by the Customer and be incorporated in to a SQL data warehouse supplied by Customer that can be accessed via standard SQL tools. The Customer can then develop queries and format the returns in PremierOne.

The legacy databases must be stored in Customer supplied relational databases (hardware and software) external to the PremierOne system and Motorola Solutions must be able to link directly to the legacy databases from MS SQL Server.

1.3.3.4 Legacy RMS Data Convert on Demand to PremierOne Records

When the need arises to import legacy RMS data into PremierOne Records Motorola Solutions can offer the alternative approach of Convert on Demand (CoD). CoD is a PremierOne Records tool that

can connect to a Microsoft SQL Server database and would be configured to read the legacy database records.

The Customer could inspect the records to determine if they need to be imported into PremierOne Records. If needed, that record or multiple records could be imported into PremierOne Records on an as-needed basis.

The legacy databases must be stored in Customer-supplied Microsoft SQL Server databases (hardware and software) external to the PremierOne system and Motorola Solutions must be able to link directly to the legacy databases from Microsoft SQL Server.

1.3.4 System Platform and Components to be Added to System Owners Existing System

This section discusses the hardware, operating system, and system software of the system to be added on premise at the System Owner's Data Center Facility. Quantities of hardware are provided in the Equipment List.

Note: It is the responsibility of the Customer to provide any specialized hardware and installation to ensure compliance with any Local, State or Federal natural disaster safety regulations.

1.3.4.1 PremierOne System Servers

The system hardware is comprised of Hewlett Packard Enterprise (HPe) servers as physical hosts.

The addition of PremierOne Records to the System Owner's existing PremierOne system will require two (2) additional Host servers for each site (Primary and DR).one additional Host server.

Host servers are HPe DL360c Gen10 servers configured with the following components:

- Dual 12-Core Intel® Xeon® Gold 6146 processor, running at 3.2 GHz, with a 25 MB L3 Cache.
- Each server also contains direct attached storage in the form of two 8 GB micro SD hard drives with Smart Array controllers in a RAID configuration.
- Four (4) - 10 Gigabit network ports.
- Each server is configured with 384 GB RAM.

1.3.4.2 Customer Provided Workstation Specifications

Workstation specifications are representative of workstations used in the testing of the latest release of system software and do not take into account any other applications.

Future releases of the system may dictate changes to the workstation specifications. Each agency should consider their own technology replacement lifecycles and policies for specific purchase decisions.

1.3.4.3 PremierOne Records Workstation Recommended Specifications

Table 1-13: PremierOne Records Workstation Recommended Specifications

Component	Description
Processor	2.0 GHz or better processor.
RAM Memory	2 GB or more of memory.
Display	1024 X 768 or higher pixel, 16+ bit color display.
Keyboard-Mouse	Standard QWERTY Keyboard.
Touchscreen	Optional.
Additional Software Applications	Adobe PDF reader (for help files). SQL Server Express 2017 CU level supporting TLS 1.2 is required. Microsoft .NET Framework v4.8. Microsoft Visual Studio for the creation of In-Module Reports.

1.3.4.4 PremierOne Records Mobile Workstation Recommended Specifications

Table 1-14: PremierOne Records Mobile Recommended Specifications

Component	Description
Processor	Intel Core or AMD Ryzen Series Processors or Newer.
RAM Memory	16 GB or more of memory.
Available Disk Space	20 GB or more of available disk space for PremierOne.
Operating System	Windows 10 Professional 64-bit.
Network Interface Card	Wireless communications minimum 3G network, 4G/5G network recommended.
Display	One (1) – 1024 x 768+ pixel, 16+ bit color display, 11.6" or larger display. Usage on devices with alternative resolutions and smaller screens should be tested and screen settings optimized. Example: On a 10.1" WUXGA screen, use a resolution of 1280 x 800 and a font size of 125%.
Keyboard	Standard QWERTY keyboard and Touchpad / Point Stick (or equivalent mouse device).
Touchscreen	Optional.
Graphics Adaptor	Integrated Processor Graphics or Discrete GPU. Latest available drivers. Shader Model 3.0 or higher is recommended. Adobe PDF reader (for help files).
Additional Software Applications	Adobe PDF reader (for help files). SQL Server Express 2017 CU level supporting TLS 1.2 is required. Microsoft .NET Framework v4.8. Microsoft Visual Studio for the creation of In-Module Reports.

1.3.4.5 Technical Considerations and Design Requirements

The hardware and licensing identified in this system may be subject to change. As technology continues to advance, Motorola Solutions may take advantage of new and different offerings for the betterment of the Customer. Any changes will be reviewed with the Customer.

Customer Responsibilities:

- Supply Windows Server Client Access Licenses (CALs) for all system client devices accessing Records System.
- Supply Mobile Device Management (MDM) software for Mobile devices, as desired by the Customer.
- Provide wireless connectivity and middleware to deliver mobile Virtual Private Network (mVPN) with routing and IP persistence to the system network. Optimal system application performance on mobile workstations requires 4G connectivity.
- Provide advanced authentication for Mobile device connectivity if required.
- Provide a network diagram depicting all the devices, device types, and interfaces that the system will connect to and through, including, but not limited to all blocked ports, hubs, switches, routers, firewalls, and any other network equipment.
- Provide IP addresses on the Customer's network for the system servers and third-party application servers. All server names and IP addresses behind Motorola Solutions' Firewalls cannot be changed.
- Provide external interface connection demarcation points at locations agreed to by Motorola Solutions. These locations shall normally be adjacent to the PremierOne equipment rack.
- Provide access, administrative or otherwise, to appropriate systems, locations, information, tools, and equipment to ensure proper connectivity, installation, operations, and maintenance of the system.
- Provide 24-hour access to a secured two-way Internet connection to the system firewalls for the purposes of deployment, maintenance and monitoring.
- Provide for outbound Internet connectivity initialized by system Servers.
- Motorola Solutions' delivery model is reliant upon our ability to perform some tasks remotely, which requires secure, remote broadband access for remote deployment, monitoring and support of the system. Customer-provided high-speed internet access with a minimum bandwidth of 10 Mbps is required at the time of project kickoff and must remain available to Motorola Solutions throughout warranty and support periods to accommodate remote support of the system. In the event that dedicated links are required, a minimum of 7.5 Mbps upload and download access is required. It is the Customer's responsibility to ensure that the aforementioned capacity is available. In the event remote broadband access is not available to Motorola Solutions, preventing us from delivering the contracted service remotely, Motorola Solutions will provide service on-site at additional cost. The additional cost will be presented to the Customer via the change provision of the contract prior to the delivery of the on-site service.
- Provide, install, maintain and service any software as required for anti-viral, anti-malware protection on the system. If the software requires connectivity to a central server for maintenance and updates, the connectivity including ports and access needs to be provided.
- For Records, unless and/or except as explicitly stated in this document, this system does not include the generation of any customer-specific Advanced Configuration Tool (ACT) modules, forms, printouts, reports or queries.

- If Customer is going to build their own local queries; the data must exist in databases that can be accessed via standard Microsoft SQL tools. The Customer must also understand the database schema so the table relations can be understood. As applicable, the Customer should also conduct a comprehensive analysis of the data to identify duplicate data/records, lost data, orphaned records, or records that have not been linked properly.

1.4 Jail Solution for PremierOne Records

1.4.1 System Overview

Motorola Solutions is pleased to present the following system for the St. Johns County Sheriff's Office, FL (hereinafter referred to as the "Customer"). Our system is based on our interpretation of the requirements derived from our discussions with you.

Motorola Solutions' offering consists of additional server hardware, server networking hardware, system software, PremierOne application and client software, interfaces and services (as stated in the Statement of Work) for the add-on of a jail management solution for PremierOne Records to the existing St. Johns County Fire Rescue ("System Owner") system.

1.4.1.1 Participating Agencies

The designated agencies participating in the system are:

- St. Johns County Fire Rescue (Hosting Agency/System Owner).
- St. Johns County Sherriff's Office (Add-on Agency).

1.4.1.2 Application Software and System Components

This System is comprised of the following component and Subsystem elements:

Records Subsystem

- Jail Management Solution for PremierOne Records.

The following Figure 1-12 represents a logical illustration of the system components.

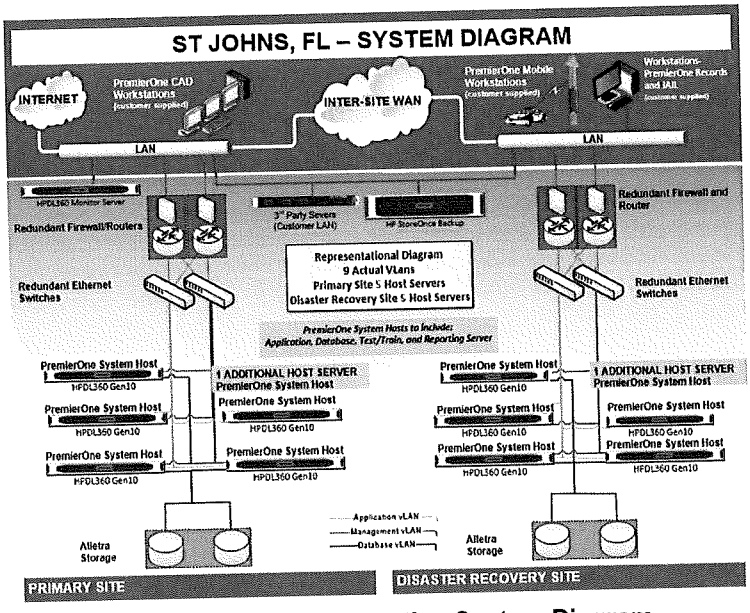


Figure 1-12: Representative System Diagram

1.4.1.3 System Application Client Software Licensing

The following Table 1-15 summarizes the number of PremierOne client application software licenses for all agencies listed in Participating Agencies.

Table 1-15: System Client Licensing

System Client Licenses	Type
Jail Management Solution for PremierOne Records	Site License

1.4.2 Application Descriptions

The following sections provide brief descriptions of Jail Management Solution for PremierOne Records application. PremierOne uses Commercially Off-the-Shelf (COTS) products therefore software development to the application framework is not provided.

1.4.2.1 Jail Management Solution (JMS)

The Jail Management Solution provide powerful tools to gather a broad range of vital inmate data. The ability to flag records enhance safety for all users. The intuitive system includes simplified booking processes and jail log information, enabling users to include multiple offences and inmates on a single entry. Additionally, the system captures and integrates corrections data system-wide, creating seamless data flow, and allowing users to process inmates from start to finish more efficiently.

Intake Workflow

The Intake Workflow enables a booking officer to capture the inmate's information from the arresting officer during the intake process. The system captures relevant name and demographic information, arrest information, charges, victim information, and probable cause statement along with notes for any immediate needs the inmate might have. Booking officers can record the bond amount for each charge. The system also captures one or more physical searches performed during intake. Users can refuse custody as needed, recording the reason for refusal. When custody is accepted a booking record is created to complete the booking process.

Booking Process

JMS streamlines inmate booking with simple, step-by-step processes and seamless integration with the Records Management system. As users enter inmate information into the system, menu-driven options facilitate the collection of important details regarding property taken, property issued, inmate medical conditions, and risk assessments. The checklist screen also allows users to see what has been completed in the booking process.

Biometric Positive ID

During the booking process biometric positive ID captures one or more fingerprints from an inmate. Upon release, users can compare the fingerprint captured during the booking process to verify the correct inmate is being released

Assessments

The Assessment feature enables users to place inmates in accordance with their risk factors, enhancing safety for inmates and jail staff alike. Users can create custom inmate assessment questionnaires that determine security restrictions and appropriate medical care. This Assessment

feature is decision-tree based, meaning that each question is dynamically determined by the inmate's previous answer. After an assessment is complete, an inmate record is automatically tagged with name alerts, flags, medical conditions, security classifications, and risk factors, as appropriate.

Inmate Flags

Users can relay vital inmate information to jail personnel using the Inmate Flags feature. If, for example, an inmate record is marked with a flag denoting that he or she is prone to violent behavior, users can click the flag to display the code, description, and detailed instructions regarding that inmate. Users can also assign optional expiration dates to these flags.

Inmate Activity

Inmate Activity combines scheduled inmate activities and past activity logs into a single location. Users can create a single activity record and add as many inmates and officers to the activity as needed. Capture notes for the activity or for an individual inmate. Apply filters to limit the activities to only those you are interested in.

Keep Separate

Users can keep specific inmates isolated from each other using the Keep Separate feature. The software provides notification when a Keep Separate violation has occurred. This feature also allows agencies to include an expiration date and narrative for each Keep Separate record.

Scheduled Events

The system enables officials to maintain situational awareness of all scheduled events. Users can set events like court appearances, work releases, and any other activity to recur daily, weekly, monthly, or annually. They can also partition events by agency as appropriate. Agencies have the ability to combine levels and locations in a jail and assign personnel to specific areas. The module's event viewer provides the time, event, inmate name, and other details that may be important for security purposes. Additionally, users can create reminders that show approaching or past due events. The software allows users to snooze, dismiss, or open event details at any time.

Jail Log

Administrators can add multiple officers and inmates to the same log entry with the Jail Log feature; this eliminates the need to create a separate incident for every person involved in an event. Users can also automatically create a jail incident from an inmate log entry. Narratives are stored in a separate detail table for security purposes.

Jail Incident Report

A Jail Incident Report provides a summary of jail incident records, capturing information about events leading to disciplinary action, criminal charges, or exposure to liability. Information reported includes inmates, officers involved, and a description of the event. An incident report can be refined by:

- Jail Incident Number.
- Time reported.
- Incident narrative.
- Incident supplemental narrative.

JMS controls who has access to incident report information by agency-defined partitions and detailed permissions

Inmate Movement

Using a Customer provided scanner and barcoded wristband system, users can efficiently track inmates as the inmates move from place to place. Agencies can create custom wristbands for each inmate and quickly log the movement of groups or individuals as they enter or leave different locations. The system also restricts users from moving inmates into an area where maximum capacity has been met, and provides a warning when gender, juvenile, or security restrictions are violated.

Commissary Management

The Commissary Management module assists correctional facilities in accurately managing inmate purchases and maintaining total inventory control. The software's all-inclusive design provides users with features such as:

- Tracking individual commissary transactions.
- Summarizes purchase and sales activities through detailed reports.
- Manages supplier accounts.

Commissary Supplier Data

Users can quickly view records for each company that supplies commissary items to your facility. In the Commissary Supplier screen, users can post or cancel orders, and track inventory. The Commissary Item screen can also be set to automatically reorder items based on current inventory levels.

Commissary Items

Users can filter approved or restricted items, keep track of supplier and product information, and control purchasing restrictions. The software can filter approved items for indigent inmates as well as items that certain inmates cannot have. Each commissary item record contains information on the supplier of each item, unit size and cost, re-orders, current balances, and purchasing restrictions. Available commissary items and prices can be filtered for inmates housed in specific areas, and the Single Commissary List shows the items available to an individual inmate.

Item Purchases

Users can view all inmate purchases from the Enter Commissary Purchases screen. The software creates a file detailing all transactions made with each purchaser, including the individual's account balance at the close of each transaction. Additionally, users can access supplier summaries and purchases, item cost, inventory orders and value, current inventory levels, orders pending, purchases payable, unit reports, and inmate purchase summaries.

Inmate Work Assignments

The Inmate Work Assignments module enables users to create profiles within the system that ties inmates to their respective jobs, facilitating accurate record keeping. Among the systems' many advanced features, administrators can associate a work credit for each job profile according to hours worked, and/or deduct work time from an inmate's sentence based on the ratio set up in the job profile.

This facilitates a culture of accountability and accomplishment by helping jail staff keep track of an inmate's work, and helping incentivize inmates to be productive and reach work goals. Additionally, the system will store past and current work assignments, giving staff a full picture of an inmate's work history. This can facilitate placement in new job openings, which users can view the second they become available.

Disciplinary Actions

The Disciplinary Actions module facilitates accountability in numerous ways from a single screen. Users can accomplish many tasks in the module, including:

- Track rule violations and subsequent discipline.
- Add narrative or supplementary data.
- Present all disciplinary hearing information in one place.
- Attach disciplinary sanctions.
- Note the timeframe for a sanction.

Additionally, the system will present all disciplinary hearing information including the date and time of the hearing, the incident number, names of disciplinary board members, and history of disciplinary action. Lastly, the system's single-source, unified database will flag inmates with active sanctions throughout the system until a sanction either expires or is manually removed from an inmate record.

1.4.3 Service Solutions

The following sections provide brief descriptions of service solutions delivered as part of the PremierOne offering.

1.4.3.1 Legacy Data Access or Data Migration

It is a very common desire for agencies when migrating to new systems to preserve and utilize the data contained in the legacy systems There are two types of data will be accessed or migrated and each type will be treated differently.

The first type of data is configuration data. This consists of code tables and other lists from the existing RMS system. This would include data such as unit identifiers, incident types, personnel information. These data types may either be imported into PremierOne system or manually entered during the provisioning process. For those tables to which data can be imported, the common process is for the Motorola Solutions team to provide spreadsheets to the Customer personnel. Customer personnel will export the data from the existing system, transform it as needed to match the provided spreadsheets and import it into the PremierOne system using the built-in import functionality. Data that will be manually entered during the provisioning process is gathered by the Customer and recorded on provisioning worksheets.

The second type of data is historical data. This consists of the transactional data that is a record of events / incidences that were recorded in the existing RMS system. This would include data such as incident information, unit history information, messaging information.

Below is the strategy being offered to accommodate access to this historical data.

1.4.3.2 Legacy Data Access - Data Warehouse

This data will be extracted from the existing JMS system by the Customer and be incorporated in to a SQL data warehouse supplied by Customer that can be accessed via standard SQL tools. The Customer can then develop queries and format the returns in PremierOne.

The legacy databases must be stored in Customer supplied relational databases (hardware and software) external to the PremierOne system and Motorola Solutions must be able to link directly to the legacy databases from MS SQL Server.

1.4.4 System Platform and Components to be Added to System Owners Existing System

This section discusses the hardware, operating system, and system software of the system to be added on premise at the System Owner's Data Center Facility. Quantities of hardware are provided in the Equipment List.

Note: It is the responsibility of the Customer to provide any specialized hardware and installation to ensure compliance with any Local, State or Federal natural disaster safety regulations.

1.4.4.1 PremierOne System Servers

The system hardware is comprised of Hewlett Packard Enterprise (HPe) servers as physical hosts.

The addition of the jail management solution for PremierOne Records to the System Owner's existing PremierOne system will require two (2) additional Host servers for each site (Primary and DR).

Host servers are HPe DL360c Gen10 servers configured with the following components:

- Dual 12-Core Intel® Xeon® Gold 6146 processor, running at 3.2 GHz, with a 25 MB L3 Cache.
- Each server also contains direct attached storage in the form of two 8 GB micro SD hard drives with Smart Array controllers in a RAID configuration.
- Four (4) - 10 Gigabit network ports.
- Each server is configured with 384 GB RAM.

1.4.4.2 PremierOne Jail Management Solution Hardware Guidelines

These hardware guidelines provide general recommendations for customers purchasing a new system. Server load is directly related to how the customer uses the software. The guidelines listed above account for this variability in software usage by providing ranges in the recommendations for processors and memory. Customers that have purchased Jail modules will typically experience a heavier load due to the advanced processing requirements of these modules.

Table 1-16: Jail Hardware Specifications

Concurrent Users[1]	Processor	Storage[2]	Memory[3]	Hypervisor
150 – 200	16 Cores	SAS RAID Controller 10k to 15k SASA Drives or SSD RAID Level 5 or 6	64 GB	VMware

Notes:

- Note that a concurrent user is defined as an instance of the Jail client.
- Three Direct-Attached Storage (DAS) using a SAS host interface is generally recommended due to its associated higher performance and lower cost. This storage option can be implemented using either an internal SAS RAID controller or an external storage device.

Conversely, Network-Attached Storage (NAS) systems are not recommended due to its decreased I/O performance. Alternatively, Storage Area Network (SAN) systems using a Fiber Channel host interface may be considered since they will provide higher performance and powerful expansion capabilities, but will also typically be accompanied with higher cost and complexity. All recommended storage options indicate a hardware RAID Level 5 or 6 implementation for maximizing both data integrity and performance across all needs. Note that software RAID implementations will incur a severe performance hit on your server and must not be used.

- Note that excess RAM not used for computational purposes is used to cache file accesses, increasing performance dramatically. Motorola Solutions' rule of thumb on new server sizing for RAM is to exceed the software requirements for memory by at least 2.5 times, devoting 60% of RAM to file caching. This is needed since the Jail application's database access is typically 80-90% in favor of reads over writes. Therefore, configuring a system with more RAM will improve performance on 64-bit systems.

1.4.5 Customer Provided Workstation Specifications

Workstation specifications are representative of workstations used in the testing of the latest release of system software and do not take into account any other applications.

Future releases of the system may dictate changes to the workstation specifications. Each agency should consider their own technology replacement lifecycles and policies for specific purchase decisions.

1.4.5.1 Jail Management Solution Workstation Recommended Specifications

Table 1-17: Jail Management Solution Recommended Specifications

Component	Description
Processor	Intel i3, i5, or i7 2.0 GHz dual core processor.
RAM Memory	16 GB or more memory.
Available Disk Space	20 GB or more available disk space for PremierOne.
Operating System	Windows 10 Professional 64-bit.
Network Interface Card	100 Mbps with 10 ms or less round-trip latency.
Display	1920x1080 resolution.
Monitor	21-inch monitor.

1.4.6 Technical Considerations and Design Requirements

The hardware and licensing identified in this system may be subject to change. As technology continues to advance, Motorola Solutions may take advantage of new and different offerings for the betterment of the Customer. Any changes will be reviewed with the Customer.

Customer Responsibilities:

- Add the required system platform and components as noted in Section 1.5.

- Supply Windows Server Client Access Licenses (CALs) for all system client devices accessing Jail Management Solution.
- Provide wireless connectivity and middleware to deliver mobile Virtual Private Network (mVPN) with routing and IP persistence to the system network. Optimal system application performance on mobile workstations requires 4G connectivity.
- Provide a network diagram depicting all the devices, device types, and interfaces that the system will connect to and through, including, but not limited to all blocked ports, hubs, switches, routers, firewalls, and any other network equipment.
- Provide IP addresses on the Customer's network for the system servers and third-party application servers. All server names and IP addresses behind Motorola Solutions' Firewalls cannot be changed.
- Provide external interface connection demarcation points at locations agreed to by Motorola Solutions. These locations shall normally be adjacent to the PremierOne equipment rack.
- Provide access, administrative or otherwise, to appropriate systems, locations, information, tools, and equipment to ensure proper connectivity, installation, operations, and maintenance of the system.
- Provide 24-hour access to a secured two-way Internet connection to the system firewalls for the purposes of deployment, maintenance and monitoring.
- Provide for outbound Internet connectivity initialized by system Servers.
- Motorola Solutions' delivery model is reliant upon our ability to perform some tasks remotely, which requires secure, remote broadband access for remote deployment, monitoring and support of the system. Customer-provided high-speed internet access with a minimum bandwidth of 10 Mbps is required at the time of project kickoff and must remain available to Motorola Solutions throughout warranty and support periods to accommodate remote support of the system. In the event that dedicated links are required, a minimum of 7.5 Mbps upload and download access is required. It is the Customer's responsibility to ensure that the aforementioned capacity is available. In the event remote broadband access is not available to Motorola Solutions, preventing us from delivering the contracted service remotely, Motorola Solutions will provide service on-site at additional cost. The additional cost will be presented to the Customer via the change provision of the contract prior to the delivery of the on-site service.
- Provide, install, maintain and service any software as required for anti-viral, anti-malware protection on the system. If the software requires connectivity to a central server for maintenance and updates, the connectivity including ports and access needs to be provided.
- If Customer is going to build their own local queries; the data must exist in databases that can be accessed via standard Microsoft SQL tools. The Customer must also understand the database schema so the table relations can be understood. As applicable, the Customer should also conduct a comprehensive analysis of the data to identify duplicate data/records, lost data, orphaned records, or records that have not been linked properly.

MOTOROLA SOLUTIONS

Section 2

Statement of Work

State-of-the-Art Technology for a Safe and Resilient Community

September 12, 2022

St. Johns County, FL

Table of Contents

Section 2

Statement of Work

2.1 APX Radios

This Statement of work section covers the APX Next Initial Programming, SmartConnect and Smart Mapping. Motorola Solutions is proposing to St. Johns County the following APX Next radios and radio related configuration.

Table 2-1: Solution Components

	Major Components
Infrastructure	Firewall and licensing
St. Johns Sheriff's Office APX Next	Qty 756 APX Next 700/800 MHz radios and Accessories
St. Johns Fire Rescue APX Next	Qty 450 APX Next XE 700/800 MHz radios and Accessories Qty 30 APX Next XE 700/800 MHz radios and VHF and Accessories

2.1.1 Project Roles

The following personnel will be assigned as required throughout the deployment of this Statement of Work.

Motorola Solutions Project Manager

The Motorola Solutions Project Manager is the single point of contact with the Customer Project Manager and is responsible for scheduling and coordinating Motorola Solutions resources and task completion. The Motorola Solutions Project Manager assures the delivery of contracted components in accordance with the project schedule and is responsible for the transition of the Customer to Motorola Solutions Customer Support post deployment.

Motorola Solutions ASTRO Field Engineer

Installs and configures the ASTRO software components of the system. Configures ASTRO network components to provide connectivity to the cloud platform.

Motorola Solutions Architect (SA)

Provides the solution overview, performs provisioning planning and data collection, provisions CommandCentral Mapping Users, Devices, and Groups, and conducts an operational demonstration.

Motorola Solutions Support

Motorola Solutions Support organization provides varying levels of service up to and including technical support services. Following project finalization, ongoing service will be provided by Motorola Solutions Support in accordance with the Customer support plan.

Customer Project Manager

The Customer Project Manager is responsible for scheduling and coordinating Customer/agency resources and task completion. The Customer Project Manager works collaboratively with the Motorola Solutions PM to assure completion of Customer tasks in accordance with the project schedule.

Customer System Administrator(s)

Responsible for SmartConnect User and radio subscriber provisioning via CommandCentral Admin and ongoing coordination with Motorola Solutions System Support.

Customer Network Administrator

Responsible for network and firewall configuration. Works with ASTRO Field Engineer to provide and verify network connectivity between the ASTRO system and the cloud platform.

2.1.2 Initial Programming

Motorola Solutions' Initial Programming service assures that customers' first APX NEXT subscribers are programmed and operational on their ASTRO system. This service is provided remotely by a Motorola Solutions technician.

The APX NEXT subscriber is programmed using RadioCentral. The initial programming service is intended to guide Customers and their supporting organizations (MR's, shops, etc.) through the transition from CPS or RM to the new programming tools.

APX NEXT Application Services, such as SmartLocate and SmartConnect, also require specific configurations within the APX NEXT The initial programming service assures that the subscribers are configured to support these applications.

Figure 2-1: APX NEXT

The service provides the following:

- Overview APX NEXT programming process and tools.
- Information on available APX NEXT training classes.
- Guided supplement to MyView and RadioCentral training.
- Guided RadioCentral access management in MyView.
- Radio Central installation and operation.
- Guided Code Plug Conversion support.
- APX NEXT Application Services settings.
- Consultation on using RadioCentral to support existing programming processes.

At the completion of the Initial Programming service customers are ready to support the addition of APX NEXT devices using their existing technical support services.

The APX Next subscriber is a smart converged device that utilizes RadioCentral for codeplug management and broadband (LTE or Wi-Fi) connections for device programming. The following steps provide a high level overview of the programming process. The Motorola Solutions technician will guide the users through this process:

- When an APX NEXT radio is ordered, an email is sent to the specified Customer System Administrator from "noreply@radiocentral.com".

> **Subject:** RadioCentral Devices Available
>
> **Hello Motorola Customer,**
>
> Congratulations! **XX** radios associated with Motorola Order **#XXXXXXXXXX** for Purchase Order **#XXXXXXXXXX** are now available on your **[AGENCY NAME]** provisioning agency.
>
> The radios are shipping to:
> **[CUSTOMER ADDRESS]**
>
> To program your new device(s), you need to download the radio central client from MyView>Device Management section.
>
> You should have already received access to MyView account. Please check your email for access instructions. If you have difficulty accessing your MyView account, please visit https://myaccount.motorolasolutions.com or call 800-674-4357 for assistance.
>
> To assure proper device deployment please ensure that your organization has received the radios **before scheduling** specific programming jobs.
>
> **Thank you,**
>
> Motorola Solutions RadioCentral Team
> +1.800.674.4357
> RadioCentral@motorolasolutions.com

- Follow the link in the email to set up the MyView Portal User Accounts. User Accounts are required for each technician that will use the RadioCentral client.
- Download and install Radio Central Client, launch the application, and login using a MyView User Account.
- Import the APX codeplug (*.mc) into Radio Central using its Codeplug Migration function.
- Program radio.

2.1.3 Initial Programming Statement of Work

The Statement of Work defines the principal activities and responsibilities of Motorola Solutions and the Customer during the Initial Programming service. The initial programming process is a collaborative effort between Customer system administrators, supporting organizations (shop or MR), and Motorola Solutions.

The Initial Programming service is provided remotely by a Motorola Solutions technician and involves the following steps:

Table 2-2: Initial Programming Steps

Step	Description
Discovery Session	Process overview and data collection.
Account and Tool Setup	Assure technicians have the required accounts and tools

Step	Description
Codeplug Conversion	Convert existing Codeplugs to APX NEXT and configure applications
Application Configuration	Add APX Next application configurations to Codeplug
ASTRO 25 Provisioning	Provision APX NEXT devices on the ASTRO System.
Programming and Verification	Program APX NEXT over LTE and validate operation
Additional Training	Overview of available training on APX NEXT programming and support documentation.

These project steps are logical groupings of related activities required to complete the project. Each step includes tasks and deliverables that both Motorola Solutions and the Customer are responsible to complete. These are described in detail within the Statement of Work.

2.1.3.1 Discovery Session

A Motorola Solutions ST will conduct a remote discovery session with the Customer System Administrator and Customer, shop, or MR technician(s) responsible for programming subscribers. The discovery session is an opportunity to document the organizations and people who will have ongoing responsibility for subscriber programming and configuration.

Motorola Solutions Responsibilities

- Conduct a remote discovery session with representatives from the Customer and any supporting organizations such as shops or MR's.
- Document the names and email addresses of the Customer System Administrator(s).
- Document the names and email addresses of the technicians responsible for subscriber programming.
- Identify existing codeplugs and determine which should be used for APX NEXT.
- Document existing Codeplug management processes.
- Identify the owners of System Keys (hardware key and/or software key). RadioCentral requires loading the system keys for all systems in the codeplug prior to scheduling a Write job to program an APX Next subscriber).
- Determine who controls the Key Loader if encryption is used. The KVL must be physically connected to the APX NEXT radio to load the initial encryption keys. A KVL-4000 or KVL-5000 keyloader is required for APX NEXT. Older versions are not compatible with the APX Next.

Customer Responsibilities

- Identify required participants from the Customer's organization, shop, or MR.
- Participate in the discovery session meeting.

Completion Criteria

- Discovery session completed.

2.1.3.2 Account & Tool Setup

APX NEXT subscribers are programmed using RadioCentral. Access to the RadioCentral tool requires a MyView (https://myview.motorolasolutions.com) account and the installation of Radio Central on a local Windows computer. The Account and Tools Setup process is an opportunity for an Motorola Solutions ST to provide hands on training and guide the System Administrator through the account creation and RadioCentral installation process.

Motorola Solutions Responsibilities

- Conduct a remote configuration session to guide the Customer System Administrator through MyView navigation. For reference see: **MN006056A01 RadioCentral User Guide** on MOL or LMX.
- Guide Customer Administrator through Adding Users to MyView and Assigning the User to RadioCentral agency for each of the subscriber programming technicians. For reference see: Managing RadioCentral access through MyView.

Note that MyView does not allow Customer administrators to add Motorola Solution accounts directly. To add a Motorola employee to a customer's MyView account and assign to a RadioCentral agency, email the request to onbaording@motorolasolutions.com (for urgent requests contact John Kopinski or call 800-674-4357 #7).

- Guide Customer, shop, or MR technician through the RadioCentral download, installation, and login process.
- Customers with existing MyView or MOL accounts would use their current Login ID and Password to log into MyView and RadioCentral.
- To verify MyView Login ID or Reset Password, use https://myaccount.motorolasolutions.com or call 800-674-4357 #7.

Customer Responsibilities

- Create MyView user accounts and assign to RadioCentral agency for all technicians.
- Download and setup RadioCentral.

Completion Criteria

- Programming technicians have installed RadioCentral, can access the tool, and are able to access the Customer's radios within RadioCentral.

2.1.3.3 Codeplug Conversion

The APX NEXT requires a suitable codeplug for operation on the Customer's ASTRO system. As it has with all earlier versions of programmable subscribers, the codeplug encapsulates a wide variety of device configurations including subscriber features, talkgroup assignments, button assignments, and other parameters.

The codeplug conversion process allows RadioCentral users to convert an existing APX codeplug to a format suitable for the APX NEXT. RadioCentral includes a conversion utility to simplify this process. However, there are some manual operations required if the source codeplug includes features not supported by the APX NEXT.

The objectives of the codeplug conversion process are twofold. First, it assures that the APX NEXT has an operational codeplug. Second, it enables the Customer, MR, or shop technician to convert additional codeplugs independently.

Motorola Solutions Responsibilities

- Work with Customer to identify the existing APX codeplugs suitable for the APX NEXT subscribers. The Initial Programming service provides support for converting up to three (3) codeplugs.
- Verify that there are no errors in the source codeplugs. RadioCentral will not successfully convert Codeplugs with errors.
- Guide Customer through the APX codeplug conversion process in RadioCentral.
- Identify and document all required pre-conversion codeplug changes. Some APX features (e.g. OTAP) are no longer supported in the APX NEXT. These features must be disabled prior to the conversion process. Complete documentation of pre-conversion changes assures that Customers can repeat the process independently if required.
- Guide Customer, shop, or MR technician through the SmartProgramming process.

Customer Responsibilities

- Provide APX codeplug(s) that contains the system and subscriber configuration desired for the APX NEXT. Customers may have several codeplugs (e.g. Police, Fire, EMS).
- If required, create a new APX NEXT codeplug based on an existing Motorola Solutions XTL/S subscriber or another manufacturer's device. Please contact your Motorola Solution Account Executive to discuss support options for this activity.

Completion Criteria

- Up to three (3) codeplugs converted from APX to APX NEXT format.

2.1.3.4 APX Next Application Setup

APX NEXT Applications include SmartLocate, SmartMapping, SmartConnect, ViQi Virtual Partner, and SmartMessaging. These applications require a software subscription, subscriber Codeplug configuration, and a deployment project to fully deploy and configure the hosted and on premise ASTRO components.

If a software feature enablement project was procured in conjunction with the APX Next subscribers the Motorola Solutions project team will provide the specific APX Next application settings. If the APX Next subscribers were procured without an application deployment project then the technician will provide Codeplug settings suitable for demonstrating the application capability in a test environment.

Motorola Solutions Responsibilities

- Configure subscription software settings (SmartLocate, SmartConnect, SmartMapping, SmartMessaging, or ViQi, etc.). These settings are based on either the default "Out of Box" settings or, in the event that feature enablement projects were purchased with the APX NEXT, the SI Project-specified application settings.

Customer Responsibilities

- None.

Completion Criteria

- APX NEXT Application features configured in Codeplug.

2.1.3.5 ASTRO 25 Provisioning

APX NEXT subscribers must be provisioned in the ASTRO Provisioning Manager and assigned a Unit ID in the same fashion as APX subscribers.

Motorola Solutions Responsibilities

- No deliverables.

Customer Responsibilities

- Provision all APX NEXT devices using the ASTRO Provisioning Manager.
- Provide APX NEXT Serial Numbers and associated Unit IDs to Motorola Solutions for use provisioning the subscription applications.

Completion Criteria

- APX NEXT subscribers provisioned on ASTRO System.

2.1.3.6 Programming and Verification

Once the APX NEXT Code plug is prepared, a technician may use RadioCentral to schedule a Write job. This uses SmartProgramming to send the configuration to the APX Next over either a LTE or Wi-FI connection.

Motorola Solutions Responsibilities

- Conduct a remote session to guide the programming technician through the SmartProgramming process.
- Guide the technician through the process of loading System Keys into RadioCentral.
- Guide the technician through the process of using the KVM to load encryption keys into the APX Next subscriber.
- Guide the technician through the firmware version upgrade.
- Guide the technician through scheduling a Write job to apply the updates to radios over LTE or Wi-Fi.
- Assist with the resolution of any problems the technician encounters.

Customer Responsibilities

- Programming technician participates in the Programming and Verification session.
- Perform all hands-on tasks such as managing hardware System Keys and KVM key loaders.
- Perform all programming tasks on the local RadioCentral application using the technician's account.
- Validates the subscriber operation on the local ASTRO system

Completion Criteria

- APX NEXT subscriber operational on the Customer's ASTRO system.

2.1.3.7 Follow Up Training and Resources

Motorola Solutions Initial Programming service is intended to facilitate a quick transition to the APX NEXT. For Customer, shops, or MRs that would like to learn more about the programming tools the following documentation and training classes and resources are available from Motorola Solutions Training Services: https://learning.motorolasolutions.com/:

- MN005015A01 MyView Portal User Guide
- AST0082 Get Ready for APX NEXT
- AST0084 APX NEXT First Steps
- AST4002 APX NEXT Overview
- AST4004 RadioCentral Overview
- AST4005 RadioCentral Workshop
- AST0086 APX NEXT Instructor's Office Hours, Prereqs: AST4004 & AST4005
- MN006056A01 RadioCentral User Guide
- APX NEXT: APX NEXT Overview | Two-way Smart Radio
- PMLN7996A APX NEXT Quick Start Guide:
- MN005642A01 APX NEXT User Guide: APX NEXT User Guide
- MN005717A01 Out of box provisioning leaflet: APX NEXT Provisioning Leaflet
- APX NEXT Programming Guide: Programming APX NEXT
- ASTRO_RCOLH ASTRO RadioCentral Online Help
- APX NEXT Help Desk: 800-MSI-HELP (800-674-4357)

2.1.4 SmartConnect Statement of Work

The Statement of Work defines the principal activities and responsibilities of Motorola Solutions and the Customer during SmartConnect deployment. The deployment process is a collaborative effort between Customer system administrators, subject matter experts, and the Motorola Solutions deployment team. Deployments involve the following steps:

Table 2-3: SmartConnect Set-up Steps

Step	Description
Project Initiation	Formal project kickoff and planning sessions
Domain and Device Setup	Provision ASTRO subscribers on the cloud platform
SmartConnect Gateway Setup	Enable connection between ASTRO system and Cloud
ASTRO Preparation	Assure ASTRO system has the correct version and components
ASTRO System Configuration	Load and Configure software for SmartConnect
Demonstration	Demonstrate SmartConnect operation
Training	SmartConnect operational and administrator training
Project Finalization	Delivery of as-built documentation and hand over to support

These project steps are logical groupings of related activities required to complete the project. Each step includes tasks and deliverables both Motorola Solutions and the Customer are responsible to complete. These are described in detail within the Statement of Work.

Motorola Solutions' project manager will use the Statement of Work to guide the deployment process and coordinate the activities of all Motorola Solutions resources and teams. The project manager will also work closely with the Customer's project manager to clearly communicate the required deployment activities and schedule tasks involving Customer resources.

2.1.4.1 Project Documentation

The following documents are delivered during the deployment process. Some are standard product documentation and others are project specific and are produced during the project.

Product Documentation

CommandCentral System Administration Guide. The Administration Guide includes information about the CommandCentral Admin tool, User provisioning, and other system administration tasks.

Operational Demonstration Script. The Operational Demonstration Script provides a customer-specific procedure for validating system configuration and operation. It references the customer specifics detailed in the Configuration Document.

SmartConnect Configuration Document. Describes the SmartConnect configuration including LMP parameters, config changes to the UNC, a backhaul capacity report, Internet connection information for the Internetworking firewall and CommandCentral Admin parameters. It is created during the project, used to configure and validate the application and network configurations, and finalized to serve as project as-built documentation. Provided to both the Customer and the Motorola Solutions Support Team.

2.1.4.2 Initiation

Project initiation occurs after procurement of SmartConnect deployment services and notice to proceed is received. During this phase, the Motorola Solutions and Customer project managers are assigned, assemble their teams, and establish a working relationship. The managers jointly review the project plan, deliverables, and schedule. Each manager coordinates preparatory tasks that serve as a foundation for specific deployment activities.

Motorola Solutions Responsibilities

- Schedule a kick-off call between Customer and Motorola Solutions project managers.
- Establish a communications plan.
- Review project work plan, schedule, and resources.
- Provide standard product documentation.
  - CommandCentral System Administration Guide.
  - CommandCentral Network Connectivity Guide.
  - SmartConnect User Guide.

Customer Responsibilities

- The customer project manager coordinates with the agency(s) and identifies the subject matter experts, system administrators, and network administrators that will participate in the project and complete Customer tasks.
- Review the Solution Description and prerequisites with the customer project team. Assure that all required components are in place or initiate procurement.
- Schedule agency personnel time to participate in the deployment process.

Completion Criteria

- Complete when Motorola Solutions and Customer project teams are identified and deployment

2.1.4.3 Data Collection and Planning Session

Motorola Solutions will conduct a remote working session with the customer System Administrators and agency user representatives to provide an overview of SmartConnect operation and collect provisioning data. This activity is performed via teleconference.

Motorola Solutions Responsibilities

- Conduct a remote, one to two hour, planning session with representatives of each agency using SmartConnect.
- Review SmartConnect functionality and configuration options.
- Document each agency's configuration, admin users, initial subscribers and users.

Customer Responsibilities

- Schedule planning session with representatives of each agency.
- Provide Administrator, User, Subscriber, and Group information for provisioning.

Completion Criteria

- Planning sessions completed.

2.1.4.4 Domain and Device Setup

The Radio Subscribers must be provisioned within the CommandCentral Cloud Platform using the Command Central Admin tool. Motorola Solutions will provision the Customer's current inventory of APX NEXT subscribers. The Customer will assume responsibility to provision all subsequently procured APX NEXT devices.

Motorola Solutions Responsibilities

- If a SmartConnect agency has not been previously established for the ASTRO system, use the CommandCentral Admin tool to establish the Customer Domain within the CommandCentral cloud platform. This activity will be initiated during the order process.
- Use the CommandCentral Admin tool to provision SmartConnect based on the information collected during the Data Collection and Planning Session activity:
  - Setup Command Central administration and user passwords.

- Provision radio subscriber devices (radio serial number and ASTRO Unit ID). All subscriber devices on an ASTRO system are provisioned by a single CC Admin agency account. This may be performed individually or by importing the device information from a .csv file.

Customer Responsibilities

- Identify System Administrator(s)
- Assure all System Administrators complete the CommandCentral Admin training.
- Use the CommandCentral Admin tool to provision all APX NEXT subscribers procured after the completion of the SmartConnect enablement project.

Completion Criteria

- All agencies, users and devices are provisioned.

2.1.4.5 SmartConnect Gateway Configuration

The SmartConnect Gateway enables the connection between the Customer's ASTRO system and the SmartConnect cloud services and broadband service. The SmartConnect Gateway must be configured to accept a connection from the ASTRO system's LMP proxy.

Motorola Solutions Responsibilities

- Enable SmartConnect Gateway service.
- Generate the passphrase for the LMPs using CCAdmin.

Customer Responsibilities

- None.

Completion Criteria

- SmartConnect Gateway connection enabled.

2.1.4.6 ASTRO Infrastructure Preparation

Operation of SmartConnect requires a minimum ASTRO infrastructure software version and specific hardware components. These elements are not included with SmartConnect and must be in place prior to SmartConnect deployment. SmartConnect requires the following ASTRO infrastructure version and equipment:

- ASTRO version: 7.17 or later.
- Internetworking Firewall hardware and software (shared component).
- Suitable Server (VMS01/VMS02 or VMS 07).

Motorola Solutions Responsibilities

- Review the current ASTRO system and document the availability and configuration of the components required for SmartConnect deployment.
- Identify any software upgrades or additional equipment required to support SmartConnect.

Customer Responsibilities

- Procure ASTRO infrastructure upgrades and equipment required for SmartConnect operation.

Completion Criteria

- Customers ASTRO infrastructure is operational with the required software version and equipment required for SmartConnect deployment.

2.1.4.7 ASTRO System Configuration

SmartConnect specific software components and network configurations must be added to the ASTRO System. Motorola Solutions will install and configure these items during the SmartConnect deployment.

Motorola Solutions Responsibilities

- Install LMR Multicast Proxy (LMP) VMs on the zone core servers. Enter CommandCentral Admin generated passphrase during the installation.
- Cable and configure the transport (core LAN switch, DMZ switch, DMZ firewall, internetworking firewall) using TNCT.
- Verify connectivity with SmartConnect Cloud Gateway via Internetworking Firewall.
- Configure NM with pseudo-site for Backup PTT using a UNC configlet for each Zone Controller and ATR in the target zone.
- Assess the number of Talk Groups and Calls to determine the required backhaul capacity. Provide backhaul capacity requirements to Customer admin.

Customer Responsibilities

- Coordinate and schedule ASTRO component software installation to minimize the impact on production operation.
- Provide dedicated internet connection for Internetworking Firewall. Assure that the network connection meets the following service level:
- The internet connection between ASTRO system (LMP) and the SmartConnect Gateway in the cloud requires a base bandwidth of 25Kbps plus a bandwidth of 20k bits per second per group call. *NOTE: If the SmartConnect Gateway is configured as "requested site" for a group in the ASTRO system, all calls on that group are routed to the SmartConnect Gateway independent whether radios have affiliated to the group or not in the broadband domain. The configuration as "requested site" ensures that the radio will be offered calls from scanned groups, but it also increases the load on the connection between the LMP and the SmartConnect Gateway.*
  - 1/1 Mbps symmetric Internet connection is required for 36 simultaneous calls (for release prior to 2019.2).
  - 5/5 Mbps symmetric Internet connection is required for 200 simultaneous calls.(for release 2019.2 and onwards).
  - Availability > 99.99%. A lower performance will decrease the SmartConnect feature reliability proportionality.
  - Packet loss less than 0.5%. A higher packet loss will lower the reliability and the audio quality.
  - Average delay introduced by the Internet Service Provider less than 20 ms.
  - Average jitter introduced on the Internet Service Provider is less than 10 ms.

Completion Criteria

- Customer ASTRO infrastructure is operational with the required software versions and configured to support SmartConnect operation.

2.1.4.8 Subscriber Provisioning

APX subscribers must be provisioned on the customer's ASTRO system prior to operation. Subscriber provisioning must include specific parameters to enable SmartConnect operation.

Motorola Solutions Responsibilities

- Provide SmartConnect provisioning parameters (FQDN for SmartConnect GW, ports).
- Provision one (1) APX subscriber to validate the parameters.
- Demonstrate the provisioning process and required parameters to customer System Administrator.

Customer Responsibilities

- Assure that all APX and APX NEXT subscriber firmware is updated to Release 20 or later.
- Assure that APX and APX NEXT subscribers have been previously provisioned on the ASTRO system.
- Assure that all APX NEXT subscribers have a current SmartProgramming application service subscription.
- Assure that APX NEXT subscribers' code plug configurations have been provisioned in RadioCentral and that the APX NEXT Subscribers have been programmed.
- Download and install the latest version of the RadioCentral programming client.
- Provision balance of APX NEXT subscribers for SmartConnect using the RadioCentral client.
- Provision balance of APX subscribers for SmartConnect using Radio Management or CPS software.
- Update the provisioning parameters of any existing subscribers that will utilize SmartConnect capability.

Completion Criteria

- All subscribers covered by a SmartConnect feature subscription are provisioned with SmartConnect parameters.

2.1.4.9 Operational Demonstration

After the solution deployment, Motorola Solutions will provide an operational demonstration to the customer project manager, system administrator, and end user representatives.

Motorola Solutions Responsibilities

- Provide the Operational Demonstration Script.
- Demonstrate SmartConnect operation..

Customer Responsibilities

- Participate in SmartConnect demonstration.

Completion Criteria

- Complete after successful demonstration of SmartConnect operation.

2.1.4.10 SmartConnect Training

SmartConnect Administrator and User training classes are available online. Access to online SmartConnect training is provided by Motorola Solutions Software Enterprise Learning Experience Portal (LXP). This subscription service provides continual access to Motorola's library of online learning content and allows users the benefit of learning at times convenient to them. Content is added and updated on a regular basis to keep information current. Online training enables Users to participate in training at their convenience.

The Customer's LXP Administrators use Panorama, a customer specific instance of the Learning Management System, to add/modify users, run reports, and add/modify groups, and define Learning Paths. Groups are a more granular segmentation of the LXP that are generally utilized to separate learners by function (i.e. dispatchers, call takers, patrol, firefighter). A Learning Path is a collection of courses that follow a logical order, and may or may not enforce linear progress.

Motorola Solutions Responsibilities

- Setup Panorama and add customer specified LXP administrators.
- Provide administrators access to learning services.motorolasolutions.com.

Customer Responsibilities

- Provide Motorola Solutions with names (first and last) and emails of Customer LXP administrators.
- Assure all System Administrators complete LXP Administrator training. The training covers:
  - Adding and maintaining Users.
  - Adding and maintaining Groups.
  - Assigning courses and Learning Paths.
  - Running reports.
  - Advise users of the availability of the LXP and SmartConnect training class.
  - Add/modify users, run reports and add/modify groups.

Completion Criteria

- Work is considered complete upon conclusion of Motorola Solutions provided LXP Administrator instruction.

2.1.4.11 Project Finalization and Handover to Support

Finalization is the process of confirming that all project activities have been completed and project documentation has been delivered. During this activity, Motorola Solutions will transition responsibility for SmartConnect from the Project Manager to the Motorola Solutions support team. The Customer's Project Manager will transition support to the System Administrator(s).

Motorola Solutions Responsibilities

- Verify project deliverables have been received by the Customer Project Manager.

- Confirm with Customer that SmartConnect is available for Customers beneficial use.
- Provide the SmartConnect Configuration Document.
- Conduct a teleconference introducing Customer to Motorola Solutions Support organization. The purpose of the teleconference is to review the SmartConnect support process and obtain contact information with the Customer's assigned system administrator(s) and the Motorola Solutions Support Team.
- Provide on-going support in accordance with the terms and conditions of the support agreement.

Customer Responsibilities

- Provide confirmation of receipt of project deliverables with the Motorola Solutions Project Manager.
- Participate in the support hand over teleconference. Assure that System Administrator(s) understand the support process and have the correct contact information.

Completion Criteria

- Project finalization is complete upon delivery of the final SmartConnect Configuration Document and the conclusion of the teleconference with Motorola Solutions Support organization.

2.1.5 SmartLocate with CommandCentral Aware Statement of Work

The Statement of Work defines the principal activities and responsibilities of Motorola Solutions and the Customer during SmartLocate deployment. The deployment process is a collaborative effort between Customer system administrators, subject matter experts, and the Motorola Solutions deployment team. Deployments involve the following steps:

Table 2-4: SmartLocate Set-up Steps

Step	Description
Project Initiation	Formal project kickoff and planning sessions
Data Collection & Planning	Aware overview, provisioning planning, and data collection
APX NEXT Provisioning	Configure APX NEXT subscribers for location reporting via LTE
Mapping Configuration	Configure connection to customer's ESRI/GIS system
Agency, User, and Device Setup	Configure agency, users, and devices on Aware cloud platform
Operational Demonstration	Demonstrate SmartLocate with Aware operation
Training	SmartLocate with Aware operational and administrator training
Project Finalization	Delivery of as-built documentation and hand over to support

These project steps are logical groupings of related activities required to complete the project. Each step includes tasks and deliverables that both Motorola Solutions and the Customer are responsible to complete. These are described in detail within the Statement of Work.

Motorola Solutions' project manager will use the Statement of Work to guide the deployment process and coordinate the activities of all Motorola Solutions resources and teams. The project manager will also work closely with the Customer's project manager to clearly communicate the required deployment activities and schedule tasks involving Customer resources.

2.1.5.1 Project Documentation

The following documents are delivered during the deployment process. Some are standard product documentation and others are project specific and are produced during the project.

Product Documentation

CommandCentral System Administration Guide. The Administration Guide includes information about the CommandCentral Admin tool, User provisioning, and other system administration tasks.

Project Documentation

SmartLocate with Aware Configuration Document. Describes the SmartLocate with Aware configuration including APX NEXT provisioning parameters, and CommandCentral Aware configuration. It is created during the project, is used to configure and validate application and network configurations, and finalized to serve as project as-built documentation. Provided to both the Customer and the Motorola Solutions Support Team.

Operational Demonstration Script. The Operational Demonstration Script provides a customer-specific procedure for validating system configuration and operation. It references the customer specifics detailed in the Configuration Document.

2.1.5.2 Project Initiation

Project initiation occurs after procurement of SmartLocate Enablement and notice to proceed is received. During this phase the Motorola Solutions and Customer project managers are assigned, assemble their teams, and establish a working relationship. The managers jointly review the project plan, deliverables, and schedule. Each manager coordinates preparatory tasks that serve as a foundation for the specific SmartLocate with CommandCentral Aware deployment activities.

Motorola Solutions Responsibilities

- Schedule a kick-off call between Customer and Motorola Solutions project managers.
- Establish communications plan.
- Review project work plan, schedule, and resources.
- Provide standard product documentation.
  - CommandCentral System Administration Guide.
  - CommandCentral Network Connectivity Guide.
  - User Guide.

Customer Responsibilities

- Customer project manager coordinates with agency(s) and identifies the subject matter experts, system administrators, and network administrators that will participate in the project and complete Customer tasks.
- Review the Solution Description and prerequisites with customer project team. Assure that all required components are in place or initiate their procurement.
- Schedule agency personnel time to participate in the deployment process.

Completion Criteria

- Complete when Motorola Solutions and Customer project teams are identified and deployment tasks are assigned and scheduled.

2.1.5.3 ASTRO Infrastructure Preparation

SmartLocate does not utilize the ASTRO infrastructure so there are no infrastructure software version, ASTRO hardware components, or data capacity requirements.

It is possible to obtain the location of APX subscribers via the ASTRO system and display the location on the Aware client. This type of operation requires additional equipment, software and services including IMW, Cloud Connect, IMW Connector, and an ASTRO data capacity study. These elements are not included with SmartLocate Enablement.

Motorola Solutions Responsibilities

- This SmartLocate with CommandCentral Aware project does not include any services related to the implementation of Aware functionality other than APX NEXT location over broadband.

Customer Responsibilities

- Determine if any additional Aware functionality is desired and work with Motorola Solutions Sales representative to define the scope and obtain a proposal.

Completion Criteria

- Information only.

2.1.5.4 Data Collection and Planning Session

Motorola Solutions will conduct a remote working session with the customer System Administrators and agency user representatives to provide an overview of Aware operation, collect provisioning data, plan the Aware group and agency configurations. This activity is performed via teleconference.

Motorola Solutions Responsibilities

- Conduct a remote, one to two hour, planning session with representatives of each agency using SmartLocate.
- Review CommandCentral Aware functionality and configuration options.
- Document each agency's configuration, admin users, initial subscribers and users.

Customer Responsibilities

- Schedule planning session with representatives of each agency.
- Provide Administrator, User, Subscriber, and Group information for provisioning.

Completion Criteria

- Planning sessions completed.

2.1.5.5 APX NEXT Provisioning

APX NEXT subscribers must be configured to report their GPS location via a LTE network. Subscriber locations are then sent via the broadband network to CommandCentral Aware. Customers are able to monitor the location of APX NEXT devices on the CommandCentral Aware client.

Motorola Solutions Responsibilities

- Verify that location updates are received from the Customer's provisioned APX NEXT subscribers.

Customer Responsibilities

- Assure that APX NEXT subscribers have been provisioned on the ASTRO system.
- Assure that the APX NEXT subscribers are programmed. Motorola Solutions includes Initial Programming support services with the first APX NEXT order.
- Update the APX NEXT Codeplugs with the following SmartLocation parameters.
  - Location Enable – On.
  - Location Reporting - Broadband or Broadband Preferred (if Aware Mapping is part of the solution).

Completion Criteria

- All APX next subscribers configured to report location.

2.1.5.6 CommandCentral Aware Geospatial Mapping Configuration

CommandCentral Aware can display Unit location data on a generic base map or on the customer's ESRI map. A single base map layer is included with SmartLocate with Aware. Aware supports multiple map layers which may be added separately.

Motorola Solutions Responsibilities

- Install and configure the connection to the Customer mapping system, (i.e. ESRI online, ESRI server, or static map layers).
- Test mapping layers and links in accordance with the system Design Document.

Customer Responsibilities

- Provide URL and access credentials for customer's ESRI/GIS system.
- Specify and publish the desired GIS map for use with SmartLocate with Aware.

Completion Criteria

- CommandCentral Aware browser client is able to display the Customer's ESRI map.

2.1.5.7 CommandCentral Aware Agency, User, and Device Setup

The Customer's Agency, Users, and Radio Subscribers must be provisioned within the CommandCentral Cloud Platform using the CommandCentral Admin tool. The provisioning process allows the Agency to define the specific capabilities and permissions of each user. Motorola Solutions will provision the Customer's current inventory of APX NEXT subscribers. The Customer will assume responsibility to provision all subsequently procured APX NEXT devices.

Motorola Solutions Responsibilities

- Use the CommandCentral Admin tool to establish the Customer and Customer's agency(s) within the CommandCentral cloud platform. This activity will be initiated during the order process.
- Provision CommandCentral Aware Users, Subscribers, Groups, and layers based on the information collected during the Data Collection and Planning Session activity.
- Use the CommandCentral Admin tool to provision CommandCentral Aware based on the information collected during the Data Collection and Planning Session activity:
  - Setup Command Central administration and user passwords.
  - Provision agency's Users (officers).
  - Provision permissions per User.
  - Provision agency's radio subscriber devices.
  - Provision User to radio subscriber.

Customer Responsibilities

- Identify System Administrator(s).
- Assure all System Administrators complete the CommandCentral Admin training.
- Use the CommandCentral Admin tool to provision all APX NEXT subscribers procured after the completion of the SmartLocate enablement project.

Completion Criteria

- All agencies, users and APX NEXT subscribers are provisioned.

2.1.5.8 CommandCentral Aware Client

CommandCentral Aware is a SaaS application that is accessed via a web browser. The Client in this context consists of a workstation and web browser.

Motorola Solutions Responsibilities

- Provide URL and System Administrator credentials for accessing the Aware application.

Customer Responsibilities

- Provide client workstations, web browsers, and network connectivity suitable for accessing the Aware application.

Completion Criteria

- Aware access is available from customer client(s).

2.1.5.9 Operational Demonstration

After the solution deployment, Motorola Solutions will provide an operational demonstration to the customer project manager, system administrator, and end user representatives. The objective of the functional demonstration is to validate Customer access to CommandCentral Aware via browser client and demonstrate the map display and location updates. This activity is performed via teleconference.

Motorola Solutions Responsibilities

- Facilitate a teleconference to perform an operational demonstration of the SmartLocate and Aware Mapping solution.
- Demonstrate the APX NEXT subscriber location is displayed on the CommandCentral Aware web client.
- Correct any configuration issues impacting access to Aware features, map display, or location updates.

Customer Responsibilities

- Review and agree to the scope of the demonstration script.
- Participate in SmartLocate with CommandCentral Aware demonstration.
- Witness the operational demonstration and acknowledge its completion.
- Provide Motorola Solutions with any requests for feature enhancements.

Completion Criteria

- Complete after successful demonstration of SmartLocate with CommandCentral Aware operation.

2.1.5.10 CommandCentral Aware Training

CommandCentral SmartLocate Administrator and User training classes are available online. Access to online CommandCentral Aware training is provided by Motorola Solutions Software Enterprise Learning Experience Portal (LXP) https://learning.motorolasolutions.com. This subscription service provides continual access to Motorola's library of online learning content and allows users the benefit of learning at times convenient to them. Content is added and updated on a regular basis to keep information current. Online training enables Users to participate in training at their convenience.

- PSA4056 - CommandCentral Aware Map View Basics.
- PSA0015 - CommandCentral Aware End User Training.
- PSA4122 - CommandCentral Aware Cloud - Customer Administration.

Motorola Solutions Responsibilities

- Provide administrators access to the Learning Experience Portal (LXP).

Customer Responsibilities

- Provide Motorola Solutions with names (first and last) and emails of Customer LXP administrators.
- Assure all System Administrators complete LXP Administrator training. The training covers:
  - Adding and maintaining Users.
  - Adding and maintaining Groups.
  - Assigning courses and Learning Paths.
  - Running reports.
- Advise users of the availability of the LXP and SmartLocate with CommandCentral Aware class.
- Add/modify users, run reports and add/modify groups.

Completion Criteria

- Work is considered complete upon conclusion of Motorola Solutions provided LXP Administrator instruction.

2.1.5.11 Project Finalization and Handover to Support

Finalization is the process of confirming that all project activities have been completed and project documentation has been delivered. During this activity Motorola Solutions transitions responsibility for SmartLocate with CommandCentral Aware from the Project Manager to the Motorola Solutions support team. The Customer's Project Manager transitions support to the System Administrator(s).

Motorola Solutions Responsibilities

- Verify project deliverables have been received by the Customer Project Manager.
- Confirm with Customer that SmartLocate with Aware is available for Customer beneficial use.
- Provide the SmartLocate with Aware Configuration Document.
- Conduct a teleconference introducing Customer to Motorola Solutions Support organization. The purpose of the teleconference is to review the support process and obtain contact information with the Customer's assigned system administrator(s) and the Motorola Solutions Support Team.
- Provide on-going support in accordance with the terms and conditions of the support agreement.

Customer Responsibilities

- Provide confirmation of receipt of project deliverables with the Motorola Solutions Project Manager.
- Participate in the support handover teleconference. Assure that System Administrator(s) understand the support process and have the correct contact information.

Completion Criteria

- Project finalization is complete upon conclusion of the teleconference with Motorola Solutions Support organization.

2.1.6 SmartMapping Statement of Work

The Statement of Work defines the principal activities and responsibilities of Motorola Solutions and the Customer during SmartMapping deployment. The deployment process is a collaborative effort between Customer system administrators, subject matter experts, and the Motorola Solutions deployment team. Deployments involve the following steps:

Table 2-5: SmartMapping Set-up Steps

Step	Description
Project Initiation	Formal project kickoff and planning sessions.
Data Collection & Planning	SmartMapping overview, provisioning planning, and data collection.
SmartMapping Provisioning	Provision SmartMapping subscribers and groups.
APX NEXT Programming	Program APX NEXT subscribers for SmartMapping operation.

Step	Description
Operational Demonstration	Demonstrate SmartMapping with Aware operation.
Training	SmartMapping User and Administrator training.
Project Finalization	Delivery of as-built documentation and hand over to support.

These project steps are logical groupings of related activities required to complete the project. Each step includes tasks and deliverables that both Motorola Solutions and the Customer are responsible to complete. These are described in detail within the Statement of Work.

Motorola Solutions' project manager will use the Statement of Work to guide the deployment process and coordinate the activities of all Motorola Solutions resources and teams. The project manager will also work closely with the Customer's project manager to clearly communicate the required deployment activities and schedule tasks involving Customer resources.

2.1.6.1 Project Documentation

The following documents are delivered during the deployment process. Some are standard product documentation and others are project specific and are produced during the project.

Product Documentation

CommandCentral System Administration Guide. The Administration Guide includes information about the CommandCentral Admin tool, User provisioning, and other system administration tasks.

Project Documentation

SmartMapping Configuration Document. Describes the SmartMapping configuration including APX NEXT provisioning parameters, and SmartMapping configuration. It is created during the project, is used to configure and validate application and network configurations, and finalized to serve as project as-built documentation. Provided to both the Customer and the Motorola Solutions Support Team.

Operational Demonstration Script. The Operational Demonstration Script provides a customer-specific procedure for validating system configuration and operation. It references the customer specifics detailed in the Configuration Document.

2.1.6.2 Project Initiation

Project initiation occurs after procurement of SmartMapping Enablement and notice to proceed is received. During this phase the Motorola Solutions and Customer project managers are assigned, assemble their teams, and establish a working relationship. The managers jointly review the project plan, deliverables, and schedule. Each manager coordinates preparatory tasks that serve as a foundation for the specific SmartMapping with CommandCentral Aware deployment activities.

Motorola Solutions Responsibilities

- Schedule a kick-off call between Customer and Motorola Solutions project managers.
- Establish communications plan.
- Review project work plan, schedule, and resources.
- Provide standard product documentation.

- CommandCentral System Administration Guide.
- User Guide.

Customer Responsibilities

- Customer project manager coordinates with agency(s) and identifies the subject matter experts, system administrators, and network administrators that will participate in the project and complete Customer tasks.
- Review the Solution Description and prerequisites with the customer's project team. Assure that all required components are in place or initiate their procurement.
- Schedule agency personnel time to participate in the deployment process.

Completion Criteria

- Complete when Motorola Solutions and Customer project teams are identified and deployment tasks are assigned and scheduled.

2.1.6.3 ASTRO 25 Infrastructure Preparation

SmartMapping does not utilize the ASTRO 25 infrastructure so there are no infrastructure software version dependencies, ASTRO 25 hardware components, or data capacity requirements.

It is possible to obtain the location of APX subscribers via the ASTRO 25 system and display the location on SmartMapping clients and the Aware client. This type of operation requires additional equipment, software and services including IMW, Cloud Connect, IMW Connector, and an ASTRO 25 data capacity study. These elements are not included with SmartMapping Enablement.

Motorola Solutions Responsibilities

- No deliverables.

Customer Responsibilities

- Determine if any additional CommandCentral Aware functionality is desired and work with Motorola Solutions Sales representative to define the scope and obtain a proposal.

Completion Criteria

- Information only.

2.1.6.4 Data Collection and Planning Session

The Motorola Solutions SA will conduct a remote working session with the customer System Administrators and agency user representatives to provide an overview of SmartMapping operation, collect provisioning data, plan the SmartMapping group and agency configurations. This activity is performed via teleconference.

Motorola Solutions Responsibilities

- Conduct a remote, one to two hour, planning session with representatives of each agency using SmartMapping.
- Review SmartMapping functionality and configuration options.
- Document each agency's configuration, admin users, initial subscribers and users.

- Document the SmartMapping agency group names, display icon (pick from list), member device IDs, and Unit Alias (map display name).
- Document the SmartMapping groups visible for each SmartMapping user account.

Customer Responsibilities

- Schedule planning session with representatives of each agency.
- Provide Administrator, User, Subscriber, and Group information for provisioning.

Completion Criteria

- Planning sessions completed.

2.1.6.5 SmartMapping Provisioning

SmartMapping users, subscribers, and groups must be provisioned within CommandCentral Admin. A Motorola Solutions SA will provision SmartMapping based on the information gathered during the Data Collection and Planning sessions. After provisioning the SA will review the configuration with the customer System Administrators via teleconference.

Motorola Solutions Responsibilities

- Provision all of the Customer's APX NEXT devices covered by a SmartMapping subscription.
- Provision SmartMapping Users.
- Provision SmartMapping Groups.
- Assign each subscriber's display groups. (Total displayed devices should not exceed 500 devices. This is intended to maximize performance).
- Review CommandCentral SmartMapping provisioning with System Administrator.

Customer Responsibilities

- Review SmartMapping provisioning.
- Customer's System Admin is responsible for maintaining the SmartMapping provisioning in CommandCentral Admin and provisioning any APX NEXT subscribers or SmartMapping subscriptions procured after the initial enablement project.

Completion Criteria

- SmartMapping provisioning completed.

2.1.6.6 APX NEXT Programming

APX NEXT subscribers must be updated with the latest subscriber firmware and have SmartMapping enabled.

Motorola Solutions Responsibilities

- No responsibilities.

Customer Responsibilities

- Assure that APX NEXT subscribers have been provisioned on the ASTRO 25 system.

- Assure that a minimum-tiered DMS Essential contract is in place for each APX NEXT subscriber.
- Download and install the latest version of the RadioCentral programming client.
- Update the APX NEXT firmware to version 2020.2 or later.
- Assure that APX NEXT subscribers' code plug configurations have been provisioned in RadioCentral and that the configuration changes have been pushed to the APX NEXT subscribers.
- Provision all APX NEXT subscribers for SmartMapping using the RadioCentral client.
  - Radio wide features / location.
    - Location Enable – On.
    - Mapping Mode = SmartMapping.

Completion Criteria

- All APX NEXT subscribers operational with suitable firmware version and SmartMapping enabled.

2.1.6.7 Operational Demonstration

After the solution deployment, Motorola Solutions will provide an operational demonstration to the customer project manager, system administrator, and end user representatives. The objective of the functional demonstration is to validate and demonstrate the SmartMapping display on APX NEXT devices. This activity is performed via teleconference.

Motorola Solutions Responsibilities

- Create a functional demonstration script.
- Conduct the demonstrations remotely using a web meeting.
- Demonstrate that the location of devices in the specified groups are displayed on the APX NEXT SmartMapping application.
- Create a summary report documenting the activities of the functional demonstration and any corrective actions taken by Customer or Motorola Solutions during the demonstration.

Customer Responsibilities

- Review and agree to the scope of the demonstration script.
- Participate in a SmartMapping demonstration.
- Conduct the SmartMapping demonstration with remote support from Motorola Solutions. This demonstration must be performed locally with at least one APX NEXT device. Ideally, devices from all defined SmartMapping groups should be active and reporting their location during the demonstration.
- Witness the operational demonstration and acknowledge its completion.
- Provide Motorola Solutions with any requests for feature enhancements.

Completion Criteria

- Complete after successful demonstration of SmartMapping operation.

2.1.6.8 SmartMapping Training

SmartMapping Administrator and User training classes are available online. Access to online SmartMapping training is provided by Motorola Solutions Software Enterprise Learning Experience Portal (LXP). This subscription service provides continual access to Motorola Solutions' library of online learning content and allows users the benefit of learning at times convenient to them. Content is added and updated on a regular basis to keep information current. Online training enables users to participate in training at their convenience.

The Customer's LXP Administrators use Panorama, a customer specific instance of the Learning Management System, to add/modify users, run reports, and add/modify groups, and define Learning Paths. Groups are a more granular segmentation of the LXP that are generally used to separate learners by function (i.e. dispatchers, call takers, patrol, firefighter). A Learning Path is a collection of courses that follow a logical order, and may or may not enforce linear progress.

Motorola Solutions Responsibilities

- Setup Panorama and add customer specified LXP administrators.
- Provide administrators access to learning services.motorolasolutions.com.

Customer Responsibilities

- Provide Motorola Solutions with names (first and last) and emails of Customer LXP administrators.
- Assure all System Administrators complete LXP Administrator training. The training covers:
  - Adding and maintaining Users.
  - Adding and maintaining Groups.
  - Assigning courses and Learning Paths.
  - Running reports.
- Advise users of the availability of the LXP and SmartMapping with CommandCentral Aware class.
- Add/modify users, run reports and add/modify groups.

Completion Criteria

- Work is considered complete upon conclusion of Motorola Solutions provided LXP Administrator instruction.

2.1.6.9 Project Finalization and Handover to Support

Finalization is the process of confirming that all project activities have been completed and project documentation has been delivered. During this activity Motorola Solutions transitions responsibility for SmartMapping from the Project Manager to the Motorola Solutions support team. The Customer's Project Manager transitions support to the System Administrator(s).

Motorola Solutions Responsibilities

- Verify project deliverables have been received by the Customer Project Manager.
- Confirm with Customer that SmartMapping is available for Customer beneficial use.
- Provide the SmartMapping Configuration Document.

- Conduct a teleconference introducing Customer to Motorola Solutions Support organization. The purpose of the teleconference is to review the support process and obtain contact information with the Customer's assigned system administrator(s) and the Motorola Solutions Support Team.
- Provide on-going support in accordance with the terms and conditions of the support agreement.

Customer Responsibilities

- Provide confirmation of receipt of project deliverables with the Motorola Solutions Project Manager.
- Participate in the support handover teleconference. Assure that System Administrator(s) understand the support process and have the correct contact information.

Completion Criteria

- Project finalization is complete upon conclusion of the teleconference with Motorola Solutions Support organization.

2.2 PremierOne CAD

2.2.1 Introduction

In accordance with the terms and conditions of the Agreement, this Statement of Work ("SOW") defines the principal activities and responsibilities of all parties for the delivery of the Motorola Solutions ("Motorola Solutions") solution as presented in this offer to the St Johns County, Florida Sheriff's Office (hereinafter referred to as "Customer"). When assigning responsibilities, the phrase "Motorola Solutions" includes our subcontractors and third-party partners. The Customer has requested to be added as an agency to the St Johns Fire Department (hereinafter referred to as "System Owner"). The Customer shall obtain commitment from System Owner that Customer is permitted to connect to and utilize the System Owner's PremierOne application, including provisioning and system administration (subject to the System Owner's restrictions).

Deviations and changes to this SOW are subject to mutual agreement between Motorola Solutions and the Customer and will be addressed in accordance with the change provisions of the Agreement.

Unless specifically stated, Motorola Solutions work be performed remotely. Customer will provide Motorola Solutions resources with unrestricted direct network access to enable Motorola Solutions to fulfill its delivery obligations.

Motorola Solutions, Customer, and System Owner will work to complete their respective responsibilities in accordance with the mutually agreed upon governing Project Schedule. Any changes to the governing Project Schedule will be mutually agreed upon via the change provision of the Agreement.

The number and type of software or subscription licenses, products, or services provided by Motorola Solutions or its subcontractors are specifically listed in the Agreement and any reference within this document as well as subcontractors' SOWs (if applicable) does not imply or convey a software or subscription license or service not explicitly listed in the Agreement.

2.2.2 Project Award

Project Initiation and Planning will begin following execution of the Agreement between Motorola Solutions and the Customer.

The following project management terms are used in this document. Since these terms may be used differently in other settings, these definitions are provided for clarity.

Project Schedule means the schedule providing dates and timeframes for completion of tasks and deliverables during the course of the project. The Project Schedule is subject to change at the mutual agreement of Motorola Solutions and the Customer.

Project Management Plan is composed of the Communications Management Plan, Risk Management Plan, and Change Management Plan that provide the criteria for managing those tasks within the project.

2.2.3 Contract Administration and Project Initiation

After the contract is dually executed, the project is set up in the Motorola Solutions' information and management systems, project resources are assigned and Project Planning activities commence. Motorola Solutions and Customer will work to complete their respective responsibilities in accordance

with the mutually agreed upon and executed Project Schedule. Any changes in the Project Schedule will be mutually agreed upon via Change Order to avert delay.

2.2.3.1 Completion and Acceptance Criteria

Following Cutover to live operations (beneficial use), the project is complete. Motorola Solutions and Customer acknowledge the completion milestone and the implementation project is formally closed.

The system will transition to the support phase of the contract per the terms and conditions of the Maintenance and Support Agreement.

Customer will provide Motorola Solutions written notification that it does not accept the completion of Motorola Solutions responsibilities or rejects a Motorola Solutions service deliverable within five (5) business days of completion or receipt of a deliverable.

The Service Completion will be acknowledged in accordance with the terms of Master Customer Agreement and the Service Completion Date will be memorialized by Motorola Solutions and Customer. Software System Completion will be in accordance with the terms of the Software Products Addendum unless otherwise stated in this Statement of Work.

2.2.4 Project Roles and Responsibilities Overview

2.2.4.1 Motorola Solutions Project Roles and Responsibilities

A Motorola Solutions team, made up of specialized personnel, will be appointed to the project under the direction of the Motorola Solutions Project Manager. Team members will be multi-disciplinary and may fill more than one role. Team members will be engaged in different phases of the project as necessary.

In order to maximize efficiencies Motorola Solutions' project team will provide services remotely via teleconference, web-conference or other remote method in fulling its commitments as outlined in this Statement of Work. Motorola Solutions project team resources will be on site at the Customer location when fulfilling commitments that are crucial to project success as noted in this Statement of Work.

The personnel role descriptions noted below provide an overview of typical project team members. There may be other personnel engaged in the project under the direction of the Project Manager. The following provided descriptions of the primary roles engaged in the delivery of the project.

Motorola Solutions' project management approach has been developed and refined based on lessons learned in the execution of hundreds of system implementations. Using experienced and dedicated people, industry-leading processes, and integrated software tools for effective project execution and control, we have developed and refined practices that support the design, production, and testing required to deliver a high quality, feature-rich system.

Project Manager

- A Motorola Solutions Project Manager will be assigned as the principal business representative and point of contact for the organization. The Project Manager's responsibilities include:
- Manage the Motorola Solutions responsibilities related to the delivery of the project.
- Maintain the project schedule and manage the assigned Motorola Solutions personnel and applicable subcontractor/supplier resources.
- Manage the Change Order process per the Agreement.

- Maintain project communications with the Customer.
- Identify and manage project risks.
- Collaborative coordination of Customer resources to minimize and avoid project delays.
- Measure, evaluate, and report the project status against the Project Schedule.
- Conduct remote status meetings on a mutually agreed basis to discuss project status.
- Prepare and submit a monthly status report that identifies the activities of the previous month, as well as activities planned for the current month, including an updated Project Schedule and action item log.
- Provide timely responses to issues related to project progress.

Application Specialist

The Motorola Solutions Application Specialist will work with the Customer project team with system provisioning. The Application Specialist's responsibilities will include:

- Provide consultation services to the Customer regarding the provisioning and operation of the Motorola Solutions system.
- Provide provisioning training to the Customer to provide the knowledge to setup and maintain the system.
- Complete the provisioning ownership handoff to the Customer.
- Complete the project-defined milestones and tasks as defined in this SOW.
- Provide guidance on the Customer's operational Change Management needs relative to the use of the Motorola Solutions system.
- Provide product training as defined by this SOW and described in the Training Plan.
- Provide on-site cutover support.

Solutions Architect

The Solutions Architect is responsible for the delivery of the technical and equipment elements of the solution. They confirm the delivered technical elements meet contracted requirements. They are engaged throughout the duration of the delivery.

Customer Success Advocate

A Customer Success Advocate will be assigned to the Customer post Go Live event. By being the Customer's trusted advisor, the Customer Success Advocate' responsibilities include:

- Assist the Customer with maximizing the use of their Motorola Solutions software and service investment.
- Actively manage, escalate, and log issues with Support, Product Management, and Sales.
- Provide ongoing customer communication about progress, timelines, and next steps.

Customer Support Services Team

The Customer Support Services team will provide ongoing support following commencement of beneficial use of the Customer's System(s) as defined in Customer Support Plan.

2.2.4.2 Customer/System Owner Project Roles and Responsibilities Overview

The success of the project is dependent on early assignment of key Customer resources. It is critical these resources are empowered to make provisioning decisions based on the Customer's operational and administration needs. The Customer project team should be engaged from project initiation through beneficial use of the system. The continued involvement in the project and use of the system will convey the required knowledge to maintain the system post completion of the project. In some cases, one person may fill multiple project roles. The project team must be committed to participate in activities for a successful implementation. The Customer shall engage the System Owner where required to complete tasks and activities.

Project Manager

The Project Manager will act as the primary Customer point of contact for the duration of the project. In the event the project involves multiple agencies, Motorola Solutions will work exclusively with a single Customer assigned Project Manager (the primary Project Manager). This includes the management of any third party vendors that are Customer Subcontractors. The Project Manager's responsibilities include:

- Communicate and coordinate with other project participants.
- Manage the Customer project team including timely facilitation of efforts, tasks, and activities.
- Maintain project communications with the Motorola Solutions Project Manager.
- Identify the efforts required of Customer staff to meet the task requirements and milestones in this SOW and Project Schedule.
- Consolidate all project-related questions and queries from Customer staff to present to the Motorola Solutions Project Manager.
- Review the Project Schedule with the Motorola Solutions Project Manager and finalize the detailed tasks, task dates, and responsibilities.
- Measure and evaluate progress against the Project Schedule.
- Monitor the project to ensure resources are available as scheduled.
- Attend status meetings.
- Provide timely responses to issues related to project progress.
- Liaise and coordinate with other agencies, Customer vendors, contractors, and common carriers.
- Review and administer change control procedures, hardware and software certification, and all related project tasks required to maintain the Project Schedule.
- Ensure Customer vendors' adherence to overall Project Schedule and Project Plan.
- Assign one or more personnel who will work with Motorola Solutions staff as needed for the duration of the project, including at least one Application Administrator for PremierOne and one or more representative(s) from the IT department.
- Identify the resource with authority to formally acknowledge and approve Change Orders, approval letter(s), and milestone recognition certificates as well as approve and release payments in a timely manner.
- Provide building access to Motorola Solutions personnel to all Customer facilities where system equipment is to be installed during the project. Temporary identification cards are to be issued to Motorola Solutions personnel if required for access to facilities.

- Ensure remote network connectivity and access to Motorola Solutions resources.
- As applicable to this project, assume responsibility for all fees for licenses and inspections and for any delays associated with inspections due to required permits.
- Provide reasonable care to prevent equipment exposure to contaminants that cause damage to the equipment or interruption of service.
- Ensure a safe work environment for Motorola Solutions personnel.
- Provide signatures of Motorola Solutions-provided milestone certifications and Change Orders within five (5) business days of receipt.

Transformation Lead

The Transformation Lead, who may or may not be your Project Manager, must be able to holistically represent your organization and be able to work cross functionally between Motorola Solutions, your organization, and all stakeholders involved in the delivery of your new system. The Transformation Lead must be empowered to acknowledge the resource and time commitments required of your organization and authorize Motorola Solutions to proceed with scheduling the Project Kickoff event.

System Administrator

The System Owner will be responsible for all System Administration responsibilities and may provide training and assign responsibilities to the Customer to complete Customer required administration responsibilities. Likewise, SSRS reports and dashboards will be provided by the System Owner, unless the Customer is granted access and training by the System Owner to perform those tasks.

IT Personnel

IT personnel provide required information related to LAN, WAN, wireless networks, server, and client infrastructure. They must also be familiar with connectivity to internal, external, and third party systems to which the Motorola Solutions system will interface.

CAD Application Administrator

The CAD Administrator manages the Customer-owned CAD provisioning maintenance as defined in Appendix A - PremierOne CAD File Build - Customer Code Tables to ensure the system operates successfully. The CAD Administrator's involvement will start at the Business Process Review (BPR) stage of the project. They will attend Provisioning and Train the Trainer Training and remain engaged throughout the project to ensure they are able to maintain the CAD provisioning post Customer Provisioning handoff. The CAD Application Administrator's responsibilities include:

- Participate in overall delivery and training activities to understand the software, interfaces, and functionality of the system.
- Participate with the SMEs during the BPR, provisioning process, and training.
- Authorize global provisioning choices and decisions, and be the point(s) of contact for reporting and verifying problems and maintaining provisioning.
- Obtain inputs from other user agency stakeholders related to business processes and provisioning.

GIS Analyst

The System Owner will make any and all geofile modifications necessary to accommodate the service boundaries required by Customer. Subsequently, the Customer will request the System Owner to make

all the geofile data and apply all regular updates to the CAD system. No GIS services are included in Motorola Solutions' proposal. This will include but is not limited to the following standard responsibilities:

- Provide GIS data in the correct schema.
- Develop, maintain, and update GIS data.
- Support of the GIS elements used in the system (Server, CAD consoles, etc.)

Subject Matter Experts

The Subject Matter Experts (SME or Super Users) are the core group of users involved with the Business Process Review (BPR) and analysis, the provisioning process, including making global provisioning choices and decisions, and training. These members should be experienced users in the working area(s) they represent, i.e. dispatch, patrol, etc., and should be empowered to make decisions related to provisioning elements, workflows, screen layouts, etc.

Training Representative

Training representatives will be the point of contact for the Motorola Solutions Application Specialist when policy and procedural questions arise. They will act as course facilitators and are the Customer's educational monitors.

Additional Resources

Additional resources, such as trainers and database administrators may also be required.

User Agency Stakeholders

User Agency Stakeholders, if the system is deployed in a multi-agency environment, are those resources representing agencies outside of the Customer's agency. These resources will provide provisioning inputs to the SMEs if operations for these agencies differ from that of the Customer agency.

2.2.4.3 General Customer Responsibilities

In addition to the Customer Responsibilities stated elsewhere in this SOW, the Customer is responsible for:

- All Customer-provided equipment including hardware and third party software necessary for delivery of the System not specifically listed as a Motorola Solutions deliverable. This will include end user workstations, network equipment, telephone, or TDD equipment and the like.
- Configuration, maintenance, testing, and supporting the third-party systems the Customer operates which will be interfaced to as part of this project. The Customer is responsible for providing Application Programming Interface (API) documentation to those systems that document the integration process for the level of interface integration defined by Motorola Solutions.
- Initiate, coordinate, and facilitate communication between Motorola Solutions and Customer's third-party vendors as required to enable Motorola Solutions to perform its duties.
- Active participation of Customer Subject Matter Experts (SME's) in project delivery meetings and working sessions during the course of the project. Customer SME's will possess requisite knowledge of Customer operations and legacy system(s) and possess skills and abilities to operate and manage the system.

- The provisioning of Customer Code Tables and GIS data as requested by Motorola Solutions. This information must be provided in a timely manner in accordance with the Project Schedule.
- Electronic versions of any documentation associated with the business processes identified.
- Providing a facility with the required computer and audio-visual equipment for training and work sessions as defined in the Training Plan.
- Ability to participate in remote project meeting sessions using Google Meet.

2.2.5 Project Planning

A clear understanding of the needs and expectations of both Motorola Solutions and the Customer are critical to fostering a collaborative environment of trust and mutual respect. Project Planning requires the gathering of project specific information that is required to set clear project expectations and guidelines, create the Project Management Plan, Project schedule and set the foundation for a successful implementation.

2.2.5.1 Project Planning Session - Teleconference/Web Meeting

A Project Planning Session teleconference will be scheduled after the Agreement has been executed between the assigned Motorola Solutions and Customer Project Managers. The agenda will include:

- Review the Agreement documents.
- A summary review of the contracted applications, query(ies) and interface(s), and Bill of materials.
- Review project delivery requirements as described in this SOW.
- Discuss which tasks will be conducted by on-site Motorola Solutions resources as well as the activities when the Motorola Solutions Project Manager will be on-site.
- Discuss Customer involvement in provisioning and data gathering to confirm understanding of the scope and time commitments required.
- Review the initial Project Schedule and incorporate Customer feedback resulting in the delivery Project Schedule. The Project Schedule will be maintained by Motorola Solutions and updated through mutual collaboration. Schedule updates that impact milestones will be Motorola Solutions addressed via the Change Order provision of the Agreement.
- Develop and finalize the Project Management Plan.
- CJIS background investigations and fingerprint requirements for Motorola Solutions employees and/or contractors. Required fingerprints will be submitted on Motorola Solutions-provided FBI FD-258 Fingerprint cards.
- Review Virtual Desktop (VD) and Learning Management System (LMS) role in the delivery and provide Customer User Name and Access Information.
- Discuss Motorola Solutions remote access requirements (24-hour access to a secured two-way Internet connection to the Motorola Solutions system firewalls for the purposes of deployment, maintenance, and monitoring).
- Discuss Customer obligation to manage change among the stakeholder and user communities.
- Review the Business Process Review Agency Pre-Kick Off Survey. The Business Process Review Agency Pre-Kick Off Survey is a Google survey sent to the Customer to collect Agency-specific information such as dispatch logistics, communication center information, operational

process, and workflow. The information in the survey is used to prepare for the Business Process Review.

- Review project completion criteria and the process for transitioning to support.

Completing the Business Process Review Agency Pre-Kick Off Survey is a critical Project Task. Delayed, incomplete, or inaccurate information may have a significant impact on the Project Schedule.

Motorola Solutions Responsibilities

- Make initial contact with the Customer Project Manager and schedule the Project Planning Session teleconference.
- Review Motorola Solutions' delivery approach and its reliance on Customer provided remote access.
- Document the mutually agreed upon Project Kickoff Meeting Agenda.
- Request user information required to establish Customer in the Motorola Solutions Learning Management System ("LMS").

Customer Responsibilities

- Schedule the availability of the Transformation Lead to meet with Motorola Solutions.
- Ensure Customer GIS Administrator reviews the PremierOne GIS build requirements.
- If requested, provide GIS sample to Motorola Solutions within ten (10) business days of the GIS Planning Meeting to avoid impact on the Project Schedule. If GIS for the Customer is the same as the System Owner, this activity may not be required.
- Provide acknowledgement of the mutually agreed upon Project Kickoff Meeting agenda.
- Provide approval to proceed with the Project Kickoff meeting.
- Provide LMS user information as requested by Motorola Solutions.
- Review and complete the Business Process Review Agency Pre-Kick Off Survey within ten (10) business days of the Project Planning Session to avoid impact on the Project Schedule.

Motorola Solutions Deliverable

Title/Description
Project Kickoff Meeting Agenda.
Business Process Review Agency Pre-Kick Off Survey Link.

2.2.5.2 Project Kickoff Meeting

The purpose of the Project Kickoff Meeting is to introduce project participants and review the scope of the project.

Motorola Solutions Responsibilities

- Schedule and facilitate the Project Kickoff Meeting to clarify roles, responsibilities, establish team-working relationships, and initiate project tasks.
- The PM, lead Application Specialist, and lead Solutions Architect travel to Customer site. Other Motorola Solutions project team resources may attend remotely.

- Present a high-level overview of project scope.
- Confirm Customer access to the LMS.

Customer Responsibilities

- Provide a meeting space equipped with remote conferencing capability enabling remote Motorola Solutions project team members to participate.
- Identify and ensure participation of key team members in kickoff and project initiation activities.
- Confirm access to the LMS.

System Owner Responsibilities

- Assign the appropriate resources as may be required to participate in the Project Kickoff Meeting.
- Assign GIS Administrator to work with the Customer to facilitate GIS planning.

Motorola Solutions Deliverables

Title/Description
Project Kickoff Meeting Minutes.

2.2.5.3 GIS Planning Session

A GIS planning session will be scheduled to review the GIS Build Requirements Document and complete an overview of the GIS components of the project. The agenda will include:

- Review the Motorola Solutions GIS Build Requirements Document.
- Review the requirements of the Customer GIS sample data provided by the Customer that is required in the Motorola Solutions system.
- Discuss any GIS related project questions.

Motorola Solutions Responsibilities

- Schedule and conduct the remote GIS Planning Session.

Customer Responsibilities

- Review the GIS Build Requirements document prior the meeting.
- Work with the System Owner to complete GIS tasks and activities.

System Owner Responsibilities

- Work with the Customer to complete GIS tasks and activities.

Providing the GIS Customer Data is a critical Project Task. Delayed, incomplete, or inaccurate information may have a significant impact on the Project Schedule.

2.2.5.4 Contract Design Review

The objective of the Contract Design Review (CDR) is to review the contracted applications, Project Schedule, bill of materials, Training Plan, Test Plan, and contractual obligations of each party. The CDR will commence immediately following the conclusion of the Project Kickoff meeting while Motorola

Solutions resources are still on site. In the event the CDR cannot commence immediately following the Project Kickoff meeting while Motorola Solutions resources are on-site, Motorola Solutions will schedule a web conference session at a mutually agreeable date and time.

Motorola Solutions Responsibilities

- Review the applications, query(s), and interface(s) described in the System Description.
- Review the initial Project Schedule and incorporate Customer feedback resulting in the implementation Project Schedule. The Project Schedule will be maintained by Motorola Solutions and updated through mutual collaboration. Schedule updates that impact milestones will be addressed via the change provision of the Agreement.
- Review the system bill of materials and note any necessary modifications.
- Review the Training Plan and note any necessary modifications.
- Plan installation activities with the Customer.
- Review and memorialize project completion criteria and definition of completion of project.
- Discuss the Test Plan that will include test procedures that define steps to validate functionality, pass/fail criteria, and resolution for deficiencies. The Test Plan will be reviewed and finalized after System Provisioning.

Customer Responsibilities

- Provide input to the Project Schedule dates.
- Review the bill of materials and operating system software configuration with the Motorola Solutions project team.
- Participate in reviewing the Training Plan.
- Provide written acknowledgement of project completion criteria.

Motorola Solutions Deliverables

Title/Description
Initial Project Schedule.

2.2.6 Environment Review and Site Preparations

2.2.6.1 Site Review and Infrastructure Planning

The purpose of the environment review is to confirm the Customer's installation environment conforms with the site requirements presented in the System Description. Motorola Solutions will facilitate a remote meeting following the Project Kickoff to verify the existing infrastructure(s) and facilities will support an optimal installation environment for the Motorola Solutions system.

PremierOne is dependent on the System Owner's and Customer's LAN/WAN for client workstation performance. System Owner and Customer will provide network connectivity and all required network infrastructures to support the PremierOne application and ensure that sufficient bandwidth exists between System Owner and Customer's network systems to support optimal performance of the applications. The recommended network requirements are described in the System Description.

Motorola Solutions makes no provision for cabling or capital improvements to the installation environment and power consumption considerations may be required to support the Motorola Solutions system.

Motorola Solutions Responsibilities

- Review the site requirements section of the System Description with the Customer.
- Facilitate meeting to review the environment infrastructure requirements.
- Prepare a report with recommendations for any site preparation required to provide a suitable environment for installation of the system equipment and identifies any deficiencies related to power, power supplies, cabling, network connectivity, and communications equipment.

Customer Responsibilities

- Provide documentation on the current infrastructure, i.e. existing hardware and operating system software components and terminal networks, as well as projected utilization statistics and other information as is reasonably required to validate final hardware requirements.
- Make knowledgeable staff available to explain the current architecture, infrastructure, and environment.
- Provide a site for the installation, operation, and maintenance of all computer equipment, workstation(s), and related peripheral in accordance with Motorola Solutions requirements and all network infrastructures described in the System Description.
- Ensure the computer processor(s), operating system software, third-party software, all associated workstations, printers, communications, and related components conform with the specifications in the System Description.
- Provide any cabling or capital improvements required for the installation environment and/or power consumption considerations.

System Owner Responsibilities

- Work with the Customer to ensure installation site and networks meet specifications to support the addition of the Customer as an agency on the PremierOne system.
- Provide 24-hour access to a secured two-way Internet connection to the PremierOne system firewalls for the purposes of installation and configuration for the Customer throughout the course of the project.
- Provide a programmer work area for Motorola Solutions on-site staff in the primary facility, located near, but outside of the computer machine room. The room will be equipped with a workstation, AC power to support workspace for a minimum of two (2) people, and Internet access. Wireless access is recommended. This work area will be available during the course of the project.

2.2.7 CAD/Mobile Business Process Review (BPR) and System Provisioning

System provisioning includes user configurable parameters (i.e. specific values for unit names, timing of events, officer or user identification, street names, to name a few) that are defined within the system. Motorola Solutions will conduct a meeting following the Project Kickoff Meeting to begin the BPR process. During this meeting, the information required to provision the system to best meet the agency's functional needs, business processes, and workflows will be identified, reviewed, and collected. The Customer's SMEs and GIS personnel will participate in these activities.

The BPR and provisioning process will be conducted with personnel from the contracting/primary agency or for the primary communications center. The contracting/primary agency is responsible for engaging all user agencies that will be provisioned on the system to obtain required inputs. A single instance of the activities described in this phase will be conducted and a single provisioning profile will be developed for law enforcement and fire dispatch unless specifically stated otherwise. If an additional BPR or provisioning for additional agencies is required, it will be addressed via the Change Order process.

The resulting BPR workbook will reflect the features to be provisioned during the provisioning activities.

2.2.7.1 Business Process Review and Requirements Gathering

Motorola Solutions Responsibilities

- Deliver the Business Process Review (BPR) workbook prior to the workshop.
- Travel to Customer site for BPR.
- Review the BPR workbook and information needed to complete it.
- Conduct operational reviews during sit-alongs and ride-alongs.
- Review the documented business processes and provide configuration options.
- Review completed BPR workbook.

Customer Responsibilities

- Schedule dispatch and Sheriff sit-alongs and ride-alongs.
- Provide resources knowledgeable in the Customer's business processes to review workflows and provide relevant documentation on workflow and operating procedures.
- Prepare call and unit statistics.
- Gather and document required data in the BPR workbook.
- Review the documented business processes and select available configuration options.
- Finalize agency and beat names for the geodatabase. All of the data will be required, but streets, address points, and common places can be works in progress to be updated as the project moves forward. The agency and beat names should be final by provisioning.
- Review the completed BPR workbook with Motorola Solutions.

Motorola Solutions Deliverables

Title/Description
Pre-BPR Checklist.
Completed BPR Workbook.

2.2.7.2 Data Gathering

Following the completion of the BPR Workbook, Motorola Solutions will work with the Customer to identify the specific data elements (i.e. incident types, status codes, offenses, etc.) required to provision the system and provide worksheets which the Customer will capture required information.

Motorola Solutions Responsibilities

- Provide Provisioning Worksheets.
- Review the Provisioning Worksheets and identify the information required for provisioning data tables.

Customer Responsibilities

- Capture required data elements in the Provisioning Worksheets.
- Complete the provisioning worksheets at least ten (10) business days prior to the scheduled start of the provisioning activity.

NOTE: The Project Schedule is highly reliant on receipt of the completed Provisioning Worksheets.

Motorola Solutions Deliverables

Title/Description
Provisioning Worksheets.

2.2.7.3 PremierOne CAD and Mobile Provisioning

Motorola Solutions will guide the CAD and Mobile system provisioning based on the data gathered during the BPR and completion of the Provisioning Workbooks.

Motorola Solutions Responsibilities

- Review tables (configurable items) and associated data.
- Travel to Customer site to perform provisioning training in accordance with the Training Plan.
- Complete limited CAD and Mobile data entry for the primary provisioning profile.
- Remotely conduct checkpoints to verify accuracy of the Customer-provisioned data.
- Review and finalize provisioning decisions for the mobile client.

Customer Responsibilities

- Supply a classroom that meets the requirements in the Training Plan for provisioning training. Provide a workstation for the instructor and at least one workstation for every two students.
- Ensure availability of the SMEs to participate in the training.
- Verify foundational data entry completed by Motorola Solutions.
- Work with the System Owner to complete all provisioning data entry.
- Participate in checkpoints.

System Owner Responsibilities

- Work with Customer to verify foundational data entry completed by Motorola Solutions.
- Work with Customer to complete all provisioning data entry.
- Participate in checkpoints.

Motorola Solutions Deliverables

Title/Description
Provisioning Training.
Checkpoint Reports.

2.2.7.4 CAD Screen Tailoring

The objective of screen tailoring is to modify the user interface (UI) for the CAD client software.

Motorola Solutions will discuss the options for modifying the UI based on the CAD UI Screen Tailoring document. We will configure an initial CAD User Interface (UI) and review it with the Customer. One Law UI will be tailored for all law enforcement dispatch users/agencies. The Customer will have one opportunity to identify additional modifications to the UI within ten (10) days following the UI review. Motorola Solutions will deliver the UI as the final version. Subsequent requests for changes will be evaluated per the change order process.

Motorola Solutions Responsibilities

- Present available options for modifying the CAD UI.
- Modify the CAD UI.
- Review CAD UI with the Customer.
- Make final modifications after Customer review.
- Deliver the final CAD UI version.

Customer Responsibilities

- Participate in initial meetings to define requested CAD UI modifications.
- Evaluate the CAD UI after the initial delivery and identify any final modification requests.

Motorola Solutions Deliverable

Title/Description
One (1) Modified LAW CAD User Interface.

2.2.7.5 Provisioning Verification

Motorola Solutions and the Customer's Application Administrator and SMEs will exercise the PremierOne system to verify the system has been provisioned in accordance with the BPR Workbook and Provisioning Worksheets and verify the system functions in accordance with the system documentation.

Motorola Solutions Responsibilities

- Provide CAD system orientation in a working session to allow Customer to verify provisioning.
- Document any anomalies identified during the verification process.

Customer Responsibilities

- Ensure the availability of the SME's that participated in the BPR and provisioning training for this activity.
- Update provisioning tables, if required.
- Work with Motorola Solutions to document any anomalies.

System Owner Responsibilities

- Provide a knowledgeable resource to participate in provisioning checkpoints.
- Work with the Customer to make any updates to provisioning tables.

Motorola Solutions Deliverables

Title/Description
Meeting minutes from working session.

2.2.8 Hardware and Software

Motorola Solutions will procure the system equipment in accordance with the bill of materials.

2.2.8.1 On-Site Installation

The objective of this activity is to install system hardware at the Customer's site. This activity addresses physical installation activities and system connectivity verification.

Motorola Solutions Responsibilities

- Install system hardware on the System Owner's server rack.
- Conduct a Power On test to validate the installed hardware and software are ready for configuration.
- Load preliminary provisioning data.
- Verify contracted software is available and accessible on the installed system.

Customer Responsibilities

- Work with System Owner to verify that server room is available and meets requirements stated in System Description.

System Owner Responsibilities

- Provide access to server rooms for installation of equipment required to support the addition of the Customer as a user agency.

Motorola Solutions Deliverable

Title/Description
Power On/Installation Verification.

2.2.8.2 Client Software Installation

Client software will be installed on the specified number of workstations/mobile devices to facilitate provisioning training and testing, and provide instruction to Customer personnel who will complete software installation on the remaining workstations.

Motorola Solutions Responsibilities

- Verify system readiness.
- Request client software.
- Deliver the Pre-Installation Preparation Checklist.
- Provide instruction on client software installation on up to five (5) CAD workstations, Mobile devices, and/or Records workstations.
- Provide instruction on client software deployment utility.
- Verify client software installation.

Customer Responsibilities

- Provide workstation/mobile device hardware in accordance with specifications.
- Assign personnel to observe software installation training.
- Complete installation of client software on remaining workstations and mobile devices.

Motorola Solutions Deliverables

Title/Description
Pre-Installation Preparation Checklist.
Installation Guide.

2.2.9 Interfaces and Integration

The installation, configuration, and demonstration of interfaces may be an iterative series of activities depending upon access to third-party systems. Interfaces will be installed and configured in accordance with the System Description and Project Schedule. Integrated functionality between Motorola Solutions developed products will be completed through the software installation and provisioning activities described herein. Integration activities that have specific requirements will be completed as outlined in this SOW.

2.2.9.1 Interface Review

Motorola Solutions and the Customer will review the connectivity and functionality described in the System Description/Interface Specifications Documents (ISDs) required to enable an interface.

Motorola Solutions Responsibilities

- Conduct a review of the interface to explain how the interface functions in the Motorola Solutions system.
- Work with the Customer's third-party vendors, as required, to clarify any connectivity issues/data transfer issues.

- Any modifications required to any interfaces following contract award will be documented and address via the Change Order provision of the Agreement prior to making changes to the interface specification and/or interface.

Customer's Responsibilities

- Provide input on the current use of the interface and verify the functional specification in the ISD meets the use case or identify desired changes to the specifications.
- Facilitate communications and assist with resolution of issues that arise between Motorola Solutions and the Customer's third-party vendor(s).
- Assume costs associated with efforts required of the third-party vendors, which may include professional services, API/SDK fees, Non-Disclosure Agreements, licenses, and configuration or development, if necessary, to support desired interface functionality.
- Initiate a Change Order for any modifications.

2.2.9.2 Interface Deployment

Connectivity will be established between the Motorola Solutions system and the external and/or third party systems to which the contracted software will interface. Motorola Solutions will configure the system to support each contracted interface. The Customer is responsible for engaging third-party vendors if and as required to facilitate connectivity and testing of the interfaces.

Motorola Solutions Responsibilities

- Establish connectivity to external and third party systems.
- Configure interfaces to support the functionality described in the System Description.
- Validate each interface can transmit and/or receive data in accordance with the System Description.

Customer Responsibilities

- Act as liaison between Motorola Solutions and third party vendors or systems as required to establish interface connectivity with the Motorola Solutions system.
- Provide personnel proficient with and authorized to make changes to the network and third party systems to support Motorola Solutions' interface installation efforts.
- Work with System Owner to provide network connectivity between PremierOne servers and the third-party systems.

Unknown circumstances, requirements, and anomalies at the time of initial design can present difficulties in interfacing to some third-party applications. These difficulties could result in a poorly performing or even a non–functional interface. When information and access to systems is provided, Motorola Solutions will be able to mitigate these difficulties. If Motorola Solutions mitigation requires additional third–party integration, application upgrades, API upgrades, and/or additional software licenses, those costs will need to be addressed through the Change Order provision of the Agreement.

System Owner Responsibilities

- Provide access to server rooms as required to facilitate interface configuration.
- Provide personnel proficient with and authorized to make changes to the network and third party systems to support Motorola Solutions' interface installation efforts.

- Work with Customer to provide network connectivity between PremierOne servers and the third-party systems.

Motorola Solutions Deliverables

Title/Description
Contracted interfaces and integration.

2.2.10 System Training

The objective of this task is to prepare for and deliver the contracted training. Motorola Solutions training is comprised of both computer-based (on-line) and instructor-led (on-site or remote). Training delivery methods vary dependent on course content. Training is delivered in accordance with the Training Plan.

Any training not specifically identified as being provided by Motorola Solutions, is expected to be provided as required by the System Owner.

2.2.10.1 Learning Management System (On-line Training)

Training is made available to Customer, in part, via Motorola Solutions' Software Enterprise Learning Management System (LMS). This subscription service provides Customer with continual access to Motorola Solutions' library of on-line learning content and allows your users the benefit of learning at times convenient to them. Content is added and updated on a regular basis to keep information current. Courses are delivered or supplemented by LMS content are described in the Training Plan.

Motorola Solutions Responsibilities

- Initial set up and addition of administrators.
- Provide instruction to Customer LMS Administrators on:
  - Adding and maintaining users.
  - Adding and maintaining Groups.
  - Assign courses and Learning Paths.
  - Running reports.

Customer Responsibilities

- Provide Motorola Solutions with names (first and last) and emails of Customer LMS administrators.
- Provide access to learningservices.motorolasolutions.com.
- Complete LMS Administrator training.
- Advise users of the availability of the LMS.
- Add/modify users, run reports, and add/modify groups.

Completion Criteria

- Work is considered complete at the conclusion of Motorola Solutions-provided LMS Administrator instruction.

2.2.10.2 Instructor-Led Training (On-site or Remote)

Motorola Solutions Responsibilities

- Deliver User Guides and training materials in electronic format.
- Perform training in accordance with the Training Plan.
- Provide limited remote support following Train the Trainer courses while Customer trainers conduct end user training.

Customer Responsibilities

- Supply classrooms with a workstation for the instructor and at least one (1) workstation for every two (2) students based on the requirements listed in the Training Plan.
- Designate training representatives who will work with the Motorola Solutions trainers in the development and delivery of training.
- Conduct end user training.

Motorola Solutions Deliverables

Title/Description
Electronic versions of User Guides and training materials.
Attendance Rosters.

2.2.11 Project Testing

The PremierOne solution has been tested and accepted by the System Owner, therefore no functional testing of the PremierOne applications installed at the Customer site is provided. Motorola Solutions will provide a functional demonstration that the applications are installed and configured in accordance with the provisioning workbooks. Motorola Solutions will also demonstrate that interfaces perform in accordance with agreed specifications.

2.2.11.1 Functional Demonstration

The objective of Functional Demonstration is to demonstrated the features and functions of the system to validate performance according to the contractual requirements. Functional Demonstration may not test all functions of the system, if identified as not being applicable to the Customer's operations or for which the system has not been provisioned.

Motorola Solutions Responsibilities

- Conduct Functional Demonstration.
- Develop remediation plan for features that may fail during the test.

Customer Responsibilities

- Witness the Functional Demonstration and acknowledge its successful completion.
- Participate in documenting items that fail testing and note the remediation action.

System Owner Responsibilities

- Participate in the functional demonstration.

Motorola Solutions Deliverable

Title/Description
Completed Functional Demonstration Results.
Remediation Plan/Schedule for failed issues, as required.

2.2.11.2 Interface Validation

The objective of Interface Validation is to verify that the installed interfaces perform in accordance with the ISDs as presented in the System Description.

Motorola Solutions is not responsible for issues arising from lack of engagement of third party and/or Customer resources to perform work required to enable/provision and/or configure an interface to a third-party system, or troubleshooting any issues on the Customer's third-party systems.

Interfaces that cannot be tested due to connectivity issues to external systems or the unavailability of Customer's third-party system will be demonstrated to show that Motorola Solutions' portion of an interface is enabled to send and/or receive data that supports the ISD. In such cases, Motorola Solutions demonstrating the elements within Motorola Solutions' control will constitute a successful demonstration and completion of the demonstration task.

Motorola Solutions Responsibilities

- Conduct Interface Validation demonstration.
- Develop remediation plan for anomalies that do not align with the functionality presented in the ISD.

Customer Responsibilities

- Provide access to a resource with access to the interfacing system to validate functionality.
- Witness the execution of the demonstration and acknowledge successful completion.
- Participate in the documentation of anomalies and work with Motorola Solutions to develop remediation action(s).

Motorola Solutions Deliverable

Title/Description
Remediation Plan/Schedule for documented anomalies, as required.

2.2.12 Go Live

2.2.12.1 Go Live Planning

Motorola Solutions will remotely assist the Customer in the transition of live operations from the Customer's legacy system to the Motorola Solutions system. Motorola Solutions will work with the Customer and System Owner to develop a detailed Cutover Plan. This plan includes the following information:

- Motorola Solutions and Customer resources and staffing.

- Pre-cutover tasks/activities to be performed leading up to go live.
- Readiness review meetings.
- Contingency/roll-back plans.
- Go live tasks and responsibilities during and after the live cut.
- Post live cut support resources and schedules.
- Issue reporting process.
- Escalation process.

Motorola Solutions Responsibilities:

- Facilitate meetings with Customer staff to develop and document the Cutover Plan.

Customer Responsibilities:

- Coordinate the participation of Customer technical and operational staff in cutover planning and development and documentation of the Cutover Plan.

Motorola Solutions Deliverable

Title/Description
Cutover Plan.

2.2.12.2 Transition to Live Operations

Following the conclusion of Functional Demonstration, Motorola Solutions and the Customer will begin transitioning the Customer from their legacy system to production use of the PremierOne applications.

Motorola Solutions Responsibilities:

- Work with Customer to schedule the date and time for the transition event.
- Execute the Cutover Plan.
- Provide resources as specified in the transition plan to support user operations and address questions.

Customer Responsibilities:

- Coordinate the participation of Customer technical and operational staff in cutover planning.
- Schedule and coordinate end user participation in the live operations cutover.
- Perform and support the cutover activities defined in the Cutover Plan.
- Provide first line support to Customer users.

System Owner Responsibilities:

- Coordinate the participation of System Owner technical and operational staff in cutover planning.
- Participate in the Cutover event.

Motorola Solutions Deliverable

Title/Description
Completion of Cutover Activities.

2.2.12.3 Documentation

As part of project completion, Motorola Solutions will validate Customer receipt of electronic copies of the following documentation:

- User Guides (for the primary products).
- CAD BPR Workbook.

2.2.13 Project Closure – Transition to Support

Following Cutover, the project is complete. Motorola Solutions and Customer certify the completion and Final System Acceptance milestone and the implementation project is formally closed.

The system will transition to the support phase of the contract per the terms and conditions of the Maintenance and Support Agreement.

2.3 PremierOne GIS

2.3.1 Overview

This document contains information regarding Motorola Solutions PremierOne GIS data requirements.

A Geographic Information System (GIS) is a system used to collect, manage, analyze, and display geographic data. This document is intended for use by personnel who are responsible for administering the GIS components of the PremierOne suite. System administration requires an understanding of both current agency system administration rules and procedures and how PremierOne functions.

2.3.2 GIS Data Requirements for Basic Functionality

2.3.2.1 Street Centerline

Street Centerlines are features that are geometrically represented as lines which represent an imaginary line running lengthwise along the center of street segments. Street segments are typically portions of a street that are bound on either side by an intersection with another street segment or dead end (cul-de-sac).

A source feature class containing street centerlines must contain the following fields:

- Left Low House
- Left High House
- Right Low House
- Right High House
- Street Name Parts Fields (may include parsed fields or may be stored entirely in a single concatenated field).
- Left Subdivision *(optional)*
- Right Subdivision *(optional)*
- Left City
- Right City
- Left Zip Code
- Right Zip Code
- State
- Description *(optional)*
- Low Cross Street Override *(optional)*
- High Cross Street Override *(optional)*
- Cross Street Bypass *(optional)*

2.3.2.2 Common Place Location Points

Common Places are features that are represented geometrically by a point which represents the precise map location associated with a specific place. The difference between a Common Place and an

Address Point is that Common Places are used for locations that are more commonly referred to by name rather than address.

Not all Common Places will have an address associated with them (mile markers, call boxes, recreational points of interest etc.).

A source feature class containing commonplace points must contain the following fields:

- Place Name
- Place Type *(optional)*
- Address *(optional)*
- Subhouse *(optional)*
- Building *(optional)*
- City
- Subdivision *(optional)*
- Zip Code
- State

Address Point Feature Class

Address Points are features that are represented geometrically by a point which represents the precise map location associated with a specific address.

A source feature class containing address points must contain the following fields:

- Address
- Subhouse *(optional)*
- Building *(optional)*
- City
- Subdivision *(optional)*
- Description *(optional)*
- Zip Code
- State

2.3.2.3 Response Boundary(s)

Response Boundaries are features that are represented geometrically by a polygon (area) which represent the smallest named geographic areas used to determine which agency and beat-assigned resources are responsible for responding to incidents created within a specific area.

Each response boundary feature is specific to a single agency.

A Response Boundary data source requires the following attributes:

- Boundary Name
- Agency ID

2.3.2.4 Optional Support Tables

Street Name Alias Table

Street name aliases must be maintained in a separate table. This table must contain at a minimum the real street name, the associated alias street name as well as the City ID.

Common Place Alias Table

Commonplace aliases may reside in the commonplace feature class or they may be maintained in a separate table. If alias data resides in a separate table the table must contain both the real commonplace name and the associated alias name.

2.3.2.5 Additional Boundary Data Types

Contractor Boundary

Contractor Boundaries are polygon (area) features which represent the geographical area used to define contractor rotations.

Each contractor boundary feature is specific to a single agency.

A contractor boundary data source requires the following attributes:

- Boundary Name
- Agency ID
- Contractor Type

2.3.2.6 Reporting District

Map Book Page boundaries are polygon (area) features which represent the geographical areas defined in a paper map book. Typically, these polygons are square or rectangular depending on the pages of the physical map book.

Reporting District boundaries is specific to a single agency.

A Map Book boundary data source requires the following attributes:

- Map Book Name
- Page Number Field *(optional)*
- Grid Reference

2.3.2.7 Map Book

Map Book Page boundaries are polygon (area) features which represent the geographical areas defined in a paper map book. Typically, these polygons are square or rectangular depending on the pages of the physical map book.

Map Book Page boundaries are not specific to agency.

A Map Book boundary data source requires the following attributes:

- Map Book Name

- Page Number Field *(optional)*
- Grid Reference

2.3.2.8 Premise Hazard Areas

Premise Hazard Areas are polygon (area) features which represent geographical areas associated with specific premise/hazard information. The initial use case for Premise Hazard areas was for the purpose of associating gate codes with incidents created within gated communities.

Premise Hazards are not specific to agency.

A Premise Hazard Area data source requires the following attributes:

- Area Name
- Area Description *(optional)*

MOTOROLA SOLUTIONS

Section 3

Equipment List

State-of-the-Art Technology for a Safe and Resilient Community

September 12, 2022

St. Johns County, FL

Table of Contents

Section 3

Equipment List

3.1 APX Radios

3.1.1 St. Johns Fire Rescue

Line #	Item Number	Description	Quantity	Term
	APX™ NEXT			
1	H45TGT9PW8AN	APX NEXT SINGLE BAND MODEL 4.5 PORTABLE.	450	
2	QA00569AP	ADD: 7/800MHZ BAND.	450	
3	QA01427AK	ALT: APX NEXT XE HOUSING GREEN.	450	
4	QA02006AE	ADD: APX NEXT XE M4.5 RUGGED RADIO.	450	
5	BD00001AA	ADD: CORE BUNDLE.	450	
6	H499KC	ENH: SUBMERSIBLE (DELTA T).	450	
7	H38DA	ADD: SMARTZONE OPERATION.	450	
8	Q806CH	ADD: ASTRO DIGITAL CAI OPERATION.	450	
9	Q361CD	ADD: P25 9600 BAUD TRUNKING.	450	
10	QA09028AA	ADD: VIQI VC RADIO OPERATION.	450	
11	QA03399AK	ADD: ENHANCED DATA.	450	
12	Q387CB	ADD: MULTICAST VOTING SCAN.	450	
13	QA00580BA	ADD: TDMA OPERATION.	450	
14	QA09001AM	ADD: WIFI CAPABILITY.	450	
15	BD00010AA	ADD: SECURITY BUNDLE.	450	
16	QA01767BL	ADD: P25 LINK LAYER AUTHENTICATION.	450	
17	Q498BN	ENH: ASTRO 25 OTAR W/ MULTIKEY.	450	
18	H797DW	ENH: DVP-XL ENCRYPTION AND ADP.	450	
19	Q15AU	ADD: AES/DES-XL/DES-OFB ENCRYPTION AND ADP.	450	
20	PMMN4137A	XVE500 REMOTE SPEAKER MICROPHONE, HIGH IMPACT GREEN, NO CHANNEL KNOB.	450	
21	NNTN9199A	IMPRES 2 SUC, 3.0A, 120VAC, TYPE A PLUG, NA.	450	
22	NNTN9217A	BATTERY PACK,BATTERY PACK,IMPRES GEN2, LIION,IP68, 4400T, UL2054 DIV 2.		

Line #	Item Number	Description	Quantity	Term
	DMS			
23	QA09030AA	ADD: MOTOROLA HOSTED RADIOCENTRAL W CPS.	450	
24	H637AA	ADD: APX NEXT DMS BUNDLE PROMO.	450	
25	LSV01P01414A	APX NEXT DMS ADVANCED SERVICE-PROMO.	450	12 MONTHS
26	PSV00S01424A	APX NEXT PROVISIONING.	1	
27	LSV01S01414A	APX NEXT DMS ADVANCED.	450	48 MONTHS
	Applications			
28	H636AB	ADD: APX NEXT APPLICATION BUNDLE PROMO.	450	
29	H638EA	ADD: SMART LOCATE MAPPING TRIAL PROMO.	450	
30	QA09017AA	ADD: LTE WITH ACTIVE SERVICE AT&T US.	450	
31	QA07710AA	ALT: STUBBY 7-800MHZ 6CM ANTENNA.	450	
32	SSV01P01407B	APX NEXT SMART PROG-PROMO.	450	1 YEAR
33	SSV01P01406A	APX NEXT SMART CONNECT - PROMO.	450	1 YEAR
34	SSV01P01476A	APX NEXT SMART LOCATE-PROMO.	450	1 YEAR
35	SSV01P01902A	APX NEXT SMART MAPPING-PROMO.	450	1 YEAR
36	SSV01P01685B	CC AWARE STARTER LOCATION & MAPPING FOR APX NEXT (1ST YEAR TRIAL).	450	1 YEAR
37	PSV01S02940A	SMARTMAPPING ENABLEMENT.	1	
38	SSV01S01407A	APX NEXT SMART PROG.	450	24 MONTHS
39	SSV01S01406A	APX NEXT SMART CONNECT.	450	24 MONTHS
40	SSV01S01476A	APX NEXT SMART LOCATE.	450	24 MONTHS
41	SSV01S01907A	APX NEXT SMART MAPPING.	450	24 MONTHS
	APX™ NEXT			
42	H45TGT9PW8AN	APX NEXT SINGLE BAND MODEL 4.5 PORTABLE.	30	
43	QA00569AP	ADD: 7/800MHZ BAND.	30	
44	QA00570AW	ADD: VHF BAND+.	30	
45	QA01427AK	ALT: APX NEXT XE HOUSING GREEN.	30	
46	QA02006AE	ADD: APX NEXT XE M4.5 RUGGED RADIO.	30	
47	BD00001AA	ADD: CORE BUNDLE.	30	
48	H499KC	ENH: SUBMERSIBLE (DELTA T).	30	

Line #	Item Number	Description	Quantity	Term
49	H38DA	ADD: SMARTZONE OPERATION.	30	
50	Q806CH	ADD: ASTRO DIGITAL CAI OPERATION.	30	
51	Q361CD	ADD: P25 9600 BAUD TRUNKING.	30	
52	QA09028AA	ADD: VIQI VC RADIO OPERATION.	30	
53	QA03399AK	ADD: ENHANCED DATA.	30	
54	Q387CB	ADD: MULTICAST VOTING SCAN.	30	
55	QA00580BA	ADD: TDMA OPERATION.	30	
56	QA09001AM	ADD: WIFI CAPABILITY.	30	
57	BD00010AA	ADD: SECURITY BUNDLE.	30	
58	QA01767BL	ADD: P25 LINK LAYER AUTHENTICATION.	30	
59	Q498BN	ENH: ASTRO 25 OTAR W/ MULTIKEY.	30	
60	H797DW	ENH: DVP-XL ENCRYPTION AND ADP.	30	
61	Q15AU	ADD: AES/DES-XL/DES-OFB ENCRYPTION AND ADP.	30	
62	PMMN4137A	XVE500 REMOTE SPEAKER MICROPHONE, HIGH IMPACT GREEN, NO CHANNEL KNOB.	30	
63	NNTN9199A	IMPRES 2 SUC, 3.0A, 120VAC, TYPE A PLUG, NA.	30	
64	NNTN9217A	BATTERY PACK,BATTERY PACK,IMPRES GEN2, LIION,IP68, 4400T, UL2054 DIV 2.	30	
	DMS			
65	QA09030AA	ADD: MOTOROLA HOSTED RADIOCENTRAL W CPS.	30	
66	H637AA	ADD: APX NEXT DMS BUNDLE PROMO.	30	
67	LSV01P01414A	APX NEXT DMS ADVANCED SERVICE-PROMO.	30	12 MONTHS
68	LSV01S01414A	APX NEXT DMS ADVANCED.	30	48 MONTHS
	Applications			
69	H636AB	ADD: APX NEXT APPLICATION BUNDLE PROMO.	30	
70	H638EA	ADD: SMART LOCATE MAPPING TRIAL PROMO.	30	
71	QA09017AA	ADD: LTE WITH ACTIVE SERVICE AT&T US.	30	
72	SSV01P01407B	APX NEXT SMART PROG-PROMO.	30	1 YEAR
73	SSV01P01406A	APX NEXT SMART CONNECT - PROMO.	30	1 YEAR
74	SSV01P01476A	APX NEXT SMART LOCATE-PROMO.	30	1 YEAR
75	SSV01P01902A	APX NEXT SMART MAPPING-PROMO.	30	1 YEAR
76	SSV01P01685B	CC AWARE STARTER LOCATION & MAPPING FOR APX NEXT (1ST YEAR TRIAL).	30	1 YEAR
77	SSV01S01407A	APX NEXT SMART PROG.	30	24

Line #	Item Number	Description	Quantity	Term
				MONTHS
78	SSV01S01406A	APX NEXT SMART CONNECT.	30	24 MONTHS
79	SSV01S01476A	APX NEXT SMART LOCATE.	30	24 MONTHS
80	SSV01S01907A	APX NEXT SMART MAPPING.	30	24 MONTHS
	Standalone Items			
81	NNTN7624C	CHARGER,CHR IMP VEH EXT NA/EU KIT.	36	
82	NNTN9115A	CHARGER, MULTI-UNIT, IMPRES G2, 6-DISP, US/NA/CA/LA PLUG, ACC-CHARGER.	30	

3.1.2 St Johns Sheriff's Office

Line #	Item Number	Description	Quantity	Term
	APX™ NEXT			
1	H45TGT9PW8AN	APX NEXT SINGLE BAND MODEL 4.5 PORTABLE.	756	
2	QA00569AP	ADD: 7/800MHZ BAND.	756	
3	BD00001AA	ADD: CORE BUNDLE.	756	
4	H499KC	ENH: SUBMERSIBLE (DELTA T).	756	
5	H38DA	ADD: SMARTZONE OPERATION.	756	
6	Q806CH	ADD: ASTRO DIGITAL CAI OPERATION.	756	
7	Q361CD	ADD: P25 9600 BAUD TRUNKING.	756	
8	QA09028AA	ADD: VIQI VC RADIO OPERATION.	756	
9	QA03399AK	ADD: ENHANCED DATA.	756	
10	Q387CB	ADD: MULTICAST VOTING SCAN.	756	
11	QA00580BA	ADD: TDMA OPERATION.	756	
12	QA09001AM	ADD: WIFI CAPABILITY.	756	
13	BD00010AA	ADD: SECURITY BUNDLE.	756	
14	QA01767BL	ADD: P25 LINK LAYER AUTHENTICATION.	756	
15	Q498BN	ENH: ASTRO 25 OTAR W/ MULTIKEY.	756	
16	H797DW	ENH: DVP-XL ENCRYPTION AND ADP.	756	
17	Q15AU	ADD: AES/DES-XL/DES-OFB ENCRYPTION AND ADP.	756	
18	QA07710AA	ALT: STUBBY 7-800MHZ 6CM ANTENNA.	756	
19	Q698AE	ALT: PLASTIC CARRY HOLSTER WITH 3 INCH CLIP.	756	

20	PMMN4136A	ACCESSORY KIT,XVP830 REMOTE SPEAKER MICROPHONE, NO CHANNEL KNOB.	756	
21	NNTN9199A	IMPRES 2 SUC, 3.0A, 120VAC, TYPE A PLUG, NA.	756	
22	NNTN9216A	BATTERY PACK,IMPRES GEN2, LIION,IP68, 4400T.	756	
	DMS			
23	QA09030AA	ADD: MOTOROLA HOSTED RADIOCENTRAL W CPS.	756	
24	H637AA	ADD: APX NEXT DMS BUNDLE PROMO.	756	
25	LSV01P01414A	APX NEXT DMS ADVANCED SERVICE-PROMO.	756	12 MONTHS
26	LSV01S01414A	APX NEXT DMS ADVANCED.	756	48 MONTHS
	Applications			
27	H636AB	ADD: APX NEXT APPLICATION BUNDLE PROMO.	756	
28	H638EA	ADD: SMART LOCATE MAPPING TRIAL PROMO.	756	
29	QA09017AA	ADD: LTE WITH ACTIVE SERVICE AT&T US.	756	
30	SSV01P01407B	APX NEXT SMART PROG-PROMO.	756	1 YEAR
31	SSV01P01406A	APX NEXT SMART CONNECT - PROMO.	756	1 YEAR
32	SSV01P01476A	APX NEXT SMART LOCATE-PROMO.	756	1 YEAR
33	SSV01P01902A	APX NEXT SMART MAPPING-PROMO.	756	1 YEAR
34	SSV01P01685B	CC AWARE STARTER LOCATION & MAPPING FOR APX NEXT (1ST YEAR TRIAL).	756	24 MONTHS
35	SSV01S01407A	APX NEXT SMART PROG.	756	24 MONTHS
36	SSV01S01406A	APX NEXT SMART CONNECT.	756	24 MONTHS
37	SSV01S01476A	APX NEXT SMART LOCATE.	756	24 MONTHS
38	SSV01S01907A	APX NEXT SMART MAPPING.	1	
39	PSV00S01424A	APX NEXT PROVISIONING.	1	
40	PSV01S02940A	SMARTMAPPING ENABLEMENT.	1	
41	PSV01S02944A	PROVISIONING SUPPORT.		
	Standalone Items			
42	NNTN9115A	CHARGER, MULTI-UNIT, IMPRES G2, 6-DISP, US/NA/CA/LA PLUG, ACC-CHARGER.	10	
43	TBD	CHARGER,CHR IMP VEH EXT NA/EU KIT.	120	

3.2 APX Enablement

Line #	Item Number	Description	Quantity
1	1	HKVN4797A	LICENSE,SMARTCONNECT ENABLEMENT
2	1	T8586	FORTINET FIREWALL APPLIANCE
3	1	HKVN4829A	LICENSE,SMARTMAPPING ENABLEMENT

3.3 PremierOne CAD

3.3.1 Microsoft, VMware, other Software Licensing, Network Management Components

The following table lists the type and number of Microsoft, VMware, Hewlett Packard Enterprise (HPe) and other licenses and the party responsible for providing them.

Table 3-1: Microsoft and VMware Licensing

Microsoft & VMware Licenses	Primary Site	DR Site	Total	Customer Provided	Motorola Solutions Provided
Microsoft SQL Server Enterprise 2017 2 Core ENT Add License	5	5	10		X
Microsoft System Center Operation Manager 2016 (SCOM)	12	12	24		X
VMware vSphere Ent+ CPU	2	2	4		X
Microsoft SQL Server Enterprise 2017 2 Core ENT Add License (for additional RDW)	1	1	2		X

The following table lists the type, number and who is providing these ancillary items:

Table 3-2: Network and Management Components

Description	Details	Customer Provided	Motorola Solutions Provided	Quantity
Client Access Licenses	Microsoft Windows Server 2016	X		1 Per Client
HPe DL360c Gen10 w/dual Xeon Gold 6146, 384 GB RAM, 2 NIC, 2 x 8GB microSD	Host Server		X	2 (1 Primary / 1 DR)
Nimble SAN Upgrade to 42TB Upgrade	Upgrade to existing SAN		X	2
Arista 7050TX-48	Replace existing Extreme Networks switches		X	2
Arista 7010TX-48	Replace existing Extreme Networks switches		X	1

3.4 PremierOne Records

3.4.1 Microsoft, VMware, other Software Licensing, Network Management Components

The following table lists the type and number of Microsoft, VMware, Hewlett Packard Enterprise (HPe) and other licenses and the party responsible for providing them.

Table 3-3:: Microsoft and VMware Licensing

Microsoft & VMware Licenses	Primary Site	DR Site	Total	Customer Provided	Motorola Solutions Provided
Microsoft SQL 2017 Standard 4 core license	4	3	7		X
Microsoft SQL 2017 Standard 2 core add-on license	5	5	10		X
Microsoft System Center Operation Manager 2016 (SCOM)	12	12	24		X
VMware vSphere Ent+ CPU	3	3	6		X
VMware Site Recovery Manager	0	2	2		X

The following table lists the type, number and who is providing these ancillary items:

Table 3-4: Network and Management Components

Description	Details	Customer Provided	Motorola Solutions Provided	Quantity
HPe DL360c Gen10 w/dual Xeon Gold 6146, 384 GB RAM, 2 NIC, 2 x 8GB microSD	Host Server		X	2 (1 Primary / 1 DR)

3.5 Jail Management Solution

3.5.1 Microsoft, VMware, other Software Licensing, Network Management Components

The following table lists the type and number of Microsoft, VMware, Hewlett Packard Enterprise (HPe) and other licenses and the party responsible for providing them.

Table 3-5: Microsoft and VMware Licensing

Microsoft & VMware Licenses	Primary Site	DR Site	Total	Customer Provided	Motorola Solutions Provided
Microsoft System Center Operation Manager 2016 (SCOM)	12	12	24		X
VMware vSphere Ent+ CPU	2	2	5		X
VMware Site Recovery Manager	0	1	1		X

The following table lists the type, number and who is providing these ancillary items:

Table 3-6: Network and Management Components

Description	Details	Customer Provided	Motorola Solutions Provided	Quantity
HPe DL360c Gen10 w/dual Xeon Gold 6146, 384 GB RAM, 2 NIC, 2 x 8GB microSD	Host Server		X	2 (1 Primary / 1 DR)

MOTOROLA SOLUTIONS

Section 4

Training

State-of-the-Art Technology for a Safe and Resilient Community

September 12, 2022

St. Johns County, FL

Table of Contents

Section 4

Training

4.1 APX NEXT

4.1.1 Training Overview

Partnering with Motorola Solutions will enable St. Johns County Sheriff's Office to build personnel competency and maximize return on investment.

Effective training ensures successful implementation and use of your communications system by all personnel for the life of the system. The training plan furnished to St. Johns County Sheriff's Office is comprised of targeted coursework developed and delivered by our expert instructors. This plan, included below, will effectively provide St. Johns County Sheriff's Office's personnel with a comprehensive understanding of the proposed system and user equipment.

We will collaborate with St. Johns County Sheriff's Office to tailor a final training plan to enable St. Johns County Sheriff's Office's organization to operate, configure, and manage the proposed solution effectively and efficiently.

4.1.2 Motorola Solutions Training

Motorola Solutions provides an expanding portfolio of training delivery methods, tools, and courses to support the training needs of our customers. The figure below shows the elements of our training methodology that qualify us as the leader in the communications training industry.

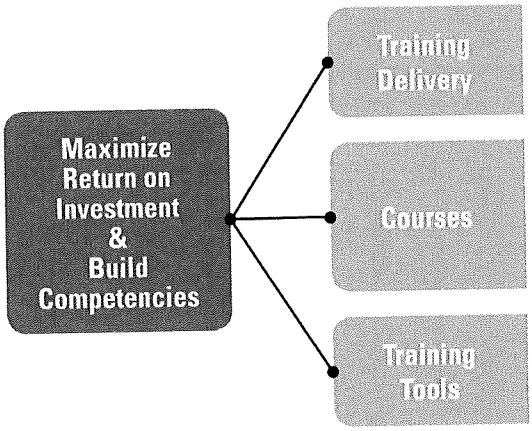


Figure 4-1: Build the competencies of St. Johns County Sheriff's Office personnel and maximize your return on investment with Motorola Solutions' expanding portfolio of training delivery methods, tools, and courses.

4.1.2.1 Training Delivery

Training Methods

Motorola Solutions' training experience and expertise enables our customers to gain the training they need to use during critical times in a variety of methods. As shown in the figure below, we offer three interactive methods of training: Online Self-Paced, Virtual Instructor-Led, and Instructor-Led.

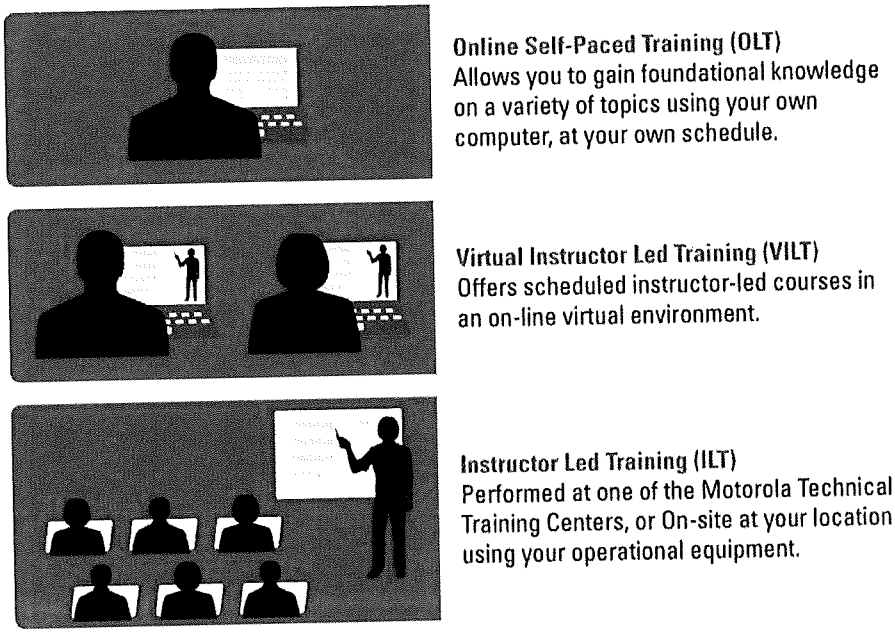


Figure 4-2: Motorola Solutions offers a variety of interactive training methods that cater to different learning techniques, allowing more effective ways to give personnel the skills they need.

These training approaches ensure our customers receive the understanding they need for the practical aspects of their jobs.

Delivery Options

Field

Field class delivery is "tailored" to the customer's specific system. We are providing classes which are not offered as standard "Open Resident" classes at our training facilities. The students benefit from working on their own systems, at their home location and within their schedules.

Motorola Facility

Resident classes are open to all Motorola customers, seating is based on availability, and participant guides and required pre-work when applicable are included in the tuition. These courses are comprehensive and are not tailored to any one customer's system. Students benefit from other students' experiences and are allowed to take systems out of service. These courses provide optimal "hands-on" training.

Motorola Facility Closed Sessions-Customer Specific

Special Resident classes are closed sessions for a particular Motorola Solutions customer. The customer is essentially renting the classroom. These courses are tailored to the customer's system as much as possible. The instructor will require the customer's system diagrams prior to the class taking place. The students will receive their ASTRO 25 IV&D manuals on CD-ROM and hard copy participant guides. Class manuals, participant guides, and required pre-work are included in the pricing of the class per student. The students are allowed to take systems out of service, which provides optimal "hands-on" training.

Motorola Solutions Instructors

We have approximately 40 instructor resources distributed across North America. These instructors are available to train customers in our Technical Training Center located in Schaumburg, Illinois, while specific training courses are available at our facility in Plantation, Florida. Training can also be delivered directly on-site at customer locations. All instructors undergo an Instructional Skills and Technical Knowledge Program, which is a globally-recognized training and instructor assessment program.

Consultative Services

Motorola Solutions provides consultative services for our customers, which includes personalized training plans and other training-related services. Our dedicated training consultant team works with our customers and Motorola Solutions account teams to identify and meet the training needs of technical, administrative end users, and other audiences.

4.1.2.2 Training Courses

Motorola Solutions offers a wide range of training courses to help our customers improve their proficiency with our expanding portfolio and get the most from their training system.

Our specialized courses/curriculums are designed for our customers' role. Whether they are an administrator, technician or user, Motorola Solutions makes sure our customers are equipped with foundational and advances skills.

General overviews of product and/or solution training offered are listed below:

Foundational Radio and Networking Training

Foundational Radio and Networking training provides new hires or staff from different skilled backgrounds fundamental knowledge. Some of these courses are online/self-paced while others are instructor led. Some topics include: Radio System Basics, Basic Networking, Communication System Concepts, Networking Essentials and Applied Networking. This allows Motorola Solutions to offer training before installation, during installation and after your solution is operational.

ASTRO 25 Infrastructure Training Courses

ASTRO 25 Infrastructure Training provides participants with a full curriculum that will enable them to maintain/service the new solution, and will give them the skills required to manage and operate the solution to obtain its fullest potential and capabilities.

ASTRO 25 Patch Management Training Course

ASTRO 25 Patch Management Training provides ASTRO 25 Land Mobile Radio (LMR) system administrators the information needed to access and patch their radio network infrastructure, update antivirus definitions, and review log files.

Console Training Courses

Console Training provides participants with a curriculum that will enable them to obtain a high-level understanding of the system configuration, general console operation, how to perform basic tasks, operating procedures for specific features, and the knowledge and skills necessary to manage and maintain the system.

Mobile and Portable Radio Training Courses

Mobile and Portable Radio Training provides participants with an introduction to the radio, the knowledge and skills necessary to perform basic radio operation, common operational tasks, operating procedures for specific features of the radio, and technical programming and maintenance of radios.

MOTOTRBO Training Courses

MOTOTRBO Training provides participants with a full curriculum that will enable them to maintain/service the new solution, and will give them the skills required to manage and operate the solution to obtain its fullest potential and capabilities.

CallWorks Training Courses

CallWorks Training provides participants with an overview of the components and functionality of the main application, operation, troubleshooting, a high-level understanding of the software, and configuration and maintenance of components of the CallWorks solution.

PremierOne Training Courses

PremierOne Training provides participants with sufficient knowledge of the PremierOne solution and its tools, giving them the skills necessary to operate and maintain the PremierOne solution.

LTE Training Courses

LTE Training provides participants a high-level understanding of the Public Safety LTE system and the network elements that comprise the system. Participants will gain knowledge of LTE architecture, signaling, system administration, and applied networking.

WAVE Training Courses

WAVE Training provides participants with an overview of the WAVE solution. It offers a basic understanding of how WAVE delivers a Radio-over-IP solution; describes features, hardware, and software requirements; how to use applications; and provides instruction in designing, integrating, and troubleshooting the WAVE solution.

4.1.2.3 Training Tools

Training Kits

Training kits are essential suitcase equipment, labs and exercises that apply to some of the ASTRO, MOTOTRBO, WAVE and LTE solutions. These kits are used in addition to equipment, in order to prevent solution downtime while training is conducted. As part of specific on-site classes, shown in Table 4-1, kits are included and shipped to our customers to allow students an in-depth, hands-on experience.

Table 4-1: Field Classes Training Kit Availability

Field Classes Training Kit Availability	
Networking Essentials	Server Virtualization
Applied Systems Networking	WAVE Certified Integration Engineer
Domain Controller	MOTOTRBO™ Systems Applied Networking

Tracking and Evaluation

All customer training is tracked and evaluated. The Project Manager and training team tracks and records all courses completed through the implementation of the project. Surveys are given to trainees to evaluate the trainers. Feedback is given and placed on our customer shared website.

End User Training Kit (EUTK)

The End User Training Kit is a knowledge-transfer tool designed to accelerate learning through customizability. Using the EUTK allows trainers to customize user/operator training to match unique button, feature programming, and displays provided in the system and radio codeplug. These tailored materials are developed by Motorola Solutions trainers using training kits that allow customer trainers to modify training materials when radio or console features change. Personnel are taught how to maneuver through and tailor the EUTK screens. The tailored selections are saved to an electronic file that the Motorola Solutions training team provides to the customer.

For a more detailed view of the training Motorola Solutions provides, please see our Product and System Technical Training Course Catalog: https://learning.motorolasolutions.com/catalog/56280enus

4.1.3 Proposed Training Overview for St. Johns County Sheriff's Office

In order to achieve the training goals identified by St. Johns County Sheriff's Office, we propose the following courses.

It is necessary that participants bring their laptop computers for all system administrator and technician classes. Materials will be delivered electronically via USB drives.

4.1.3.1 Radio User Training Plan

Course Title	Target Audience	Sessions	Duration	Location	Date	Participants
APX NEXT Portable (1 Model) Radio Training Train-the-Trainer Utilizing the End User Training Kit (Instructor-led)	Radio Trainers	1	1 day	St. Augustine, FL	Prior to training end users	15

4.1.4 Course Descriptions for St. Johns County Sheriff's Office

Course descriptions for St. Johns County Sheriff's Office are included on the following pages.

4.1.4.1 APX NEXT Train-the-Trainer

Course Synopsis and Objectives:	This course provides radio trainers with an introduction to the APX NEXT radio, its basic operation and tailored job aids available for assistance in operation. The learning experience is a mix of facilitation and hands-on activities to help users perform common tasks associated with the APX NEXT operation. Segmentation between user groups (i.e. Police, Fire/EMS, and Public Service) is encouraged to help focus instruction on the specific operational issues of the individual user group. This course is geared for customers who have an experienced dedicated training staff in their organization. It provides the customer's identified training personnel with the knowledge and practice applying training techniques that will enable them to successfully train their students. Trainers will use audio visual (Interactive End User Toolkits – iEUTK), facilitation and "hands-on" activities to facilitate learning events supported by tailored or customized training materials and job aides. They will become proficient in discussing common tasks associated with the operation of the customer's radios. After completing the course the participant will be able to: ▪ Understand a high-level overview of the customer system configuration. ▪ Understand the general radio operation. ▪ Understand proper operating procedures for specific customer features. ▪ Perform basic operational tasks of the radio. ▪ Utilize the provided job aids to perform specific tasks associated with the radio.
Delivery Method:	ILT - Instructor-led training
Duration:	8 hours
Participants:	Trainers, Supervisors and Support Personnel
Class Size:	Up to 15
Prerequisite:	Previous two-way radio and training experience

Curriculum:

Basics:
- Controls
- Buttons
- Switches
- Setting up APX NEXT
- Mics/Speakers
- Indicators

Using APX NEXT:
- On/Off/Standby
- SmartTouch/Onscreen keyboard
- Widgets
- Adjustments
- Battery Management
- Updates

Specific Features:
- Changing Talkgroups/Channels
- Changing Zones
- Mute tones of keypad
- Talkgroup Call
- Private Call
- Accessing Private Call Feature
- Initiating Private Call
- Call List Programming
- Announcement/All Call (Calls involving Multiple Talkgroups)
- Initiating Announcement/All Call
- Direct/Talkaround
- Failsoft
- Radio Profiles
- Accessing and changing Radio Profile
- Secure Operations
- ARS

Optional Features:
- Scan
- Scan program
- Priority Scan
- Dynamic Priority
- Telephone Interconnect
- Accessing Telephone Interconnect Feature
- Initiating a Phone Call
- Phone List Programming
- Contacts

Services:
- Smart Connect
- ViQi Voice Control
- ViQi Virtual Partner
- SmartLocate
- Radio Central
- SmartProgramming

Connectivity
- LTE
- Wi-Fi
- Bluetooth

	Data Services: ▪ Text Messaging ▪ Accessing the Text Messaging Feature ▪ Creating a Free Form Text Message ▪ Sending a "Canned " Text Message ▪ GPS ▪ OTAP User Interface ▪ Encryption ▪ Emergency

4.1.5 Proposed Training Overview for St. John's County Fire Rescue

In order to achieve the training goals identified by St. John's County Fire Rescue, we propose the following courses.

It is necessary that participants bring their laptop computers for all system administrator and technician classes. Materials will be delivered electronically via USB drives.

4.1.5.1 Radio User Training Plan

Course Title	Target Audience	Sessions	Duration	Location	Date	Participants
APX NEXT XB Portable (1 Model) **APX NEXT XN Portable (1 Model)** **Radio Training Train-the-Trainer** Utilizing the End User Training Kit (Instructor-led)	Radio Trainers	1	1 day	St. Augustine, FL	Prior to training end users	15

4.1.5.2 Course Descriptions for St. John's County Fire Rescue

Course descriptions for St. John's County Fire Rescue are included on the following pages.

4.1.5.3 APX NEXT Train-the-Trainer

Course Synopsis and Objectives:	This course provides radio trainers with an introduction to the APX NEXT radio, its basic operation and tailored job aids available for assistance in operation. The learning experience is a mix of facilitation and hands-on activities to help users perform common tasks associated with the APX NEXT operation. Segmentation between user groups (i.e. Police, Fire/EMS, and Public Service) is encouraged to help focus instruction on the specific operational issues of the individual user group. This course is geared for customers who have an experienced dedicated training staff in their organization. It provides the customer's identified training personnel with the knowledge and practice applying training techniques that will enable them to successfully train their students. Trainers will use audio visual (Interactive End User Toolkits – iEUTK), facilitation and "hands-on" activities to facilitate learning events supported by tailored or customized training materials and job aides. They will become proficient in discussing common tasks associated with the operation of the customer's radios. After completing the course the participant will be able to: ▪ Understand a high-level overview of the customer system configuration. ▪ Understand the general radio operation. ▪ Understand proper operating procedures for specific customer features. ▪ Perform basic operational tasks of the radio. ▪ Utilize the provided job aids to perform specific tasks associated with the radio.
Delivery Method:	ILT - Instructor-led training

Duration:	8 hours
Participants:	Trainers, Supervisors and Support Personnel
Class Size:	Up to 15
Prerequisite:	Previous two-way radio and training experience
Curriculum:	**Basics:** ▪ Controls ▪ Buttons ▪ Switches ▪ Setting up APX NEXT ▪ Mics/Speakers ▪ Indicators **Using APX NEXT:** ▪ On/Off/Standby ▪ SmartTouch/Onscreen keyboard ▪ Widgets ▪ Adjustments ▪ Battery Management ▪ Updates **Specific Features:** ▪ Changing Talkgroups/Channels ▪ Changing Zones ▪ Mute tones of keypad ▪ Talkgroup Call ▪ Private Call ▪ Accessing Private Call Feature ▪ Initiating Private Call ▪ Call List Programming ▪ Announcement/All Call (Calls involving Multiple Talkgroups) ▪ Initiating Announcement/All Call ▪ Direct/Talkaround ▪ Failsoft ▪ Radio Profiles ▪ Accessing and changing Radio Profile ▪ Secure Operations ▪ ARS **Optional Features:** ▪ Scan ▪ Scan program ▪ Priority Scan ▪ Dynamic Priority ▪ Telephone Interconnect ▪ Accessing Telephone Interconnect Feature ▪ Initiating a Phone Call ▪ Phone List Programming ▪ Contacts **Services:** ▪ Smart Connect ▪ ViQi Voice Control ▪ ViQi Virtual Partner ▪ SmartLocate ▪ Radio Central ▪ SmartProgramming

	Connectivity ▪ LTE ▪ Wi-Fi ▪ Bluetooth **Data Services:** ▪ Text Messaging ▪ Accessing the Text Messaging Feature ▪ Creating a Free Form Text Message ▪ Sending a "Canned " Text Message ▪ GPS ▪ OTAP User Interface ▪ Encryption ▪ Emergency

4.2 PremierOne CAD and Mobile Training Plan

4.2.1 Course Listing

The following matrix delineates the classes that have been proposed for the PremierOne product line. The matrix includes the number of classes per course type, the maximum number of participants per class and the location of each of the classes. Additional class modules may be obtained by the Customer for an additional fee.

Motorola Solutions offers in-person, remote, and Learning Management System ("LMS") training. Computer-based LMS training is available on demand during the deployment process and for 30 days after live cut. Continued availability of the training module is based on the LMS training package included in the proposal.

- LMS-P – students must complete LMS *prerequisites* before attending in-person training.
- LMS-C – these training *classes* are entirely conducted via LMS on demand with no in-person training component.
- LMS-R – this training offers *refresher* components that can be taken on demand after the in-person training is completed.
- Customer – in-person training conducted at the Customer site with an instructor onsite.
- Remote – scheduled in-person training conducted with a remote instructor.

Table 4-2: Course Listing

Course Module	Maximum No. Attendees Per Class	Number of Classes Included	Total Users Trained	Method of Instruction	Not To Exceed (hours) per Class
PremierOne CAD/Mobile Client Installation	N/A	N/A	N//A	LMS-C	4
PremierOne CAD/Mobile Provisioning Training	6	1	6	Customer LMS-R	24
PremierOne Computer Aided Dispatch Train-the-Trainer	12	1	12	LMS-P Customer	32
PremierOne Mobile Train-the-Trainer for Law Agencies	12	1	12	Virtual	4
PremierOne Mobile Train-the-Trainer for Law Agencies	N/A	N/A	N/A	LMS-C	4

4.2.2 Training Overview

Motorola considers training to be an extremely important aspect of the system installation and requires working closely with the Customer. Motorola utilizes a Learning Management System for both online and onsite training. The Learning Management System will be demonstrated during the project kick-off. Shortly after kick off the Customer will designate a Customer Training Representative. This individual will be the contact for the Learning Management System and Motorola trainers. Access to the Learning

Management System will be provided to each Customer PremierOne User. The Customer Training Representative will provide Motorola user names and email addresses so access to the LMS can be completed. The Customer Training Representative should be familiar with the Customer's daily operations and must attend (or designate a replacement) each Motorola educational course. Motorola trainers will rely on this representative to be the one point of contact for Motorola staff when policy and procedural questions arise, act as course facilitator, and act as the Customer's educational monitor. The Customer will also identify the personnel who will serve as trainers. These individuals must participate in all the Train-the-Trainer courses. In addition to the skills described below, the Customer's trainers must have prior experience as a classroom instructor and a thorough understanding of the Customer's operations. Other courses will require participants from different areas of the Customer's operations as shown in the individual course descriptions, detailed in Motorola training course descriptions.

4.2.2.1 System Administrator

The Customer will appoint a key individual to act as the System Administrator. This individual will be responsible for reporting/verifying problems, completing and maintaining application configuration, and performing system administrative duties such as system back-ups, archives, etc. The designated individual should be proficient in Windows and possess database administration and PC and System knowledge. Motorola strongly recommends that the system administrator(s) be proficient in the prerequisites defined in the document.

The Customer is responsible for ensuring that its system administrators are proficient in the prerequisite technologies. These technologies are embedded in the Motorola applications; however, training in these technologies will not be provided by Motorola.

Microsoft Technologies

- Windows Administration.
- SQL Server 2017.
- SQL Server Reporting Services.
- System Center 2016 (SCOM).

4.2.2.2 Training Facilities and Schedules

The Customer shall provide facilities for training courses which are alcohol and smoke-free. Both the classroom and workshop classes will require a projector that can be connected to a PremierOne System workstation, white-board for instructor's use and shall accommodate student note taking. The workshop format also requires multi-monitor student workstations. Students and instructors will dedicate class time to training and will not be subject to interruptions. At least two days prior to each onsite training course, the instructor shall have access to the training facility and all workstations for setup and workstation configuration. All training will be held at the Customer's site or online utilizing the Learning Management System; at least two weeks prior to onsite training courses, the customer must supply Motorola with a roster of course attendees and they will be provided access to Pre-Requisite training that must be completed prior to the onsite training course start date. Motorola and the Customer shall mutually agree to training schedules to accommodate the Customer's shift operations and other site-specific requirements. Evening courses will end by 11:00 p.m. Weekends and Holidays will not be used as training days.

4.2.2.3 Training Methods and Procedures

Motorola offers onsite training and online training both coordinated with the Software Enterprise learning management system. Types of training courses include:

- Administrative workshops: focused on providing specialized users with in-depth knowledge on the features, operational, and administrative functions of the system.
- Train the Trainer: instructor-led classroom training that provides key individuals with extensive hands-on use of the system utilizing true-to-life incident scenarios so they can develop and provide training to new users.
- End User Training: Instructor-led classroom training that provides users with instruction on subject matter relevant to their respective role in using and or supporting the PremierOne System. In addition to facilitated discussion, End User training consist workshop elements where needed, to provide hands on demonstration of the material being presented.
- Instructor Led online training using the Learning Management System.
- Online "Anytime" training using the Learning Management System.

Students have should a typing proficiency of 25 wpm, knowledge of PCs and Microsoft Windows, and have completed course prerequisites as listed in the course descriptions prior to the classroom training.

Designated Motorola Application Specialists will provide application instruction using several techniques and materials.

- Instructor Lesson Plan: The instructor's tool for planning the detailed course content on a module-by-module basis.
- Training Course Agenda: The student handout that outlines the course sequence of events including duration, and course modules.
- Worksheets, Job-Aids, Quizzes, retention instructional activities.
- Training Course Objectives: The instructor's predefined course objectives. These are provided for Train-the-Trainer classes only.
- Evaluations: On the final day of a training class, the students will be asked to complete an Instructor Evaluation form. They are optional forms and anonymity is acceptable.
- Certificates of Attendance: Students completing the onsite and online classes will receive Certificates of Attendance.
- Attendance Rosters: Customers will provide to the Motorola instructor a roster listing the names of training participants ten (10) days prior to the start of the course. Instructors will complete Attendance Rosters of actual participants for each day of training
- Prerequisite training for onsite courses using the Learning Management System to provide base knowledge for all students prior to the start of on the onsite class.
- Motorola PremierOne User Documentation: An electronic copy of the applicable Motorola Reference Manuals and documentation will be provided prior to training. The Customer is responsible for duplicating and delivering manuals to participating students prior to class commencement.

4.2.2.4 Training Subsystem

PremierOne has a fully functional training environment that will enable the Customer's trainers to provide on-going training. This training subsystem allows training to continue without interruption of the real time operations. Use of the training subsystem is covered in the Train the Trainer classes.

4.2.2.5 Session Attendance

Motorola is committed to providing a quality training experience and desires that the Customer receives the maximum benefit from each onsite training session. Each training session has been sized to provide the optimal training environment that meets the needs of the students in relation to the complexity of the material being presented. Given the nature of the material being presented and the intensity of the training, it is imperative that maximum course numbers not be exceeded. In the event the number of students in attendance exceeds the published maximum number of students and the list of participants identified on the training roster, Motorola will take corrective action, ensuring the integrity of the session is maintained and the student's ability to learn is protected. Motorola corrective action may include:

- Delaying the start of training until the number of students in attendance is in line with the maximum number of students allowed for the session.
- Splitting the class into multiple sessions. In such a case, the Customer will be charged for multiple occurrences of the class plus additional expenses, including travel related expenses, incurred by Motorola Solutions.
- Delaying the classroom training until the Prerequisite training has been completed in the LMS by each learner.

4.2.2.6 Learning Management System (LMS) Requirements

The LMS is accessed via internet browser. Accounts to access the LMS are created for each learner using their Email address. All learners accessing LMS content must have an account in the LMS. A learner will need to have access to the internet via workstation, laptop, tablet or smartphone to access learning. Audio accompanies visual display; speakers or headsets for listening are recommended. Course assessment evaluations are also accessed via the LMS. Access to these evaluations in the classroom is suggested.

4.2.3 Course Descriptions

The following tables provide detailed descriptions of training courses that will be provided as part of the system at the location indicated.

Table 4-3: PremierOne CAD/Mobile Client Installation (LMS)

Goal:	Provide selected personnel with sufficient knowledge to install PremierOne CAD and/or Mobile client software on workstations. Includes prerequisite third-party software. If the customer desires, an imaging solution can be presented.
Course Materials:	LMS-C
Location:	On Demand
Duration:	Approximately 1 hour of online training material
Participants:	IT staff who are responsible for installing workstation software

Class Size:	N/A
Prerequisite:	Knowledge of Microsoft operating systems and basic software installation practices.
Instructor:	LMS
Environment Setup:	Each workstation or device must have an internet connection to the LMS system.

Table 4-4: PremierOne CAD/Mobile Provisioning Training

Goal:	Provide detailed instruction on Mobile and Computer Aided Dispatch (CAD) provisioning data files.
Course Materials:	▪ PremierOne CAD/Mobile Provisioning Guide ▪ Course Outline
Location:	Customer's facility
Duration:	▪ 24 hours over three consecutive days on-site ▪ Approximately 8 hours online prerequisite training
Participants:	Those responsible for making the decisions on configuration options and have participated in the business process review.
Class Size:	Maximum of six (6) students
Prerequisite:	▪ LMS Prerequisite training courses. ▪ Knowledge of current Mobile and CAD application and configuration and agency SOPs. ▪ Microsoft and ESRI proficiency as defined in the Prerequisites Section.
Instructor:	Motorola Solutions Application Specialist
Environment Setup:	▪ One (1) workstation for each participant. ▪ Each workstation or device used for LMS prerequisites must have an internet connection. ▪ CAD workstation for each participant with network connection to the PremierOne servers. ▪ Instructor's workstation(s). ▪ Projector. ▪ White board (if possible). ▪ Microsoft Excel should be installed on at least one training workstation.

Table 4-5: PremierOne Computer Aided Dispatch Train-the-Trainer

Goal:	Provide selected personnel with sufficient knowledge to support a comprehensive end user training program.
Course Materials:	▪ CAD User Guide ▪ CAD Online Help (accessible through the CAD Client) ▪ Course Outline ▪ LMS refresher training courses
Location:	Customer's facility
Duration:	▪ Up to 32 hours over four consecutive business days on-site. ▪ Approximately 8 hours of online prerequisite material.
Participants:	Instructors who are responsible for the in house training of employees and for ongoing user training.
Class Size:	Maximum of twelve (12) students
Prerequisite:	Knowledge of current CAD application and customer operations. LMS Prerequisite training courses.

	- PremierOne CAD Overview - PremierOne CAD/Logging in - PremierOne CAD/Logging Out - PremierOne CAD/Info Panel - PremierOne CAD/Dynamic Help - PremierOne CAD/Function Keys - PremierOne CAD/Keyboard Shortcuts - PremierOne CAD/Command Line Syntax/Punctuation - PremierOne CAD/Clearing the Work Area - PremierOne CAD/Location Verification
Instructor:	Motorola Solutions Application Specialist
Environment Setup:	- Each workstation or device used for LMS prerequisites must have an internet connection. - CAD workstation for each participant with network connection to the PremierOne servers. - Instructor's workstation(s) with network connection. - Projector. - White board (if possible).

Table 4-6: PremierOne Mobile Train-the-Trainer

Goal:	Provide selected personnel with sufficient knowledge to support a comprehensive end user training program.
Course Materials:	- PremierOne Mobile User Guide - Course Outline
Location:	Virtual training using AdobeConnect
Duration:	Up to 4 hours in a single business day
Participants:	Instructors who are responsible for the in house training of employees and for ongoing user training.
Class Size:	Maximum of twelve (12) students
Prerequisite:	Knowledge of current Mobile application and customer operations.
Instructor:	Motorola Solutions Application Specialist
Environment Setup:	- A workstation or device for each participant with network connection. - Instructor's workstation(s) with network connection. - Projector. - White board (if possible).

Table 4-7: PremierOne Mobile Train-the-Trainer (LMS-C)

Goal:	Provide selected personnel with sufficient knowledge to support a comprehensive end user training program.
Course Materials:	PremierOne Mobile User Guide **Mobile End User Courses** (Access to courses for functionality not being utilized can be restricted if requested.) - PremierOne Mobile/Overview and Navigation - PremierOne Mobile/Logging In - PremierOne Mobile Logging Off - PremierOne Mobile/Status Monitors - PremierOne Mobile/Monitored Areas/Agencies - PremierOne Mobile/Viewing and Updating Incidents

	- PremierOne Mobile/Traffic Stops - PremierOne Mobile/Unit Status - PremierOne Mobile/Closing an Incident - PremierOne Mobile/Incident Searches - PremierOne Mobile/Syncing Mobile - PremierOne Mobile/Field Initiated Incidents - PremierOne Mobile/Incident Recall - PremierOne Mobile/Follow Me Settings - PremierOne Mobile/Incident Persons and Vehicles - PremierOne Mobile/Premise Hazards - PremierOne Mobile/Self-Dispatching - PremierOne Mobile/Queries - PremierOne Mobile/Editing Capabilities and Skills - PremierOne Mobile/Error Reports - PremierOne Mobile/Assigning Report Number(s) - PremierOne Mobile/Contractors - PremierOne Mobile/Stacked Incidents - PremierOne Mobile/Mapping - PremierOne Mobile/Lock and Unlocking Session - PremierOne Mobile/Switch Users - PremierOne Mobile/Change Roles - PremierOne Mobile/Incident Attachments - PremierOne Mobile/Messaging - PremierOne Mobile/Command Line - PremierOne Mobile/Mobile Speech
Location:	On Demand
Duration:	Approximately 4 hours of online prerequisite training material.
Participants:	Instructors who are responsible for the in house training of employees and for ongoing user training.
Class Size:	N/A
Prerequisite:	Knowledge of current Mobile application and customer operations.
Instructor:	LMS-C
Environment Setup:	Each workstation or device used for LMS courses must have an internet connection.

MOTOROLA SOLUTIONS

Section 5

Pricing

State-of-the-Art Technology for a Safe and Resilient Community

September 12, 2022

St. Johns County, FL

Table of Contents

Section 5

Pricing

5.1 Pricing Summary

5.1.1 APX NEXT and PremierOne Suite

Qty	Model	MSRP	Contract Discounted Unit Price	Extended Price
SJFR XE & Mobiles				
450	APX NEXT XE Single Band		$8,117	$3,652,650
30	APX NEXT XE Dual Band		$8,920	$267,600
	DMS 5 YR Advanced		$370	$177,566
	YRS 2 & 3 SMART Subscriptions		$600	$288,000
36	Vehicular Charger		$465	$16,746
30	6-Slot Charger		$1,036.75	$31,103
480		**$7,053,237**	**APX NEXT Hardware/Software Total**	**$4,433,665**
	Systems Integration Services - Engineer, System Technologist, Project Manager, Local Service, and Customer Training			$211,119
			FR Radios Solution Total	**$4,644,784**
			Trade-In of quantity 480 existing APX Radios	($168,000)
			QTY 450+ Volume Incentive	($125,000)
			FR Radios Sale Price	**$4,351,784**
SJSO APX NEXT & Mobiles				
756	APX NEXT Single Band		$7,396	$5,591,376
	DMS 5 YR ADVANCED		$370	$279,667
	YRS 2 -& 3 SMART Subscriptions		$600	$453,600
10	6 Slot Charger		$1,037	$10,368
120	Vehicular Charger		$465	$55,819
756		**$9,509,662**	**APX NEXT Hardware/Software Total**	**$6,390,829**
	Systems Integration Services - Engineer, System Technologist, Project Manager, Local Service, and Customer Training			$248,881

Qty	Model	MSRP	Contract Discounted Unit Price	Extended Price
			Solution Total	**$6,639,710**

Trade-In of quantity 756 existing APX Radios	($264,600)
QTY 750+ Volume Incentive	($160,000)
SO Radios Sale Price	**$6,215,110**
Combined SO & FD 1200+ Radios	($198,000)
Combined FD & SO Radios Sale Price	**$10,368,894**

The below items for the St. Johns County Sheriff's Office, St. Augustine Police, and St. Augustine Beach Police are Optional and may be purchased at the below pricing prior to December 23, 2022.

P1 CAD Consolidation for SO Base System	**$1,460,810**
Combined Radios & CAD Incentive	($400,000)
Combined Radios & CAD Sale Price	**$11,429,704**
P1 Records & Jail	**$1,671,550**
Combined CAD, Records & Jail Incentive	($300,000)
Combined Radios & CAD Sale Price	**$12,801,254**
Years 2 through 5 of CAD Maintenance	**$1,173,920**
Years 4 and 5 of SMART Subscriptions	**$741,600**
Contract Total	**$14,716,774**

All Radio Pricing above is valid through November 18, 2022.

DMS 5 YRS & SMART Subscriptions YRS 2 & 3 must be prepaid.

5.1.2 Maintenance PremierOne Suite

Maintenance Detail	Year 1	Year 2	Year 3	Year 4	Year 5	Total 5 Years
Maintenance and Subscriptions (CAD)	Warranty**	$190,760.00	$194,200.00	$201,400.00	$209,300.00	$795,660.00
Maintenance and Subscriptions (RMS/JAIL)	-	Warranty**	$129,300.00	$134,300.00	$139,500.00	$403,100.00
Two (2) Annual User Conference Registrations	Included	$1,990.00	$1,990.00	$1,990.00	$1,990.00	$7,960.00
Onsite Upgrade Services	NA	Included with existing system				Included*
Hardware / Third Part SW upgrade (up to 1 over term)	NA	$25,700.00	$25,700.00	$25,700.00	$25,700.00	$102,800.00
Hardware Upgrade services (up to 1 over term)	NA	Included with existing system				Included*
Subtotal before Additional Discount	NA	$218,450.00	$351,190.00	$363,390.00	$376,490.00	$1,309,520.00
Multi-Year Discount	NA	($20,100.00)	($38,500.00)	($38,500.00)	($38,500.00)	($135,600.00)
PremierOne Annual Maintenance (for SO CAD, RMS, and Jail)	$0.00	$198,350.00	$312,690.00	$324,890.00	$337,990.00	$1,173,920.00

Optional PremierOne CAD SmartCop RMS Interface	Year 1	Year 2	Year 3	Year 4	Year 5	Total 5 Years
Interface Integration and Maintenance	$39,782	$2,490	$2,490	$2,490	$2,490	$49,742

Pricing for the entire PremierOne Suite, both CAPX and OPX, is captured above and will allow St. Johns to gain economies of scale on the purchase of the PremierOne Suite, while allowing for staggered implementation of solutions to meet the needs and concerns of an entire overhaul of the current system. This price lock guarantees a smooth transition for St. Johns to add RMS, and Jail over the next 2 years.

Embedded Maintenance for Microsoft products is limited to Systems Center Operations Manager embedded

Maintenance Detail	Year 1	Year 2	Year 3	Year 4	Year 5	Total 5 Years

licenses. Maintenance for Microsoft Windows Server and Microsoft SQL Server is NOT included.

***OnSite Upgrade Services are only required for the Standard Release Upgrades (4.5, 4.6, etc.). All On Demand and Cumulative upgrades are included in base maintenance delivered remotely. Standard Releases are available approximately once each year but do not have to be taken each year. Five (5) is suggested over 10 years (every other year); however, fewer or more may be selected. This will be combined with the existing system upgrade planning and schedule.**

**Warranty for Jail and RMS will start at go-Live for RMS and Jail. This is expected to be completed 1 years after CAD go-Live.

This proposal is valid through November 18, 2022 and is subject to the terms and conditions of the St Johns County Motorola Solutions Master Purchase Agreement.

PremierOne maintenance is proposed under the terms and conditions of the existing PremierOne Maintenance Agreement.

MOTOROLA SOLUTIONS

Section 6

Contractual Documentation

State-of-the-Art Technology for a Safe and Resilient Community

September 12, 2022

St. Johns County, FL

Table of Contents

Section 6

Contractual Documentation

Motorola Solutions has Amendment Two to the Master Purchase Agreement between St. Johns County and Motorola Solutions, Inc. on the following pages.

AMENDMENT TWO TO THE MASTER PURCHASE AGREEMENT BETWEEN ST. JOHNS COUNTY AND MOTOROLA SOLUTIONS, INC.

THIS AMENDMENT TWO TO THE AGREEMENT, by and between St. Johns County Board of County Commissioners, Florida (County), and Motorola Solutions, Inc., a Delaware corporation authorized to transact business in the State of Florida (Motorola); collectively referenced as "Parties".

WHEREAS, the County and Motorola entered into a Master Purchase Agreement No. 227662 for radio communications equipment, products and services, dated March 23, 2017 ("Agreement");

WHEREA, the County and Motorola signed the Amendment One to the Agreement on June 25, 2019 to provide certain products and services described in said amendment;

WHEREA, Section 16.8 of the Agreement provides that any changes to the Agreement must be documented in writing and signed by each party's authorized signatories;

WHEREAS, the parties wish to include additional equipment and services to the Agreement;

And

NOW, THEREFORE, the County and Motorola hereby agree to add the terms and conditions to the Agreement as follows:

1. The exhibits listed below are incorporated into and made a part of this Agreement:

Exhibit A	Payment Schedule
Exhibit B	Motorola's Proposal dated September 12, 2022 (the "Proposal")
Exhibit C	Additional Terms and Conditions: 1. Subscription Software Addendum 2. Data Processing Addendum

For clarity, the terms and conditions described in Exhibit C would prevail over the ones in the Agreement (No. 227662) only with respect of the offering described in the Proposal.

2. TERM

The parties wish to continue using the renewal option stated in Section 4 of the Agreement.

3. CONTRACT PRICE. The Contract Price in U.S. dollars is modified to include an additional $14,716,774, for the work described in Motorola's Proposal, Exhibit B. The pricing summary is set forth in Section 5 Pricing of Exhibit B. Motorola has priced the services, Software, and Equipment as an integrated system. A reduction in Software or Equipment quantities, or services, may affect the overall Contract Price, including discounts if applicable.

4. Customer affirms that a purchase order or notice to proceed is not required for contract performance or for subsequent years of service, if any, and that sufficient funds have been appropriated in accordance with applicable law. The Customer will pay all invoices as received from Motorola and any changes in scope will be subject to the change order process as described in this Agreement. At the time of execution of this Agreement, the Customer will provide all necessary reference information to include on invoices for payment in accordance with this Agreement.

5. INFLATION REVIEW. For multi-year agreements, at the end of the first year of the Agreement and each year thereafter, a CPI percentage change calculation shall be performed using the U.S. Department of Labor, Consumer Price Index, "All Items," Unadjusted Urban Areas (CPI-U). Should the annual inflation rate increase greater than 3% during the previous year, Motorola shall have the right

to increase all future maintenance prices by the CPI increase amount exceeding 3%. "All Items," not seasonally adjusted shall be used as the measure of CPI for this price adjustment. The adjustment calculation will be based upon the CPI for the most recent twelve (12) month increment beginning from the most current month available as posted by the U.S. Department of Labor (http://www.bls.gov) immediately preceding the new maintenance year. For purposes of illustration, if in Year 5 the CPI reported an increase of 8%, Motorola may increase the Year 6 price by 5% (8%-3% base).

Except as set forth in this Amendment Two, all other terms and conditions of the Agreement remain unchanged and in full force and effect.

IN WITNESS WHEREOF, the County and Motorola execute this Amendment One to the Agreement as follows:

St. Johns County Board of County
Motorola Solutions, Inc.

Motorola: Motorola Solutions, Inc.

By: _____

Name: _____

Title: _____

Date: _____

Customer: St. Johns County FL Board of County Commissioners

By: _____

Name: _____

Title: _____

Date: _____

EXHIBIT A

Payment Schedule for PSA System Agreement

Except for a payment that is due on the Effective Date, Customer will make payments to Motorola within thirty (30) days after the date of each invoice. Customer will make payments when due in the form of a check, cashier's check, or wire transfer drawn on a U.S. financial institution. If Customer has purchased additional Professional or Subscription services, payment will be in accordance with the applicable addenda. Payment for the System purchase will be in accordance with the following milestones.

System Purchase Including Years 2&3 APXNEXT Software Subscriptions (excluding Subscribers)

1. **20% of the System Price due upon Execution of Contract (due upon receipt);**
2. **20% of the System Price due upon Completion of Project Kickoff/Contract Design Review;**
3. **35% of the System Price due upon Delivery of applicable System Hardware and Application Software to Customer Site;**
4. **10% of the System Price due upon Installation at Customer Site;**
5. **10% of the System Price due upon Successful Completion of System Live Cut; and**
6. **5% of the System Price due upon Final Acceptance.**

100% of the Subscriber Contract Price will be invoiced upon shipment (as shipped).

Motorola shall make partial shipments of equipment and will request payment upon shipment of such equipment. In addition, Motorola shall invoice for installations completed on a site-by-site basis or when professional services are completed, when applicable. The value of the equipment shipped/services performed will be determined by the value shipped/services performed as a percentage of the total milestone value. Unless otherwise specified, contract discounts are based upon all items proposed and overall system package. For invoicing purposes only, discounts will be applied proportionately to the FNE and Subscriber equipment values to total contract price. Overdue invoices will bear simple interest at the maximum allowable rate by state law.

For Lifecycle Support Plan Services:
Motorola will invoice Customer annually in advance of each year of the plan.

EXHIBIT B

MOTOROLA PROPOSAL DATED SEPTEMBER 12, 2022

EXHIBIT C

Additional Terms and Conditions

1. Subscription Software Addendum

This Subscription Software Addendum (this "**SSA**") including its Exhibit, forms part of the Master Purchase Agreement ("MPA" or "Agreement") to reflect the parties' agreement with regard to the subscription services. Capitalized terms used in this SSA, but not defined herein, will have the meanings set forth in the MPA.

1. Addendum. This SSA governs Customer's purchase of Subscription Software (and, if set forth in the Proposal) from Motorola, and will form part of the Parties' Agreement. Additional Subscription Software-specific Addenda or other terms and conditions may apply to certain Subscription Software, where such terms are provided or presented to Customer.

2. Delivery of Subscription Software.

2.1. Delivery. During the applicable Subscription Term (as defined below), Motorola will provide to Customer the Subscription Software set forth in an Ordering Document, in accordance with the terms of the Agreement. Motorola will provide Customer advance notice (which may be provided electronically) of any planned downtime. Delivery will occur upon Customer's receipt of credentials required for access to the Subscription Software or upon Motorola otherwise providing access to the Subscription Software. If agreed upon in an Ordering Document, Motorola will also provide Services related to such Subscription Software.

2.2. Modifications. In addition to other rights to modify the products and services set forth in the MPA, Motorola may modify the Subscription Software, any associated recurring Services and any related systems so long as their functionality (as described in the applicable Ordering Document) is not materially degraded. Documentation for the Subscription Software may be updated to reflect such modifications. For clarity, new features or enhancements that are added to any Subscription Software may be subject to additional Fees.

2.3. User Credentials. If applicable, Motorola will provide Customer with administrative user credentials for the Subscription Software, and Customer will ensure such administrative user credentials are accessed and used only by Customer's employees with training on their proper use. Customer will protect, and will cause its Authorized Users to protect, the confidentiality and security of all user credentials, including any administrative user credentials, and maintain user credential validity, including by updating passwords. Customer will be liable for any use of the Subscription Software through such user credential (including through any administrative user credentials), including any changes made to the Subscription Software or issues or user impact arising therefrom. To the extent Motorola provides Services to Customer in order to help resolve issues resulting from changes made to the Subscription Software through user credentials, including through any administrative user credentials, or issues otherwise created by Authorized Users, such Services will be billed to Customer on a time and materials basis, and Customer will pay all invoices in accordance with the payment terms of the MPA.

2.4. Beta Services. If Motorola makes any beta version of a software application ("**Beta Service**") available to Customer, Customer may choose to use such Beta Service at its own discretion, provided, however, that Customer will use the Beta Service solely for purposes of Customer's evaluation of such Beta Service, and for no other purpose. Customer acknowledges and agrees that all Beta Services are offered "as-is" and without any representations or warranties or other commitments or protections from Motorola. Motorola will determine the duration of the evaluation period for any Beta Service, in its sole discretion, and Motorola may discontinue any Beta Service at any time. Customer acknowledges that Beta Services, by their nature, have not been fully tested and may contain defects or deficiencies.

3. Subscription Software License and Restrictions.

3.1. Subscription Software License. Subject to Customer's and its Authorized Users' compliance with the Agreement, including payment terms, Motorola hereby grants Customer and its Authorized Users a limited, non-transferable, non-sublicenseable, and non-exclusive license to use the Subscription Software identified in an Ordering Document, and the associated Documentation, solely for Customer's internal business purposes. The foregoing license grant will be limited to use in the territory and to the number of licenses set forth in an Ordering Document (if applicable), and will continue for the applicable Subscription Term. Customer may access, and use the Subscription Software only in Customer's owned or controlled facilities, including any authorized mobile sites; provided, however, that Authorized Users using authorized mobile or handheld devices may also log into and access the Subscription Software remotely from any location. No custom development work will be performed under this Addendum.

3.2. End User Licenses. Notwithstanding any provision to the contrary in the Agreement, certain Subscription Software is governed by a separate license, EULA, or other agreement, including terms governing third-party software, such as open source software, included in the Subscription Software. Customer will comply, and ensure its Authorized Users comply, with such additional license agreements.

3.3. Customer Restrictions. Customers and Authorized Users will comply with the applicable Documentation and the copyright laws of the United States and all other relevant jurisdictions (including the copyright laws where Customer uses the Subscription Software) in connection with their use of the Subscription Software. Customer will not, and will not allow others including the Authorized Users, to make the Subscription Software available for use by unauthorized third parties, including via a commercial rental or sharing arrangement; reverse engineer, disassemble, or reprogram software used to provide the Subscription Software or any portion thereof to a human-readable form; modify, create derivative works of, or merge the Subscription Software or software used to provide the Subscription Software with other software; copy, reproduce, distribute, lend, or lease the Subscription Software or Documentation for or to any third party; take any action that would cause the Subscription Software, software used to provide the Subscription Software, or Documentation to be placed in the public domain; use the Subscription Software to compete with Motorola; remove, alter, or obscure, any copyright or other notice; share user credentials (including among Authorized Users); use the Subscription Software to store or transmit malicious code; or attempt to gain unauthorized access to the Subscription Software or its related systems or networks.

4. Term.

4.1. Subscription Terms. The duration of Customer's subscription to the first Subscription Software and any associated recurring Services ordered under this SSA (or the first Subscription Software or recurring Service, if multiple are ordered at once) will commence upon delivery of such Subscription Software (and recurring Services, if applicable) and will continue for a twelve (12) month period or such longer period identified in an Ordering Document (the "**Initial Subscription Period**"). Following the Initial Subscription Period, Customer's subscription to the Subscription Software and any recurring Services will automatically renew for additional twelve (12) month periods (each, a "**Renewal Subscription Year**"), unless either Party notifies the other Party of its intent not to renew at least thirty (30) days before the conclusion of the then-current Subscription Term. (The Initial Subscription Period and each Renewal Subscription Year will each be referred to herein as a "**Subscription Term**".) Motorola may increase Fees prior to any Renewal Subscription Year. In such case, Motorola will notify Customer of such proposed increase no later than thirty (30) days prior to commencement of such Renewal Subscription Year. Unless otherwise specified in the applicable Ordering Document, if Customer orders any additional Subscription Software or recurring Services under this SSA during an in-process Subscription Term, the subscription for each new Subscription Software or recurring Service will (a) commence upon delivery of such Subscription Software or recurring Service, and continue until the conclusion of Customer's then-current Subscription Term (a "**Partial Subscription Year**"), and (b) automatically renew for Renewal Subscription Years thereafter, unless either Party notifies the other Party of its intent not to renew at least thirty (30) days before the conclusion of the then-current Subscription Term. Thus, unless otherwise specified in the

applicable Ordering Document, the Subscription Terms for all Subscription Software and recurring Services hereunder will be synchronized.

4.2. Term. The term of this SSA (the "**SSA Term**") will commence once both parties execute this amendment two.

4.3. Termination. Notwithstanding the termination provisions of the MPA, Motorola may terminate this SSA (or any Addendum or Ordering Documents hereunder), or suspend delivery of Subscription Software or Services, immediately upon notice to Customer if (a) Customer breaches **Section 3 – Subscription Software License and Restrictions** of this SSA, or any other provision related to Subscription Software license scope or restrictions set forth in an Addendum or Ordering Document, or (b) it determines that Customer's use of the Subscription Software poses, or may pose, a security or other risk or adverse impact to any Subscription Software, Motorola, Motorola's systems, or any third party (including other Motorola customers). Customer acknowledges that Motorola made a considerable investment of resources in the development, marketing, and distribution of the Subscription Software and Documentation, and that Customer's breach of the Agreement will result in irreparable harm to Motorola for which monetary damages would be inadequate. If Customer breaches this Agreement, in addition to termination, Motorola will be entitled to all available remedies at law or in equity (including immediate injunctive relief).

4.4. Wind Down of Subscription Software. In addition to the termination rights in the MPA, Motorola may terminate any Ordering Document and Subscription Term, in whole or in part, in the event Motorola plans to cease offering the applicable Subscription Software or Service to customers.

5. Payment.

5.1. Payment. Unless otherwise provided in an Ordering Document (and notwithstanding the provisions of the MPA), Customer will prepay an annual subscription Fee set forth in an Ordering Document for each Subscription Software and associated recurring Service, before the commencement of each Subscription Term. For any Partial Subscription Year, the applicable annual subscription Fee will be prorated based on the number of months in the Partial Subscription Year. The annual subscription Fee for Subscription Software and associated recurring Services may include certain one-time Fees, such as start-up fees, license fees, or other fees set forth in an Ordering Document. Motorola will have the right to suspend the Subscription Software and any recurring Services if Customer fails to make any payments when due.

5.2. License True-Up. Motorola will have the right to conduct an audit of total user licenses credentialed by Customer for any Subscription Software during a Subscription Term, and Customer will cooperate with such audit. If Motorola determines that Customer's usage of the Subscription Software during the applicable Subscription Term exceeded the total number of licenses purchased by Customer, Motorola may invoice Customer for the additional licenses used by Customer, pro-rated for each additional license from the date such license was activated, and Customer will pay such invoice in accordance with the payment terms in the MPA.

6. Liability.

6.1. ADDITIONAL EXCLUSIONS. IN ADDITION TO THE EXCLUSIONS FROM DAMAGES SET FORTH IN THE MPA, AND NOTWITHSTANDING ANY PROVISION OF THE AGREEMENT TO THE CONTRARY, MOTOROLA WILL HAVE NO LIABILITY FOR (A) INTERRUPTION OR FAILURE OF CONNECTIVITY, VULNERABILITIES, OR SECURITY EVENTS; (B) DISRUPTION OF OR DAMAGE TO CUSTOMER'S OR THIRD PARTIES' SYSTEMS, EQUIPMENT, OR DATA, INCLUDING DENIAL OF ACCESS TO USERS, OR SHUTDOWN OF SYSTEMS CAUSED BY INTRUSION DETECTION SOFTWARE OR HARDWARE; (C) AVAILABILITY OR ACCURACY OF ANY DATA AVAILABLE THROUGH THE SUBSCRIPTION SOFTWARE OR SERVICES, OR INTERPRETATION, USE, OR MISUSE THEREOF; (D) TRACKING AND LOCATION-BASED SERVICES; OR (E) BETA SERVICES.

6.2. Voluntary Remedies. Motorola is not obligated to remedy, repair, replace, or refund the purchase price for the disclaimed or excluded issues in the MPA or **Section 6.1 – Additional Exclusions** above, but if Motorola agrees to provide Services to help resolve such issues, Customer will reimburse Motorola for its reasonable time and expenses, including by paying Motorola any Fees set forth in an Ordering Document for such Services, if applicable.

7. Motorola as a Controller or Joint Controller. In all instances where Motorola acts as a controller of data, it will comply with the applicable provisions of the Motorola Privacy Statement at https://www.motorolasolutions.com/en_us/about/privacy-policy.html#privacystatement, as may be updated from time to time. Motorola holds all Customer Contact Data as a controller and shall Process such Customer Contact Data in accordance with the Motorola Privacy Statement. In instances where Motorola is acting as a joint controller with Customer, the Parties will enter into a separate Addendum to the Agreement to allocate the respective roles as joint controllers.

8. Survival. The following provisions will survive the expiration or termination of this SSA for any reason: **Section 4 – Term**; Section **5 – Payment**; **Section 6.1 – Additional Exclusions**; **Section 8 – Survival**.

Subscription Services Addendum
Exhibit A: FirstNet and AT&T Service Terms

Public Safety Entity ("Customer") Responsibilities for access to and use of "First Net" Service as provided by

AT&T

General. The Customer is responsible for complying with AT&T Acceptable Use Policy found at att.com/aup and applicable AT&T Service Guides found at att.com/servicepublications.

Privacy. The Customer is responsible for complying with all applicable privacy laws. The Customer is responsible for obtaining consent from and giving notice to its Users regarding Motorola's and AT&T's collection and use of User information in connection with a Service. The Customer will only make accessible or provide Personal Data to Motorola and AT&T when it has the legal authority to do so.

User Eligibility. The Customer shall verify, or assist Motorola and AT&T in verifying, as stated below, the eligibility of its Users to use the Service. The Customer is required to verify and confirm that its Users are authorized and eligible to use Service. The Customer must perform periodic audits on a regular, but not less than once per year, basis to identify any individuals who are no longer eligible for Service. The Customer must produce such information as may be requested through AT&T by the FirstNet Authority and the United States Government to verify eligibility of its users.

Limitations on the Service. THE CUSTOMER ACKNOWLEDGES THAT SERVICE IS MADE AVAILABLE ONLY WITHINTHE OPERATING RANGE OF THE NETWORKS. SERVICE MAY BE TEMPORARILY REFUSED, INTERRUPTED, ORLIMITED BECAUSE OF: (A) FACILITIES LIMITATIONS; (B) TRANSMISSION LIMITATIONS CAUSED BY ATMOSPHERIC,TERRAIN, OTHER NATURAL OR ARTIFICIAL CONDITIONS ADVERSELY AFFECTING TRANSMISSION, WEAKBATTERIES, SYSTEM OVERCAPACITY, MOVEMENT OUTSIDE A SERVICE AREA OR GAPS IN COVERAGE IN A SERVICE AREA AND OTHER CAUSES REASONABLY OUTSIDE OF MOTOROLA OR AT&T'S CONTROL SUCH AS, BUT NOT LIMITED TO, INTENTIONAL OR NEGLIGENT ACTS OF THIRD PARTIES THAT DAMAGE OR IMPAIR THE NETWORK OR DISRUPT SERVICE; OR (C) EQUIPMENT MODIFICATIONS, UPGRADES, RELOCATIONS, REPAIRS, AND OTHER SIMILAR ACTIVITIES NECESSARY FOR THE PROPER OR IMPROVED OPERATION OF SERVICE.

Limitations on Service of Carrier Partners. CARRIER PARTNER NETWORKS ARE MADE AVAILABLE AS-IS AND MOTOROLA AND AT&T MAKES NO WARRANTIES OR REPRESENTATIONS AS TO THE AVAILABILITY OR QUALITY OF ROAMING SERVICE PROVIDED BY CARRIER PARTNERS, AND MOTOROLA AND AT&T WILL NOT BE LIABLE IN ANY CAPACITY FOR ANY ERRORS, OUTAGES, OR FAILURES OF CARRIER PARTNER NETWORKS. ROAMING ON CARRIER PARTNER NETWORKS OUTSIDE THE FIRSTNET SERVICE AREA (IF ANY) SHALL BE AVAILABLE AS DESCRIBIED IN THE SERVICE GUIDE.

User Disclosures. THE CUSTOMER UNDERSTANDS AND AGREES THAT IT: (1) HAS NO CONTRACTUAL RELATIONSHIP WITH THE UNDERLYING WIRELESS SERVICE CARRIER; (2) IS NOT A THIRD PARTY BENEFICIARY OF ANY AGREEMENT BETWEEN [CUSTOMER] AND THE UNDERLYING CARRIER; (3) THAT THE UNDERLYING CARRIER HAS NO LIABILITY OF ANY KIND TO [USER], WHETHER FOR BREACH OF CONTRACT, WARRANTY, NEGLIGENCE, STRICT LIABILITY IN TORT OR OTHERWISE; AND (4) THAT DATA TRANSMISSIONS AND MESSAGES MAY BE DELAYED, DELETED OR NOT DELIVERED, AND 911 OR SIMILAR EMERGENCY CALLS MAY NOT BE COMPLETED

Medical Devices (FDA and HIPAA Responsibilities). The Customer shall be responsible for FDA compliance as a "distributor" of the Device to its users. Except as necessary to provide the Service to the Customer, The Customer shall not convey any protected health information ("PHI") to AT&T, as that term

is defined in the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health ("HITECH") Act regulations. Motorola and/or AT&T shall not function as the Customer's business associate in rendering the Services; such Services will be limited to providing conduit or mere data transmission services to the Customer in accordance with guidance on the "conduit exception" under HIPAA. Each Party shall bear its own costs associated with regulatory compliance.

Audits. Customer may be subject to occasional audits by AT&T or its agents to verify compliance with this Exhibit A.

2. Data Processing Addendum

This Data Processing Addendum, including its Schedules and Annexes ("DPA"), forms part of the Master Purchase Agreement ("MPA" or "Agreement")) to reflect the parties' agreement with regard to the Processing of Customer Data, which may include Personal Data. In the event of a conflict between this DPA, the MPA or any Schedule, Annex or other addenda to the MPA, this DPA must prevail.

When Customer renews or purchases new Products or Services, the then-current DPA must apply and must not change during the applicable Term. When Motorola provides new features or supplements the Product or Service, Motorola may provide additional terms or make updates to this DPA that must apply to Customer's use of those new features or supplements.

1. Definitions.

All capitalized terms not defined herein must have the meaning set forth in the Agreement.

"**Customer Data**" means data including images, text, videos, and audio that are provided to Motorola by, through, or on behalf of Customer and its Authorized Users or their end users, through the use of the products and services. Customer Data does not include Customer Contact Data, Service Use Data, other than that portion comprised of Personal Information, or Third Party Data.

"Customer Contact Data" means data Motorola collects from Customer, its Authorized Users, and their end users for business contact purposes, including without limitation marketing, advertising, licensing, and sales purposes.

"Data Protection Laws" means all data protection laws and regulations applicable to a Party with respect to the Processing of Personal Data under the Agreement.

"Data Subjects" means the identified or identifiable person to whom Personal Data relates.

"Metadata" means data that describes other data.

"Motorola Data" means data owned by Motorola and made available to Customer in connection with the Products and Services.

"Personal Data" or **"Personal Information"** means any information relating to an identified or identifiable natural person transmitted to Motorola by, through, or on behalf of Customer and its Authorized Users or their end users as part of Customer Data. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Process" or **"Processing"** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, copying, analyzing, caching, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Security Incident" means an incident leading to the accidental or unlawful destruction, loss, alteration or disclosure of, or access to Customer Data, which may include Personal Data, while processed by Motorola. .

"**Service Use Data**" means data generated about the use of the Products and Services through Customer's use or Motorola's support of the Products and Services, which may include Metadata, Personal Data, product performance and error information, activity logs, and date and time of use.

"Sub-processor" means other processors engaged by Motorola to Process Customer Data which may include Personal Data.

"Third Party Data" means information obtained by Motorola from publicly available sources or its third party content providers and made available to Customer through the Products or Services.

2. Processing of Customer Data

2.1. Roles of the Parties. The Parties agree that with regard to the Processing of Personal Data hereunder, Customer is the Controller and Motorola is the Processor who may engage Sub-processors pursuant to the requirements of **Section 6** entitled "Sub-processors" below.

2.2. Motorola's Processing of Customer Data. Motorola and Customer agree that Motorola may use and Process Customer Data, including the Personal Information embedded in Service Use Data, only in accordance with Customer's documented instructions for the following purposes: (i) to perform Services and provide Products under the Agreement; (ii) analyze Customer Data to operate, maintain, manage, and improve Motorola products and services; and (iii) create new products and services. Customer agrees that its Agreement (including this DPA), along with the Product and Service Documentation and Customer's use and configuration of features in the Products and Services, are Customer's complete and final documented instructions to Motorola for the processing of Customer Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer's Agreement. Customer represents and warrants to Motorola that Customer's instructions, including appointment of Motorola as a Processor or sub-processor, have been authorized by the relevant controller. Customer Data may be processed by Motorola at any of its global locations and/or disclosed to Sub-processors. It is Customer's responsibility to notify Authorized Users of Motorola's collection and use of Customer Data, and to obtain any required consents, provide all necessary notices, and meet any other applicable legal requirements with respect to such collection and use. Customer represents and warrants to Motorola that it has complied with the terms of this provision.

2.3. Details of Processing. The subject-matter of Processing of Personal Data by Motorola hereunder, the duration of the Processing, the categories of Data Subjects and types of Personal Data are set forth on **Annex I** to this DPA.

2.4. Disclosure of Processed Data. Motorola must not disclose Customer Data to any third party except to Motorola's suppliers and channel partners as necessary to provide the products and services unless permitted under this Agreement, authorized by Customer or required by law. In the event a government or supervisory authority demands access to Customer Data, to the extent allowable by law, Motorola must provide Customer with notice of receipt of the demand to provide sufficient time for Customer to seek appropriate relief in the relevant jurisdiction. In all circumstances, Motorola retains the right to comply with applicable law.

2.5. Customer's Obligations. Customer is solely responsible for its compliance with all Data Protection Laws and establishing and maintaining its own policies and procedures to ensure such compliance. Customer must not use the Products and Services in a manner that would violate applicable Data Protection Laws. Customer must have sole responsibility for (i) the lawfulness of any transfer of Personal Data to Motorola, (ii) the accuracy, quality, and legality of Personal Data provided to Motorola; (iii) the means by which Customer acquired Personal Data, and (iv) the provision of any required notices to, and obtaining any necessary acknowledgements, authorizations or consents from Data Subjects. Customer takes full responsibility to keep the amount of Personal Data provided to Motorola to the minimum necessary for Motorola to perform in accordance with the Agreement. Customer must be solely responsible for its compliance with applicable Data Protection Laws.

2.6. Customer Indemnity. To the extent allowed by law, Customer will defend, indemnify, and hold Motorola and its subcontractors, subsidiaries and other affiliates harmless from and against any and all damages, losses, liabilities, and expenses (including reasonable fees and expenses of attorneys) arising from any actual or threatened third-party claim, demand, action, or proceeding arising from or related to

Customer's failure to comply with its obligations under this Agreement and/or applicable Data Protection Laws. Motorola will give Customer prompt, written notice of any claim subject to the foregoing indemnity. Motorola will, at its own expense, cooperate with Customer in its defense or settlement of the claim.

3. **Service Use Data**. Except to the extent that it is Personal Information, Customer understands and agrees that Motorola may collect and use Service Use Data for its own purposes, provided that such purposes are compliant with applicable Data Protection Laws. Service Use Data may be processed by Motorola at any of its global locations and/or disclosed to Sub-processors.

4. **Third-Party Data and Motorola Data**. Motorola Data and Third Party Data may be available to Customer through the Products and Services. Customer and its Authorized Users may use the Motorola Data and Third Party Data as permitted by Motorola and the applicable third-party data provider, as described in the Agreement or applicable Addendum. Unless expressly permitted in the Agreement or applicable Addendum, Customer must not, and must ensure its Authorized Users must not: (a) use the Motorola Data or Third-Party Data for any purpose other than Customer's internal business purposes or disclose the data to third parties; (b) "white label" such data or otherwise misrepresent its source or ownership, or resell, distribute, sublicense, or commercially exploit the data in any manner; (c) use such data in violation of applicable laws ; (d) use such data for activities or purposes where reliance upon the data could lead to death, injury, or property damage; (e) remove, obscure, alter, or falsify any marks or proprietary rights notices indicating the source, origin, or ownership of the data; or (f) modify such data or combine it with Customer Data or other data or use the data to build databases. Additional restrictions may be set forth in the Agreement or applicable Addendum. Any rights granted to Customer or Authorized Users with respect to Motorola Data or Third-Party Data must immediately terminate upon termination or expiration of the applicable Addendum, Ordering Document, or the MPA. Further, Motorola or the applicable Third Party Data provider may suspend, change, or terminate Customer's or any Authorized User's access to Motorola Data or Third-Party Data if Motorola or such Third Party Data provider believes Customer's or the Authorized User's use of the data violates the Agreement, applicable law or by Motorola's agreement with the applicable Third Party Data provider. Upon termination of Customer's rights to use of any Motorola Data or Third-Party Data, Customer and all Authorized Users must immediately discontinue use of such data, delete all copies of such data, and certify such deletion to Motorola. Notwithstanding any provision of the Agreement to the contrary, Motorola has no liability for Third-Party Data or Motorola Data available through the Products and Services. Motorola and its Third Party Data providers reserve all rights in and to Motorola Data and Third-Party Data not expressly granted in an Addendum or Ordering Document.

5. **Motorola as a Controller or Joint Controller.** In all instances where Motorola acts as a Controller it must comply with the applicable provisions of the Motorola Privacy Statement at https://www.motorolasolutions.com/en_us/about/privacy-policy.html#privacystatement as each may be updated from time to time. Motorola holds all Customer Contact Data as a Controller and must Process such Customer Contact Data in accordance with the Motorola Privacy Statement. In instances where Motorola is acting as a Joint Controller with Customer, the Parties must enter into a separate addendum to the Agreement to allocate the respective roles as joint controllers.

6. **Sub-processors.**

6.1. **Use of Sub-processors**. Customer agrees that Motorola may engage Sub-processors who in turn may engage Sub-processors to Process Personal Data in accordance with the DPA. A current list of Sub-processors is set forth at **Annex III**. When engaging Sub-processors, Motorola must enter into agreements with the Sub-processors to bind them to obligations which are substantially similar or more stringent than those set out in this DPA.

7. **Changes to Sub-processing**. The Customer hereby consents to Motorola engaging Sub-processors to process Customer Data provided that: (i) Motorola must use its reasonable endeavors to provide at least 10 days' prior notice of the addition or removal of any Sub-processor, which may be given by posting details of such addition or removal at a URL provided to Customer in **Annex III**; (ii) Motorola imposes data protection terms on any Sub-processor it appoints that protect the Customer Data to the

same standard provided for by this Addendum; and (iii) Motorola remains fully liable for any breach of this clause that is caused by an act, error or omission of its Sub-processor(s). The Customer may object to Motorola's appointment or replacement of a Sub-processor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, Motorola will either appoint or replace the Sub-processor or, if in Motorola's discretion this is not feasible, the Customer may suspend or terminate this Agreement. **Data Subject Requests.** Motorola must, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject, including without limitation requests for access to, correction, amendment, transport or deletion of such Data Subject's Personal Data and, to the extent applicable, Motorola must provide Customer with commercially reasonable cooperation and assistance in relation to any complaint, notice, or communication from a Data Subject. Customer must respond to and resolve promptly all requests from Data Subjects which Motorola provides to Customer. Customer must be responsible for any reasonable costs arising from Motorola's provision of such assistance under this Section. **Data Transfers**

Motorola agrees that it must not make transfers of Personal Data under this Agreement from one jurisdiction to another unless such transfers are performed in compliance with this Addendum and applicable Data Protection Laws. Motorola agrees to enter into appropriate agreements with its affiliates and Sub-processors, which will permit Motorola to transfer Personal Data to its affiliates and Sub-processors. Motorola agrees to amend as necessary its agreement with Customer to permit transfer of Personal Data from Motorola to Customer. Motorola also agrees to assist the Customer in entering into agreements with its affiliates and Sub-processors if required by applicable Data Protection Laws for necessary transfers.

8. **Security.** Motorola must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed by the Processing of Personal Data, taking into account the costs of implementation; the nature, scope, context, and purposes of the Processing; and the risk of varying likelihood and severity of harm to the data subjects. The appropriate technical and organizational measures implemented by Motorola are set forth in **Annex III**. In assessing the appropriate level of security, Motorola must weigh the risks presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise Processed.

9. **Security Incident Notification**. If Motorola becomes aware of a Security Incident, then Motorola must (i) notify Customer of the Security Incident without undue delay, (ii) investigate the Security Incident and apprise Customer of the details of the Security Incident and (iii) take commercially reasonable steps to stop any ongoing loss of Personal Data due to the Security Incident if in the control of Motorola. Notification of a Security Incident must not be construed as an acknowledgement or admission by Motorola of any fault or liability in connection with the Security Incident. Motorola must make reasonable efforts to assist Customer in fulfilling Customer's obligations under Data Protection Laws to notify the relevant supervisory authority and Data Subjects about such incident.

10. **Data Retention and Deletion**.

Except for anonymized Customer Data, as described above, or as otherwise provided under the Agreement, Motorola must delete all Customer Data no later than ninety (90) days following termination or expiration of the MPA or the applicable Addendum or Ordering Document unless otherwise required to comply with applicable law.

11. **Audit Rights**

11.1 **Periodic Audit.** Motorola will allow Customer to perform an audit of reasonable scope and duration of Motorola operations relevant to the Products and Services purchased under the Agreement, at Customer's sole expense, for verification of compliance with the technical and organizational measures set forth in **Annex II** if (i) Motorola notifies Customer of a Security Incident that results in actual compromise to the Products and/or Services purchased; or (ii) if Customer reasonably believes Motorola is not in compliance with its security commitments under this DPA, or (iii) if such audit is legally required

by the Data Protection Laws. Any audit must be conducted in accordance with the procedures set forth in **Section 11.3** of this DPA and may not be conducted more than one time per year. If any such audit requires access to confidential information of Motorola's other customers, suppliers or agents, such portion of the audit may only be conducted by Customer's nationally recognized independent third party auditors in accordance with the procedures set forth in **Section 11.3** of this DPA. Unless mandated by GDPR or otherwise mandated by law or court order, no audits are allowed within a data center for security and compliance reasons. Motorola must, in no circumstances, provide Customer with the ability to audit any portion of its software, products, and services which would be reasonably expected to compromise the confidentiality of any third party's information or Personal Data.

11.2 Satisfaction of Audit Request. Upon receipt of a written request to audit, and subject to Customer's agreement, Motorola may satisfy such audit request by providing Customer with a confidential copy of a Motorola's applicable most recent third party security review performed by a nationally recognized independent third party auditor, such as a SOC2 Type II report or ISO 27001 certification, in order that Customer may reasonably verify Motorola's compliance with national standards.

11.3 Audit Process. Customer must provide at least sixty days (60) days prior written notice to Motorola of a request to conduct the audit described in **Section 11.1**. All audits must be conducted during normal business hours, at applicable locations or remotely, as designated by Motorola. Audit locations, if not remote will generally be those location(s) where Customer Data is accessed, or Processed. The audit must not unreasonably interfere with Motorola's day to day operations. An audit must be conducted at Customer's sole cost and expense and subject to the terms of the confidentiality obligations set forth in the Agreement. Before the commencement of any such audit, Motorola and Customer must mutually agree upon the time, and duration of the audit. Motorola must provide reasonable cooperation with the audit, including providing the appointed auditor a right to review, but not copy, Motorola security information or materials provided such auditor has executed an appropriate non-disclosure agreement. Motorola's policy is to share methodology and executive summary information, not raw data or private information. Customer must, at no charge, provide to Motorola a full copy of all findings of the audit.

12. Regulation Specific Terms

12.1. HIPAA Business Associate. If Customer is a "covered entity" or a "business associate" and includes "protected health information" in Customer Data as those terms are defined in 45 CFR § 160.103, execution of the MPA includes execution of the Motorola HIPAA Business Associate Agreement Addendum ("BAA"). Customer may opt out of the BAA by sending the following information to Motorola in a written notice under the terms of the Customer's Agreement.

12.2. FERPA. If Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA), apply, Motorola acknowledges that for the purposes of the DPA, Motorola is a "school official" with "legitimate educational interests" in the Customer Data, as those terms have been defined under FERPA and its implementing regulations, and Motorola agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials. Customer understands that Motorola may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer must be responsible for obtaining any parental consent for any end user's use of the Online Service that may be required by applicable law and to convey notification on behalf of Motorola to students (or, with respect to a student under 18 years of age and not in attendance at a post-secondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data in Motorola's possession as may be required under applicable law

12.3. CJIS. Motorola agrees to support the Customer's obligation to comply with the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy and must comply with the terms of the CJIS Security Addendum for the Term of this Agreement and such CJIS Security Addendum is incorporated herein by reference. Customer hereby consents to allow Motorola "screened" personnel as defined by the CJIS Security Policy to serve as an authorized "escort" within the meaning of CJIS Security

Policy for escorting unscreened Motorola personnel that require access to unencrypted Criminal Justice Information for purposes of Tier 3 support (e.g. troubleshooting or development resources). In the event Customer requires access to Service Use Data for its compliance with the CJIS Security Policy, Motorola must make such access available following Customer's request. Notwithstanding the foregoing, in the event the MPA or applicable Ordering Document terminates, Motorola must carry out deletion of Customer Data in compliance with Section 10 herein and may likewise delete Service Use Data within the time frame specified therein. To the extent Customer objects to deletion of its Customer Data or Service Use Data and seeks retention for a longer period, it must provide written notice to Motorola prior to expiration of the 30 day period for data retention to arrange return of the Customer Data and retention of the Service Use Data for a specified longer period of time.

12.4. CCPA. If Motorola is Processing Personal Data within the scope of the California Consumer Protection Act ("CCPA"), Customer acknowledges that Motorola is a "Service Provider" within the meaning of CCPA. Motorola must process Customer Data and Personal Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in this DPA and as permitted under the CCPA, including under any "sale" exemption. In no event will Motorola sell any such data. If CCPA applies, Personal Data must also include any data identified with the CCPA definition of personal data.

13. Motorola Contact. If Customer believes that Motorola is not adhering to its privacy or security obligations hereunder, Customer must contact the Motorola Data Protection Officer at Motorola Solutions, Inc., 500 W. Monroe, Chicago, IL USA 90661-3618 or at privacy1@motorolasolutions.com.

ANNEX I

A. LIST OF PARTIES

1. **Data exporter(s):** Customer

   Role (controller/processor): Controller

2. **Data importer(s):** Motorola Solutions, Inc.

   Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data subjects include the data exporter's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by data importer. Motorola acknowledges that, depending on Customer's use of the Online Service, Customer may elect to include personal data from any of the following types of data subjects in the Customer Data:

- Employees, contractors, and temporary workers (current, former, prospective) of data exporter;
- Dependents of the above;
- Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of data exporter's services;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter;
- Stakeholders or individuals who passively interact with data exporter (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the data exporter);
- Minors; or
- Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).

Categories of personal data transferred

Customer's use of the Products and Services, Customer may elect to include personal data from any of the following categories in the Customer Data:

- Basic personal data (for example place of birth, street name, and house number (address), Agreement code, city of residence, country of residence, mobile phone number, first name, last

name, initials, email address, gender, date of birth), including basic personal data about family members and children;

- Authentication data (for example user name, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
- Commercial Information (for example history of purchases, special offers, subscription information, payment history);
- Biometric Information (for example DNA, fingerprints and iris scans);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of Wi-Fi access points);
- Photos, video, and audio;
- Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);
- Device identification (for example IMEI-number, SIM card number, MAC address);
- Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location, and organizations);
- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);
- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;
- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of

uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or

- Any other personal data identified under applicable law or regulation.

Sensitive data transferred *(if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

The frequency of the transfer *(e.g. whether the data is transferred on a one-off or continuous basis).*

Data may be transferred on a continuous basis during the term of the MPA or other agreement to which this DPA applies.

Nature of the processing

The nature, scope and purpose of processing personal data is to carry out performance of Motorola's obligations with respect to provision of the Products and Services purchased under the MPA and applicable Ordering Documents. The data importer utilizes a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors utilize such facilities

Purpose(s) of the data transfer and further processing

The nature, scope and purpose of processing personal data is to carry out performance of Motorola's obligations with respect to provision of the Products and Services purchased under the MPA and applicable Ordering Documents. The data importer utilizes a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors utilize such facilities

The period for which the personal data will be retained, *or, if that is not possible, the criteria used to determine that period*

Data retention is governed by Section 10 of this Data Processing Addendum

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Transfers to sub-processors will only be for carrying out the performance of Motorola's obligations with respect to provision of the Products and Services purchased under the MPA and applicable Ordering Documents. The data importer utilizes a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors utilize such facilities. In accordance with the DPA, the data exporter agrees the data importer may hire other companies to provide limited services on data importer's behalf, such as providing customer support. Any such sub-processors must be permitted to obtain Customer Data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Customer Data for any other purpose.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Measures of pseudonymization and encryption of personal data

Where technically feasible and when not impacting services provided:

- We minimize the data we collect to information we believe is necessary to communicate, provide, and support products and services and information necessary to comply with legal obligations.
- We encrypt in transit and at rest.
- We pseudonymize and limit administrative accounts that have access to reverse pseudonymization.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

In order to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services, Motorola Solutions Information Protection policy mandates the institutionalization of information protection throughout solution development and operational lifecycles. Motorola Solutions maintains dedicated security teams for its internal information security and its products and services. Its security practices and policies are integral to its business and mandatory for all Motorola Solutions employees and contractors The Motorola Chief Information Security Officer maintains responsibility and executive oversight for such policies, including formal governance, revision management, personnel education and compliance. Motorola Solutions generally aligns to the NIST Cyber Security Framework as well as ISO 27001.

Some of the system configuration is under the control of the customer.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Security Incident Procedures Motorola Solutions maintains a global incident response plan to address any physical or technical incident in an expeditious manner. Motorola maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. For each security breach that is a Security Incident, notification will be made in accordance with the Security Incident Notification section of this DPA.

Business Continuity and Disaster Preparedness Motorola maintains business continuity and disaster preparedness plans for critical functions and systems within Motorola's control that support the Products and Services purchased under the Agreement in order to avoid services disruptions and minimize recovery risks.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Motorola periodically evaluates its processes and systems to ensure continued compliance with obligations imposed by law, regulation or contract with respect to the confidentiality, integrity, availability, and security of Customer Data, including personal information. Motorola documents the results of these evaluations and any remediation activities taken in response to such evaluations. Motorola periodically has third party assessments performed against applicable industry standards, such as ISO 27001, 27017, 27018 and 27701.

Measures for user identification and authorization

Identification and Authentication. Motorola uses industry standard practices to identify and authenticate users who attempt to access Motorola information systems. Where authentication mechanisms are based on passwords, Motorola requires that the passwords are at least eight characters long and are changed regularly. Motorola uses industry standard password protection practices, including practices designed to

maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

Access Policy and Administration. Motorola maintains a record of security privileges of individuals having access to Customer Data, including personal information. Motorola maintains appropriate processes for requesting, approving and administering accounts and access privileges in connection with the Processing of Customer Data. Only authorized personnel may grant, alter or cancel authorized access to data and resources. Where an individual has access to systems containing Customer Data, the individuals are assigned separate, unique identifiers. Motorola deactivates authentication credentials on a periodic basis.

Measures for the protection of data during transmission

Data is generally encrypted during transmission within the Motorola managed environments. Encryption in transit is also generally required of any sub-processors. Further, protection of data in transit is also achieved through the access controls, physical and environmental security, and personnel security described throughout this Annex II.

Measures for the protection of data during storage

Data is generally encrypted during storage within the Motorola managed environments. Encryption in storage is also generally required of any sub-processors. Further, protection of data in storage is also achieved through the access controls, physical and environmental security, and personnel security described throughout this Annex II.

Measures for ensuring physical security of locations at which personal data are processed

Motorola maintains appropriate physical and environment security controls to prevent unauthorized access to Customer Data, including personal information. This includes appropriate physical entry controls to Motorola facilities such as card-controlled entry points, and a staffed reception desk to protect against unauthorized entry. Access to controlled areas within a facility will be limited by job role and subject to authorized approval. Use of an access badge to enter a controlled area will be logged and such logs will be retained in accordance with Motorola policy. Motorola revokes personnel access to Motorola facilities and controlled areas upon separation of employment in accordance with Motorola policies. Motorola policies impose industry standard workstation, device and media controls designed to further protect Customer Data, including personal information.

Measures for ensuring personnel security

Access to Customer Data. Motorola maintains processes for authorizing and supervising its employees, and contractors with respect to monitoring access to Customer Data. Motorola requires its employees, contractors and agents who have, or may be expected to have, access to Customer Data to comply with the provisions of the Agreement, including this Annex and any other applicable agreements binding upon Motorola.

Security and Privacy Awareness. Motorola must ensure that its employees and contractors remain aware of industry standard security and privacy practices, and their responsibilities for protecting Customer Data and Personal Data. This must include, but not be limited to, protection against malicious software, password protection, and management, and use of workstations and computer system accounts. Motorola requires periodic Information security training, privacy training, and business ethics training for all employees and contract resources

Sanction Policy. Motorola maintains a sanction policy to address violations of Motorola's internal security requirements as well as those imposed by law, regulation, or contract.

Background Checks. Motorola follows its standard mandatory employment verification requirements for all new hires. In accordance with Motorola internal policy, these requirements must be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation and any additional checks as deemed necessary by Motorola.

Measures for ensuring events logging

Motorola maintains policies requiring continuous monitoring and event logging on all production information resources. Application audit trail logs must be captured on all production Motorola information resources. Audit trail logs of production Motorola information resources are regularly reviewed and appropriate remedial actions are taken when necessary.

Measures for ensuring system configuration, including default configuration

Motorola on-site systems are provided with a default secure configuration that may require Customer input to complete the secure configuration. For example, some default configurations must be changed by the Customer to maintain a secure system (e.g., default usernames and passwords, connecting to active directory, etc.). This completion of the default secure configuration is dependent on the Customer input for transitioning from the default secure configuration to a secure configuration.

Measures for internal IT and IT security governance and management

The Motorola Solutions Enterprise Information Security organization is structured as follows: Governance/ Risk/ Compliance, Threat Intelligence & Vulnerability Management, Detection, Protection, and Response. Motorola assesses organization's effectiveness annually via external assessors who report and share the assessment findings with Motorola Audit Services who tracks any identified remediations. For more information, please see the Motorola Trust Center at https://www.motorolasolutions.com/en_us/about/trust-center/security.html

Measures for certification/assurance of processes and products

Motorola performs internal Secure Application Review and Secure Design Review security audits and Production Readiness Review security readiness reviews prior to service release. Where appropriate, privacy assessments are performed for Motorola's products and services. A risk register is created as a result of internal audits with assignments tasked to appropriate personnel. Security audits are performed annually with additional audits as needed. Additional privacy assessments, including updated data maps, occur when material changes are made to the products or services. Further, Motorola Solution has achieved AICPA SOC2 Type 2 reporting and ISO/IEC 27001:2013 certification for many of its development and support operations.

Measures for ensuring data minimization

Motorola Solutions policies require processing of all personal information in accordance with applicable law, including when that law requires data minimization. Further, Motorola Solutions conducts privacy assessments of its products and services and evaluates if those products and services support the principles of processing, such as data minimization.

Measures for ensuring data quality

Motorola Solutions policies require processing of all personal information in accordance with applicable law, including when that law requires ensuring the quality and accuracy of data. Further, Motorola Solutions conducts privacy assessments of its products and services and evaluates if those products and services support the principles of processing, such as ensuring data quality.

Measures for ensuring limited data retention

Motorola Solutions maintains a data retention policy that provides a retention schedule outlining storage periods for personal data. The schedule is based on business needs and provides sufficient information to identify all records and to implement disposal decisions in line with the schedule. The policy is periodically reviewed and updated.

Measures for ensuring accountability

To ensure compliance with the principle of accountability, Motorola Solutions maintains a Privacy Program which generally aligns its activities to both the Nymity Privacy Management and Accountability Framework and NIST Privacy Framework. The Privacy Program is audited annually by Motorola Solutions Audit Services.

Measures for allowing data portability and ensuring erasure

When subject to a data request to move, copy or transfer their personal data, Motorola Solutions will provide personal data to the Controller in a structured, commonly used and machine readable format. Where possible and if the Controller requests it, Motorola Solutions can directly transmit the personal information to another organization.

***For transfers to (sub-) processors**, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.*

If, in the course of providing products and services under the MPA, Motorola Solutions transfers information containing personal data to third parties, said third parties will be subjected to a security assessment and bound by obligations substantially similar, but at least as stringent, as those included in this DPA.

ANNEX III

LIST OF SUB-PROCESSORS

Not Applicable

MOTOROLA SOLUTIONS

Attachment A

Interface Specification Documents

State-of-the-Art Technology for a Safe and Resilient Community

September 12, 2022

St. Johns County, FL

Table of Contents

Attachment A

Interface Specification Documents

A.1 PremierOne CAD - Third-Party Mobile Client API Interface

A.1.1 Interface Description

A.1.1.1 Introduction

This Interface Specification Document (ISD) provides a description of the capabilities of PremierOne Third-Party Mobile Client API Interface (Interface) and the scope of work involved in delivering this Interface. Motorola Solutions will deploy the Interface and verify the functionality described in this ISD. If Customer desires any changes to this ISD scope, those changes can be addressed via the change provision of the contract.

A.1.1.2 Interface Overview

The Interface defines communication between PremierOne CAD/Mobile Client and a third-party vendor desiring to extract CAD information, such as person or vehicle information, for use in an external client running on the CAD Mobile Data Terminal. Motorola Solutions provides an Application Programming Interface (API) to meet this requirement.

The Interface is designed to assist developers with technical aspects of how third party external systems consume PremierOne query response and CAD Incident data. There are two mechanisms for extracting data, either by ***Request*** or by ***Subscription***. Both methods are defined in the API.

Figure A-1 shows the connectivity and primary data flow across the system.

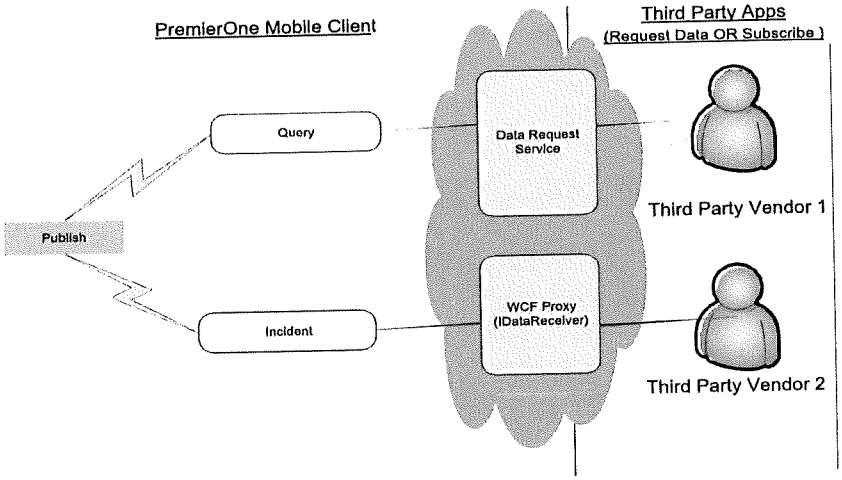


Figure A-1: Third-Party Mobile Client API Interface Diagram

Information required for installation, configuration, test and support purposes regarding this Interface will be gathered during the ISD review.

A.1.1.3 Data Exchange

The Data Elements and Exchange process are defined in the PremierOne Mobile Client API.

A.1.1.4 Business Process

None.

A.1.1.5 User Experience

Table A-1 below describes the user experience for both methods of implementing the Interface.

Table A-1: User Experience

Step	User Action	Interface Action System Behavior	Notes
1	Start the PremierOne Mobile client and log onto PremierOne	The user is logged on to the PremierOne Mobile client and the Interface is ready for requests.	The API is not available until the PremierOne Mobile client is started and the PremierOne user is logged into PremierOne Mobile client.
2	Start the Third-Party Application and enter the PremierOne User ID	For Subscription data, third-party applications register with PremierOne using the WCF API hosted by PremierOne. Third-party applications are required to provide the active logged-on PremierOne user's User ID via the API in addition to the third-party	The registration is required only for "By Subscription" data.

Step	User Action	Interface Action System Behavior	Notes
		authentication information of User ID and password.	
3	Submit a Query on the PremierOne Mobile Client	• The query is sent to the external systems via the PremierOne server. • The query result messages are returned to the PremierOne Mobile client. • The query result messages are forwarded to registered applications or available for using a "By Request" query.	PremierOne stops forwarding messages for "By Subscription" applications if there is any error accessing the third party hosted WCF service.
4	The unit is Dispatched to an Incident	• The Mobile client receives the dispatch information. • The dispatch (incident) information is forwarded to registered applications or available for a "By Request" query.	
5	Start a Crash Report or Case Report on the External Application	• Third party application presents the data received from PremierOne and pre-populates the form.	The exact user experience might be different depending on the implementation by the external application.
6	Close the External Applications	• Registered external applications unregisters with PremierOne using the API. • External applications exit.	
7	Logoff from the PremierOne Mobile Client	The Interface is disabled. All the "By Subscription" registrations are discarded.	
8	Close the PremierOne Mobile Client	PremierOne Mobile client exits.	

A.1.1.6 Use Cases

Use Cases describe specific user and system interactions provided by the Interface. They provide traceability for the Test Cases in the Interface Test Procedure.

Table A-2: Use Cases

Use Cases	Description
UC-01	Start third-party application. • Client authenticates. [SUBSCRIPTION Implementation Only].

Use Cases	Description
UC-02	Submit a query in PremierOne CAD. • The query is sent to the external systems via the PremierOne server. • The query result messages are returned to the PremierOne Mobile client. • The query result messages are forwarded to registered applications or available for using a "By Request" query.
UC-03	The unit is dispatched to an Incident. • The Mobile client receives the dispatch information. • The dispatch (incident) information is forwarded to registered applications or available for a "By Request" query.
UC-04	Start a Crash report or Case Report on the external application. • Third party application presents the data received from PremierOne and pre-populates the form.

A.1.2 Operational Considerations

A.1.2.1 Connectivity

Connectivity needs to be established between PremierOne CAD and the Interface over the Customer Enterprise Network.

The communication is handled via client-based protocols including Microsoft .NET, WCF, and XML. No external network connectivity is required for this Interface.

A.1.2.2 Exception Handling and Logging

PremierOne exceptions are logged in both the Windows Event Log on the application server and the PremierOne database.

A.1.2.3 Security

There are no additional security requirements for the Interface, beyond the standard implementation for PremierOne CAD.

A.1.2.4 Performance

There are no explicit performance requirements for the Interface.

A.1.2.5 High Availability and Disaster Recovery

There are no additional High Availability or Disaster Recovery requirements for the Interface, beyond the standard implementation for PremierOne CAD.

A.1.2.6 System Administration

Customer is responsible for contacting Motorola Solutions when changes occur in the Interface or Customer Enterprise Network, which might affect the Interface.

Customer is responsible for keeping the reference data synchronized between PremierOne and the Interface system.

A.1.3 Statement of Work

A.1.3.1 Overview

This section defines the principal activities and responsibilities of Motorola Solutions and the Customer, during the interface deployment. This Statement of Work provides understanding of the work required by all parties for the interface implementation.

Motorola Solutions assumes no responsibility for training, installation, configuration, on-going support or warranty for any third-party systems and/or software not included as part of the contracted solution.

A.1.3.2 Responsibilities

Motorola Solutions Responsibilities

- Conduct an ISD review session with the Customer subject matter experts to obtain details regarding the Interface.
- Implement the Interface.
- Provide the customer with the PremierOne Mobile Client API.
- Provide remote support, up to 40 hours, to assist the Customer and third-party vendor with deploying this API.
- Provide guidance on hardware, software and network connectivity that may be required of Customer to support the interface implementation use and maintenance, prior to implementation.
- Conduct a functional demonstration validating the Interface works in accordance with this ISD.

Customer Responsibilities

- Participate in the ISD review session and provide details required for interface installation, configuration, test and support.
- Familiarize themselves with this ISD.
- Provide all hardware, software and network connectivity not specifically provided by Motorola Solutions, prior to implementation.
- Procure all customer third-party licenses and API documentation, as required.
- The customer's third-party system must be on a version supported by the customer third-party. Customer will procure any required upgrades.
- Coordinate Customer third-party involvement with the implementation and testing of the Interface, as required.
- Witness the functional demonstration of the Interface.
- Protect the Enterprise Network against unauthorized access.
- Provide secure connections between PremierOne and the Interface.
- Manage customer third-party responsibilities to completion, as applicable, enabling Motorola Solutions to complete its responsibilities.

- Manage communication between Motorola Solutions and Customer third-party, enabling Motorola Solutions to complete its responsibilities.

A.1.3.3 Implementation Plan

Table A-3: Implementation Plan

Task	Owner
Provide PremierOne Mobile Client API.	Motorola Solutions
Develop the application per the PremierOne Mobile Client API.	Third-party vendor
Coordinate development of the third-party vendor application and testing.	Customer

A.2 PremierOne CAD - SMTP Notification Interface

A.2.1 Interface Description

A.2.1.1 Introduction

This Interface Specification Document (ISD) provides a description of the capabilities of PremierOne CAD and Customer Mail Relay Server and the scope of work involved in delivering this interface. Motorola Solutions will deploy the interface and verify the functionality described in this ISD. If Customer desires any changes to this ISD scope, those changes can be addressed via the change provision of the contract.

A.2.1.2 Interface Overview

The Simple Mail Transfer Protocol (SMTP) Interface (Interface) enables PremierOne CAD to send email messages to non-PremierOne recipients on external domains. This Interface also allows PremierOne CAD to send text messages to mobile devices, if the mobile carrier has an SMS gateway to receive emails. PremierOne CAD can be provisioned to send system generated emails or PremierOne user can send ad-hoc emails to external recipients.

PremierOne uses Microsoft Internet Information Services (IIS) SMTP Virtual Server to send messages internally between PremierOne users. The SMTP Virtual Server is connected to the Customer mail relay server. It will forward messages addressed to non-PremierOne recipients to the Customer mail relay server, which will handle these messages. The Customer mail relay server will forward messages addressed to Short Message Service (SMS/Text message) user to the appropriate SMS gateway of the service provider.

Figure A-2 shows the connectivity and primary data flow across the system.

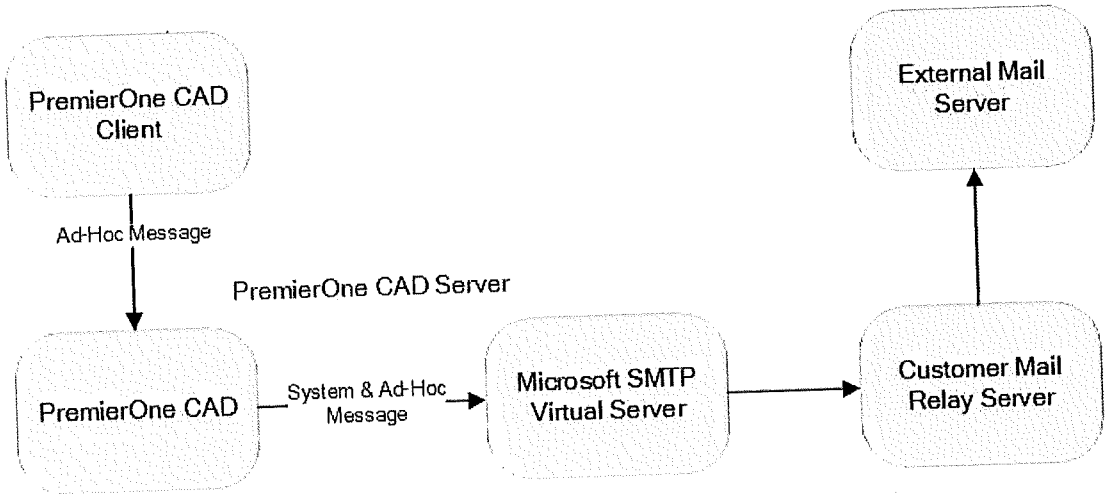


Figure A-2: SMTP Outbound Interface Diagram

The Interface can be configured to receive email messages from external mail servers. This is not in scope of the SMTP interface implementation. Inbound emails from external domains is identified as a security risk, as it can infect PremierOne or be utilized to spam the PremierOne system. If this feature is desired by the Customer, Motorola Solutions will provide it as a change order for Customer consideration.

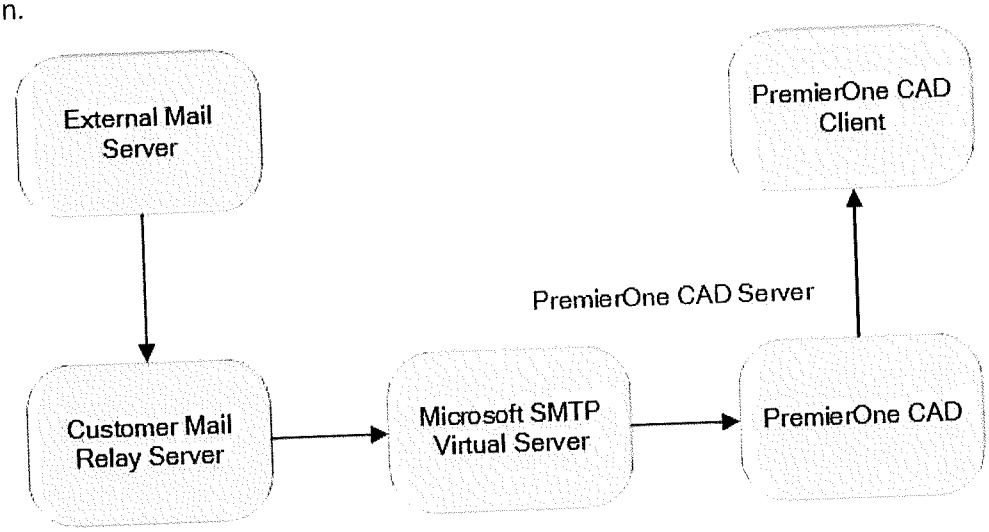


Figure A-3: SMTP Inbound Interface Diagram

Information required for installation, configuration, test and support purposes regarding this Interface will be gathered during the ISD review.

A.2.1.3 Data Exchange

The SMTP Virtual Server and Customer mail relay server handles the message exchange. Any domain may be specified in PremierOne CAD; however, the Customer mail relay server may block domains.

The data flow diagram captures the events, triggers and message exchange between the systems.

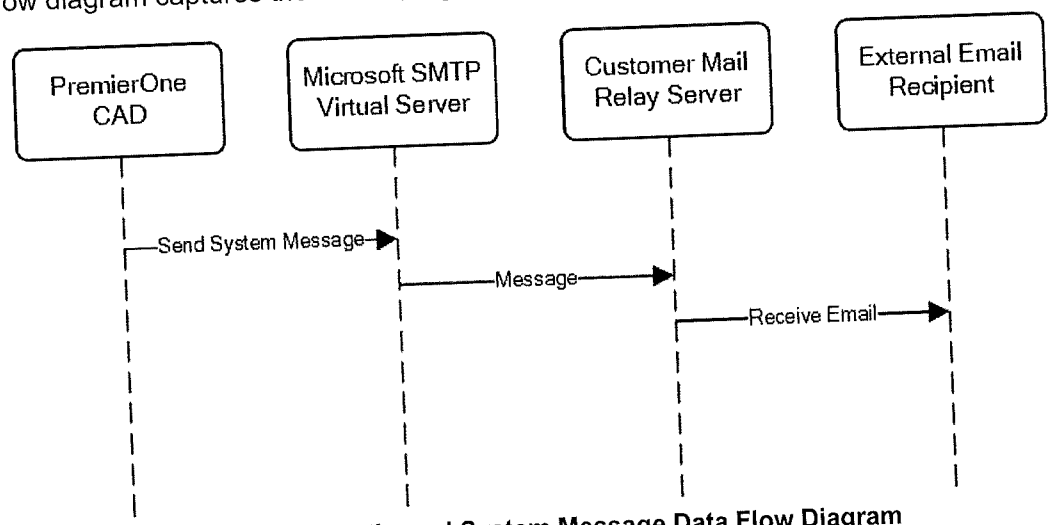


Figure A-4: Outbound System Message Data Flow Diagram

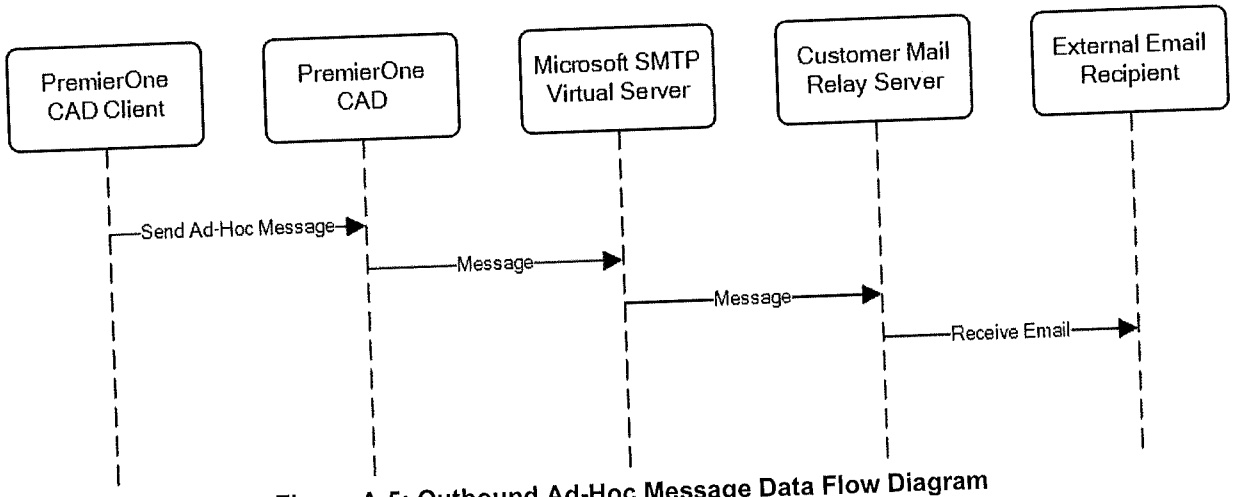


Figure A-5: Outbound Ad-Hoc Message Data Flow Diagram

PremierOne CAD user can receive email messages sent by an external user, if the Interface is configured to receive incoming messages.

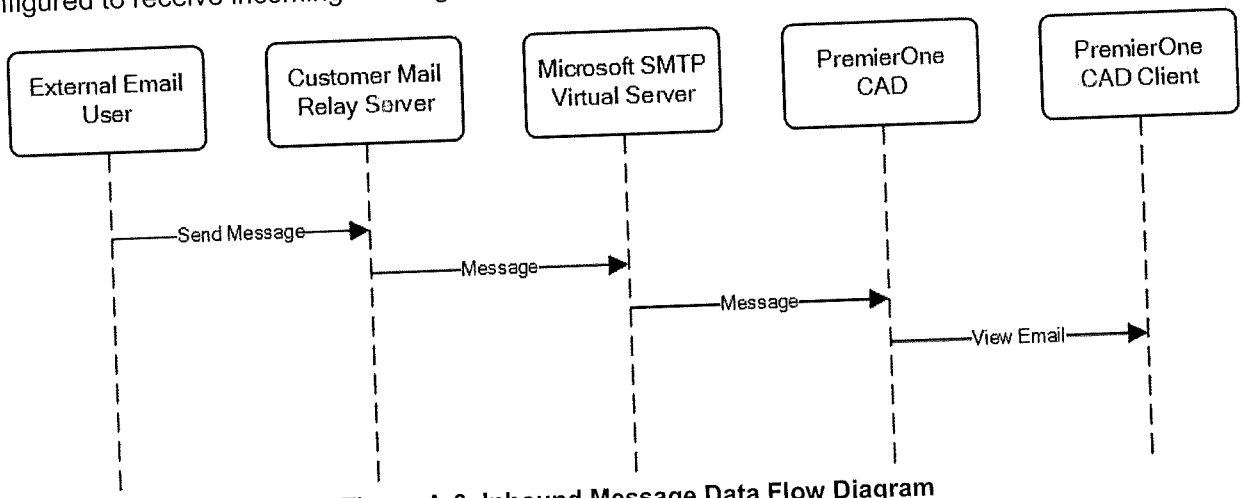


Figure A-6: Inbound Message Data Flow Diagram

A.2.1.4 Business Process

None.

A.2.1.5 User Experience

Alerting or Incident Notification feature in PremierOne CAD can be used to send system messages. PremierOne can send email messages to dispatched units, based on the alerting scheme provisioned in PremierOne CAD. The incident notification feature allows PremierOne to notify users based on the incident data. The message format can be configured in the Email Format Configuration and the message can be provisioned to include details about the incident.

PremierOne CAD user can send ad-hoc email messages to non-PremierOne recipients using the Messages form and standard email address.

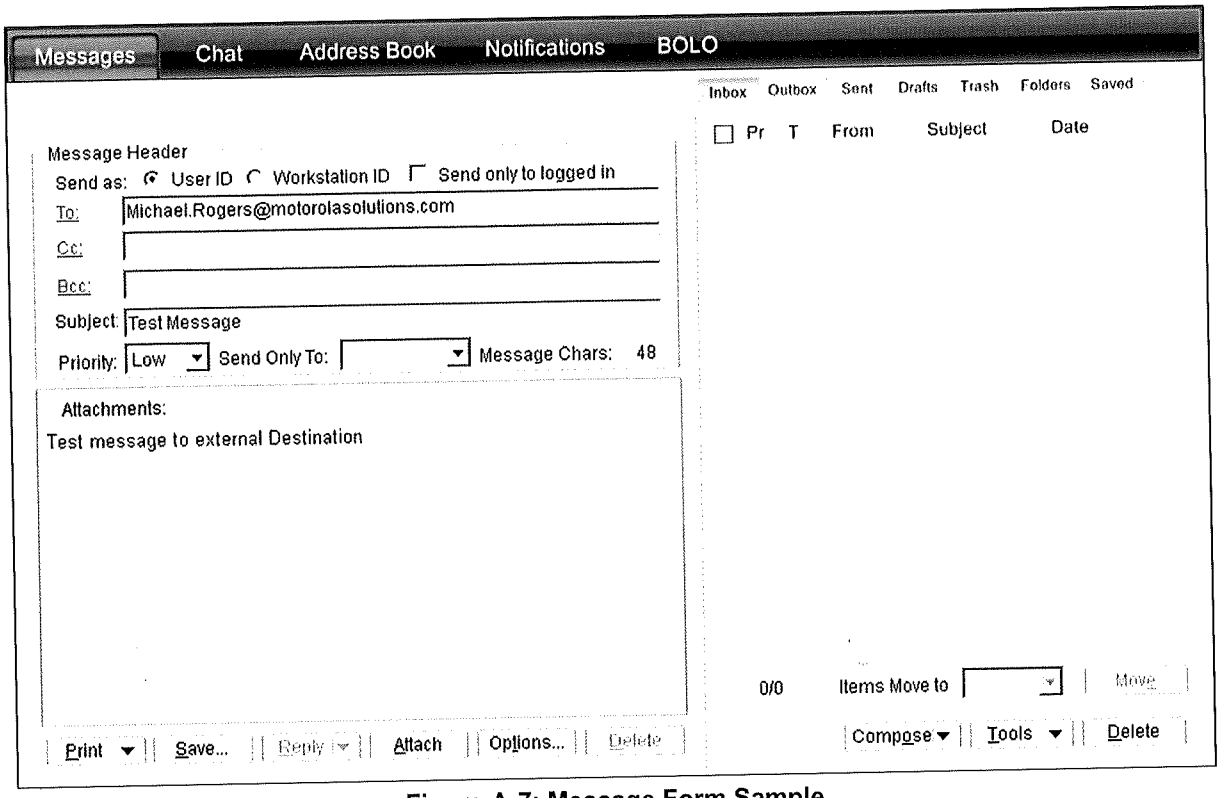


Figure A-7: Message Form Sample

A.2.1.6 Use Cases

Use Cases describe specific user and system interactions provided by the Interface. They provide traceability for the Test Cases in the Interface Test Procedure.

Table A-4: Use Cases

Use Cases	Description
UC-01	PremierOne system can send emails to external recipients.
UC-02	PremierOne user can send emails to external recipients.
UC-03	PremierOne system can receive emails from external users (optional feature).
UC-04	PremierOne user can view emails from external users (optional feature).

A.2.2 Operational Considerations

A.2.2.1 Connectivity

Connectivity needs to be established between PremierOne and the Customer mail relay server over the Customer Enterprise Network.

A.2.2.2 Exception Handling and Logging

PremierOne exceptions are logged in both the Windows Event Log on the application server and the PremierOne database.

Mail delivery exceptions will be logged by the Customer mail relay server.

A.2.2.3 Security

Receiving inbound messages from external domains is identified as a security risk, as it can infect PremierOne or be utilized to spam the PremierOne system. Motorola Solutions recommends against configuring the Interface to accept inbound messages from external systems. If the Customer chooses to receive inbound messages, the Customer accepts all risks associated with receiving inbound emails by the Interface.

A.2.2.4 Performance

There are no explicit performance requirements for the Interface.

A.2.2.5 High Availability and Disaster Recovery

There are no additional High Availability or Disaster Recovery requirements for the Interface, beyond the standard implementation for PremierOne CAD.

The Interface will be configured on the PremierOne recovery servers, if one is available.

A.2.2.6 System Administration

Customer is responsible for contacting Motorola Solutions when changes occur in the Customer Mail Relay Server or Customer Enterprise Network, which might affect the Interface.

Customer is responsible for contacting Motorola Solutions when Mail Relay address changes.

A.2.3 Statement of Work

A.2.3.1 Overview

This section defines the principal activities and responsibilities of Motorola Solutions and the Customer, during the interface deployment. This Statement of Work provides understanding of the work required by all parties for the interface implementation.

Motorola Solutions assumes no responsibility for training, installation, configuration, on-going support or warranty for any third-party systems and/or software not included as part of the contracted solution.

A.2.3.2 Responsibilities

Motorola Solutions Responsibilities

- Conduct an ISD review session with the Customer subject matter experts to obtain details regarding the Customer mail relay server connection, permissible external domains, system email formatting, alerting and notification scheme.
- Implement the Interface and configure for outbound mail operation with a single Customer mail relay server.
- Provide guidance on hardware, software and network connectivity that may be required of Customer to support the interface implementation use and maintenance, prior to implementation.
- Conduct a functional demonstration validating the Interface works in accordance with this ISD.

Customer Responsibilities

- Participate in the ISD review session and provide details required for interface installation, configuration, test and support.
- Coordinate with email service provider to determine any necessary changes required to support the additional volume required for the Interface.
- Familiarize themselves with this ISD.
- Provide all hardware, software and network connectivity not specifically provided by Motorola Solutions, prior to implementation.
- The customer's third-party system must be on a version supported by the customer third-party. Customer will procure any required upgrades.
- Witness the functional demonstration of the Interface.
- Protect the Enterprise Network against unauthorized access.
- Provide secure connections between PremierOne and the Interface.
- Manage customer third-party responsibilities to completion, as applicable, enabling Motorola Solutions to complete its responsibilities.
- Manage communication between Motorola Solutions and Customer third-party, enabling Motorola Solutions to complete its responsibilities.

A.2.3.3 Implementation Plan

Table A-5: Implementation Plan

Task	Owner
Configure SMTP Virtual Server on PremierOne servers.	Motorola Solutions
Establish network connectivity between PremierOne and the Customer Mail Relay Server.	Customer
Provision PremierOne CAD to direct outbound mails to the Customer Mail Relay Server.	Motorola Solutions
Configure the Interface in PremierOne CAD for outbound mail.	Motorola Solutions

Task	Owner
Configure Customer Mail Relay Server to accept and forward outbound mails from PremierOne CAD.	Customer
Provision Alerting Scheme, Incident Notification and Email Formatting for System Message in PremierOne CAD.	Customer / Motorola Solutions
Provision PremierOne CAD to receive inbound mails from the Customer Mail Relay Server (optional feature).	Motorola Solutions
Configure the Interface in PremierOne CAD for inbound mail (optional feature).	Motorola Solutions
Configure Customer Mail Relay Server to forward inbound mails to PremierOne CAD (optional feature).	Customer

A.3 PremierOne™ Suite - State Query Interface

A.3.1 Interface Description

A.3.1.1 Introduction

This Interface Specification Document (ISD) provides a description of the capabilities of PremierOne Suite State Query Interface (Interface) and the scope of work involved in delivering this Interface. Motorola Solutions will deploy the Interface and verify the functionality described in this ISD. If Customer desires any changes to this ISD scope, those changes can be addressed via the change provision of the contract.

A.3.1.2 Interface Overview

The Interface allows PremierOne users to submit transactions to State and Federal systems, via the State Message Switch. These transactions are most typically ones that perform inquiries, although transactions that enter, modify, locate, and clear information are also possible.

The State Message Switch provides links to State systems like Department of Motor Vehicles (DMV) and national law enforcement systems like National Crime Information Center (NCIC).

Query requests made on PremierOne CAD, Records or Mobile clients are routed to one of the PremierOne application servers. The PremierOne Query Service processes the request and determines which data source(s) can fulfill the request. This information is then passed to the PremierOne Common Services Interface (CSI) component, which translates the request to XML messages and passes it on to the CommSys ConnectCIC. ConnectCIC handles the State connection and translates the messages to the query strings required by the State. The State Message Switch forwards the request to the appropriate system.

When a response is received, ConnectCIC parses and returns the response to CSI as an XML message. CSI parses the response and forwards it to PremierOne Messaging Service, which handles the routing of the query response to the requestor.

Figure A-8 shows the connectivity and primary data flow across the system.

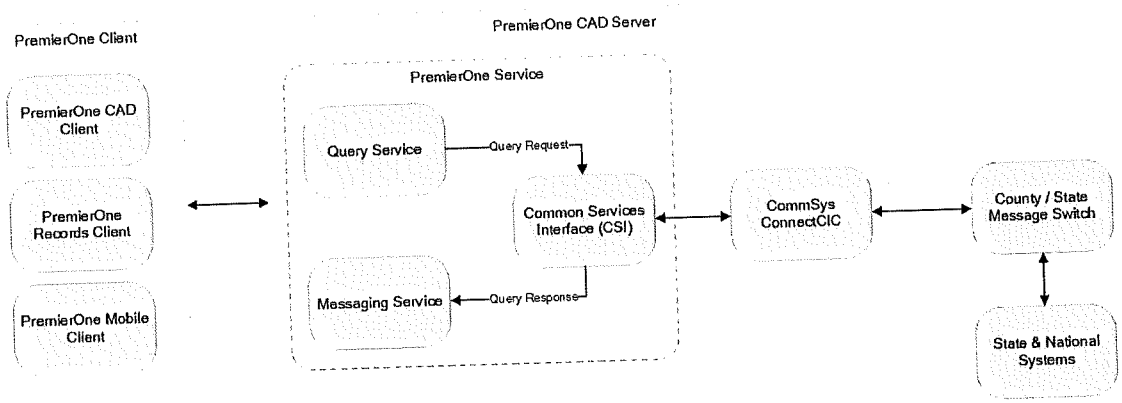


Figure A-8: State Query Interface Diagram

Information required for installation, configuration, test and support purposes regarding this State Query Interface will be gathered during the ISD review.

A.3.1.3 Data Exchange

PremierOne services and CommSys ConnectCIC manage the data transformation and exchange process. The State Message Switch may direct a single query request to multiple systems, and each system will provide its own response.

The data flow diagram captures the events, triggers and message exchange between the systems.

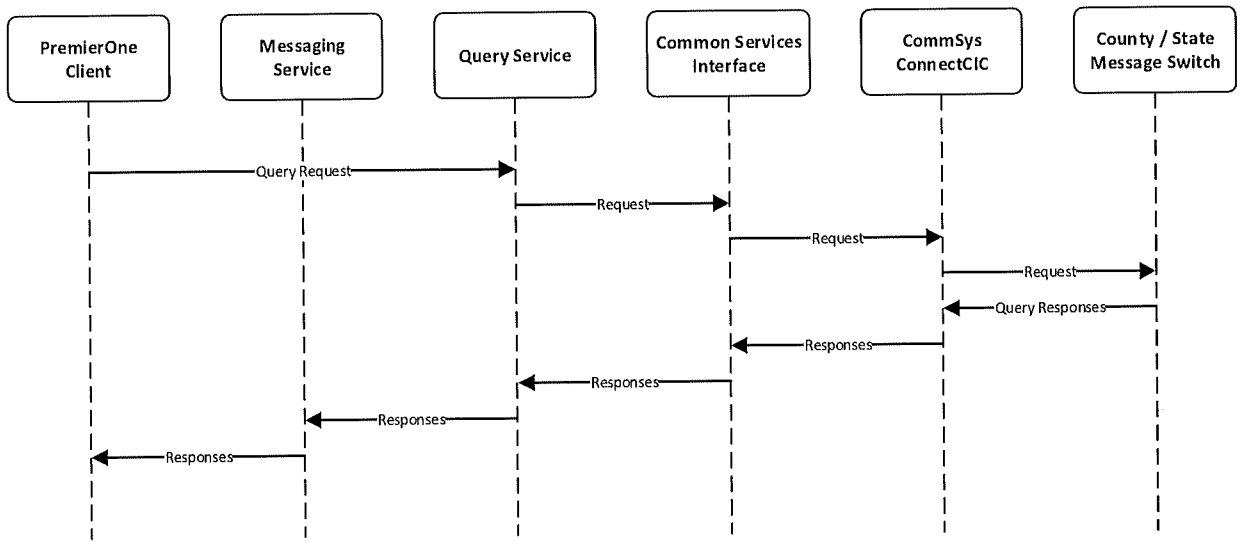


Figure A-9: State Query Data Flow Diagram

A.3.1.4 Business Process

None.

A.3.1.5 User Experience

PremierOne user can select a query type, enter the required query parameters and submit the query using a Query Request form similar to the sample in Figure A-10. The same query forms are available throughout the PremierOne Suite; CAD, Records and Mobile client. User access to the query forms is managed by the user roles provisioned in PremierOne.

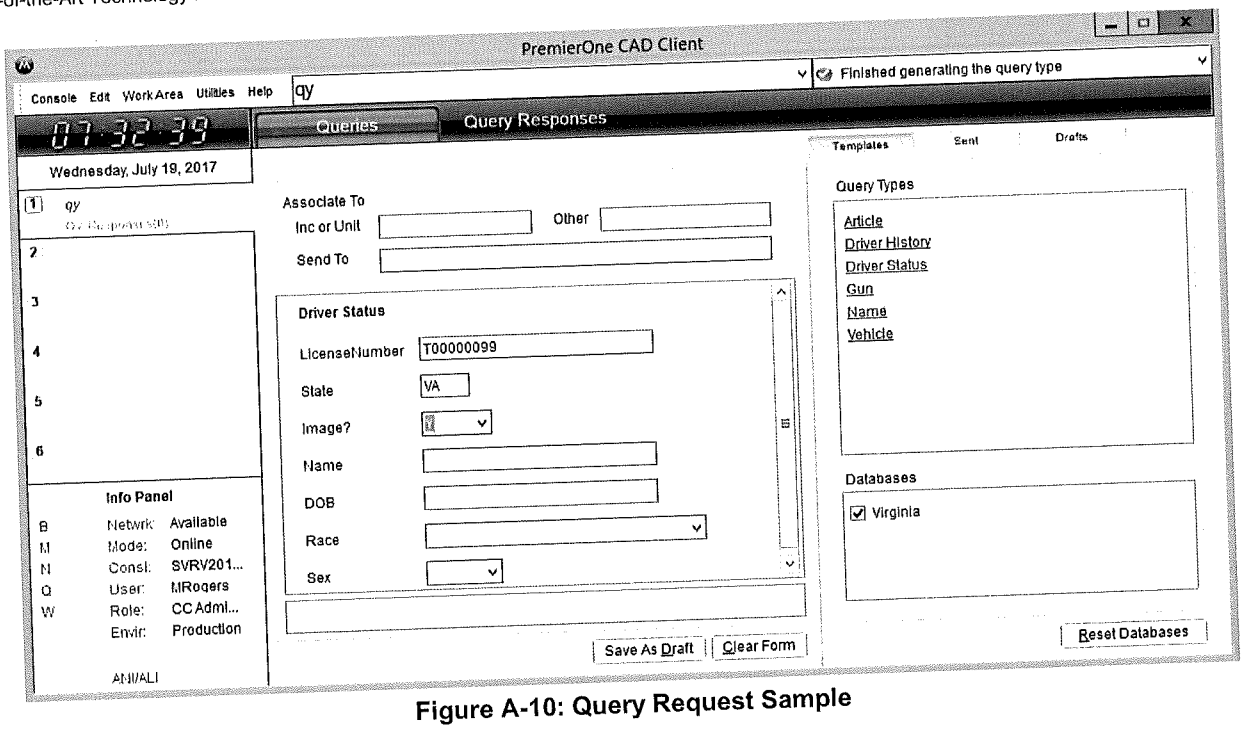


Figure A-10: Query Request Sample

PremierOne administrator may also create a command line version of a query form, similar to Figure A-11 command line query sample. This allows users to quickly submit frequently used queries. The administrator may also configure the system so queries can be submitted using person and vehicle information entered in an incident.

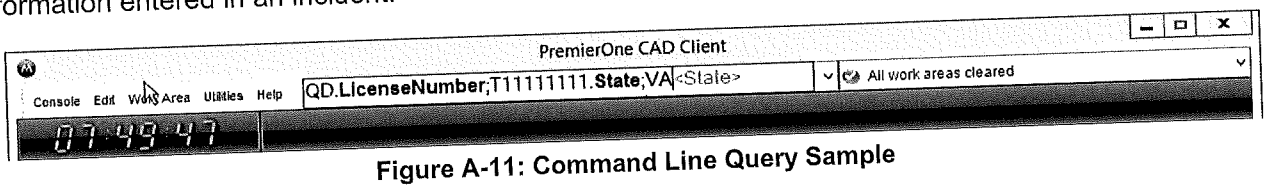


Figure A-11: Command Line Query Sample

Query Request forms are built upon the underlying data supplied by the External System. A form could use one or more underlying data sources. Thus, query responses from a particular form could be from multiple data sources.

Query responses are displayed in the Query Responses tab of the query window similar to the sample in Figure A-12. They may also be displayed in a dedicated window outside of the main CAD client window.

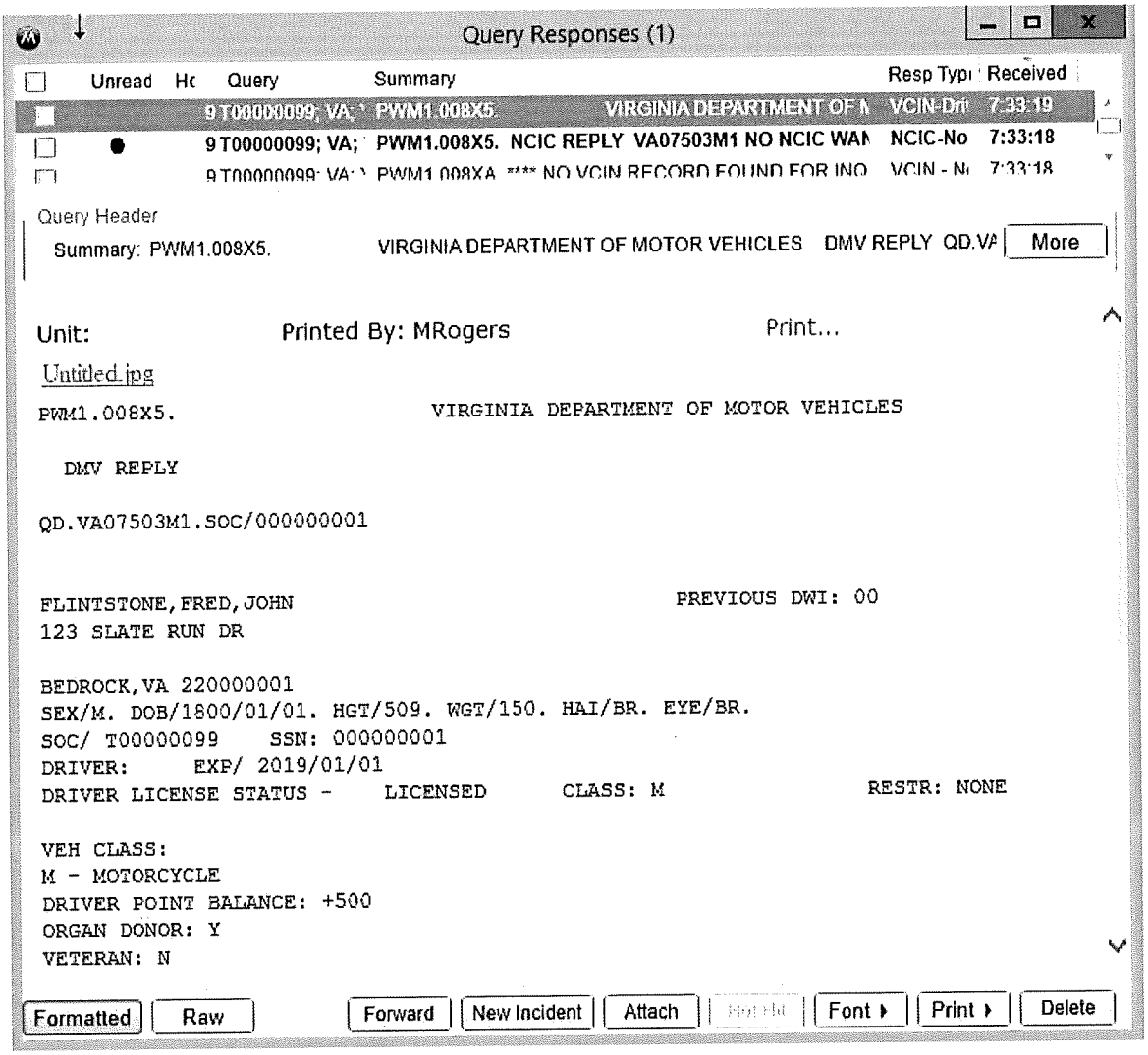


Figure A-12: Query Response Sample

In most States, the query response sent back from the State Message Switch is a block of text. This text will be displayed to the user. Certain responses may be parsed, by ConnectCIC, which involves examining the response and determining where certain key data such as names, addresses, and license status are placed. This structured response is available as discrete values to PremierOne. This can be used to provide a visually formatted response that emphasizes key information. Figure A-13 provides a representative sample of a formatted query response.

Query Responses can be formatted for Workstations and Mobile clients. Query formatting is done using Extensible Stylesheet Language Transformations (XSLT) and the result is displayed using Hypertext Markup Language (HTML). The HTML transformation provides an enhanced level of formatting beyond the raw text that is returned in the query responses. The enhanced formatting can be helpful to call out specific data elements, or display images if they are included in the response from the External System.

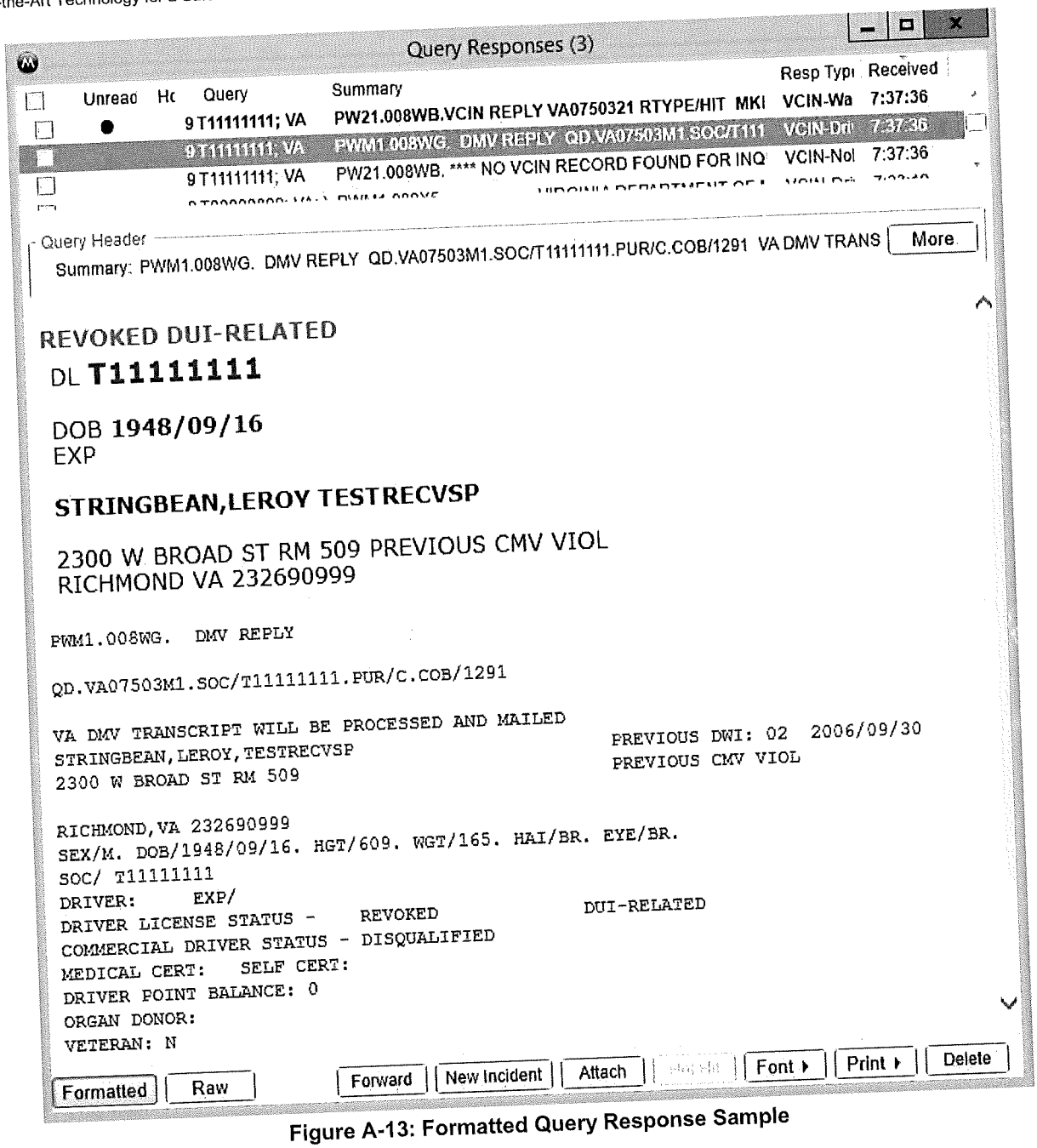


Figure A-13: Formatted Query Response Sample

A structured response may also be used to populate the person or vehicle information in an incident, without requiring the retyping of the information from a response. The user may run a query on a driver using their operator license number, and then use this feature to populate the person form with the person's details from the query response.

Cascading and drill-down queries can be provisioned by using details from the structured query response as input to subsequent queries. Cascading queries run automatically using these results and a drill-down query is run when the user clicks on the hyperlink on the response form.

The HTML transformation and structured response services are not in scope of the Interface implementation. If these additional features are desired by the Customer, Motorola Services will review the requirements and provide a separate quote for the enhanced response formatting during the interface discovery phase.

A.3.1.6 Use Cases

Use Cases describe specific user and system interactions provided by the Interface. They provide traceability for the Test Cases in the Interface Test Procedure.

Table A-6: Use Cases

Use Cases	Description
UC-01	PremierOne user can submit a transaction from a form and view the responses.
UC-02	PremierOne user can submit a transaction from a command line and view the responses.
UC-03	PremierOne user can submit a transaction using the data in an incident and view the responses.
UC-04	PremierOne user can incorporate details from a response into an incident.

A.3.2 Operational Considerations

A.3.2.1 Connectivity

Connectivity needs to be established between PremierOne Suite and the State Message Switch, over the Customer Enterprise Network, using TCP protocol. The connection needs to meet the State's security requirements

A.3.2.2 Exception Handling and Logging

PremierOne exceptions are logged in both the Windows Event Log on the application server and the PremierOne database.

CommSys ConnectCIC logs query errors and parsing issues to the ConnectCIC log file on the PremierOne application server.

A.3.2.3 Security

User access to the query forms are managed by user roles in PremierOne.

Users need to be certified according to the State requirements and have a valid user account to access the State system. Devices used to submit queries must also meet the State security requirements.

A.3.2.4 Performance

There are no explicit performance requirements for the Interface.

The query response is dependent on the State connection and response time of the data sources. Query response is displayed as it is received from the external data source.

A.3.2.5 High Availability and Disaster Recovery

There are no additional High Availability or Disaster Recovery requirements for the Interface, beyond the standard implementation for PremierOne Suite.

Availability of queries on the Disaster Recovery (DR) server is dependent on the connectivity to the State, additional connection and equipment might be required to establish this connection.

A.3.2.6 System Administration

Customer is responsible for contacting Motorola Solutions when changes occur in the Interface or Customer Enterprise Network, which might affect the Interface.

Customer is responsible for contacting Motorola Solutions when State changes the parameters or the response formats of the queries.

Customer is responsible for maintaining user credentials, ORIs and Mnemonics as required by the State.

A.3.3 Statement of Work

A.3.3.1 General

The following Statement of Work (SOW) defines the scope of work involved in delivering an interface between the State and the St Johns Sheriff's Office's ("Customer") PremierOne CAD System. This document includes the responsibilities of Motorola and the Customer.

A.3.3.2 Overview

This section defines the principal activities and responsibilities of Motorola Solutions and the Customer, during the interface deployment. This Statement of Work provides understanding of the work required by all parties for the interface implementation.

Motorola Solutions assumes no responsibility for training, installation, configuration, on-going support or warranty for any third-party systems and/or software not included as part of the contracted solution.

A.3.3.3 Responsibilities

Motorola Solutions Responsibilities

- Conduct an ISD review session with the Customer subject matter experts to obtain details regarding transaction types, query criteria, and response transformation.
- Implement the Interface for six forms with basic response formatting and two response types per request.
- Provide the transactions identified during the ISD review session.
- Provide the response parsing identified during the ISD review session.
- Provide eight hours of training and support for the Customer to provision additional queries.

- Provide guidance on hardware, software and network connectivity that may be required of Customer to support the interface implementation use and maintenance, prior to implementation.
- Conduct a functional demonstration validating the Interface works in accordance with this ISD.

Customer Responsibilities

- Participate in the ISD review session and provide details required for interface installation, configuration, test and support.
- Familiarize themselves with this ISD.
- Provide all hardware, software and network connectivity not specifically provided by Motorola Solutions, prior to implementation.
- The customer's third-party system must be on a version supported by the customer third-party. Customer will procure any required upgrades.
- Coordinate Customer third-party involvement with the implementation and testing of the Interface, as required.
- Provide Users, Originating Agency Identifiers (ORIs) and Device Identifier (Mnemonics) for each device as required by the State.
- Assist with provisioning Query Forms, Hot Hits, Pick Lists and Response Formats.
- Witness the functional demonstration of the Interface.
- Protect the Enterprise Network against unauthorized access.
- Provide secure connections between PremierOne and the Interface.
- Manage customer third-party responsibilities to completion, as applicable, enabling Motorola Solutions to complete its responsibilities.
- Manage communication between Motorola Solutions and Customer third-party, enabling Motorola Solutions to complete its responsibilities.

A.3.3.4 Implementation Plan

Table A-7: Implementation Plan

Task	Owner
Establish network connectivity between PremierOne and the State Message Switch	Customer
Provide PremierOne to State Query documentation	Motorola Solutions
Procure ConnectCIC Transactions and Licenses from CommSys	Motorola Solutions
Install and configure ConnectCIC on PremierOne servers	Motorola Solutions
Configure CSI component for the Interface on PremierOne servers	Motorola Solutions
Load Query Metadata in PremierOne	Motorola Solutions
Configure Query Interface in PremierOne	Motorola Solutions / Customer
Provision Query Request Form in PremierOne	Motorola Solutions / Customer
Configure Query Response in PremierOne for Workstation and Mobile	

Task	Owner
Provision user roles to access query in PremierOne	Customer
Provision ORI, Mnemonic, State User Id in PremierOne	Customer
Test State connection	Customer

A.4 PremierOne - DataWorks Mugshot Interface

A.4.1 Interface Description

A.4.1.1 Interface Overview

Information is exchanged across this two-way interface between Motorola Solution's PremierOne Records application and the DataWorks Mugshot application.

Inmate information shall be entered in the Inmate Booking document within PremierOne Records. Once the booking officer determines that the information is complete and ready to be sent to the Mugshot application the user shall submit the document to Workflow. Through this workflow stage, the interface submits the inmate demographics to the mugshot application via web services.

After the collection of mugshots and SMT photos, the mugshot system will send the Photos information to the PremierOne Records system to update the inmate's booking record.

The interface diagram shows the connectivity and primary data flow across the system. Blue represents the new systems and software that will be deployed to implement the interface. Green represents existing systems required for the interface.

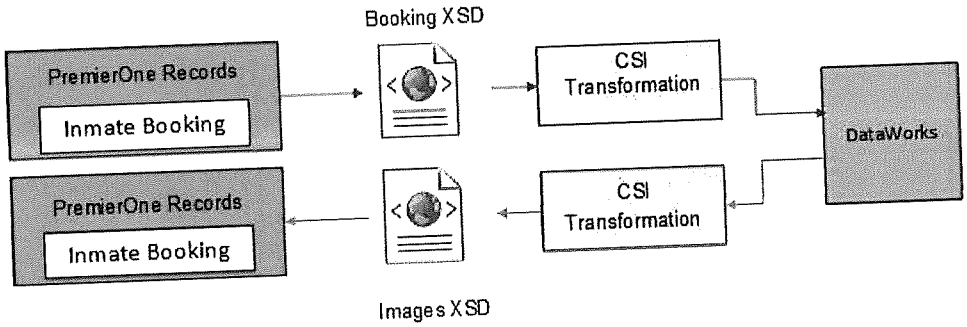


Figure A-14: Imageware Interface Diagram

A.4.1.2 Data Exchange

When a completed Inmate Booking Document is successfully sent to workflow, CSI shall read the document, transform the PremierOne XML into the DataWorks XML schema and route to the DataWorks Web Service.

DataWorks shall be listening on the DataWorks Web Service on the defined port for incoming messages from PremierOne. As messages are received, DataWorks shall process the documents and route the documents to the mugshot machine.

After the photos of mugshots and SMT's are collected, the DataWorks mugshot system will send the photos to the PremierOne Records system to be added to the inmate booking record. DataWorks shall send the XML document to the PremierOne web service. PremierOne shall be listening on the defined address/port and retrieve any messages delivered across the web service.

A.4.1.3 Business Process

Inmate demographics shall be exported to the mugshot machine for the process of inmate photos. This eliminates duplicate entry of inmate information.

Once the images and prints have been processed, DataWorks will make the photos available for PremierOne CSI to import these back into the inmate booking record.

A.4.1.4 User Experience

When an inmate booking record is created in the PremierOne Records system, the user enters the inmate's demographic information, arrest information and charge data. Once the booking document is completed, the user can send the document through the booking workflow process in PremierOne

The mugshot user will review the Inmate Booking documents available on the mugshot station and select the desired record. If found, the user can select the record for import to the mugshot station for further processing which shall pre-populate the mugshot record with the booking demographic information with details previously entered in PremierOne.

The mugshot user may continue to complete the mugshot process. This action will make the images available for import into PremierOne Records upon completion of taking all photos..

A.4.1.5 Use Case

Use Cases describe specific user and system interactions provided by the interface. They provide traceability for the Test Cases in the Acceptance Test Plan (ATP).

Table A-8: Use Case

Use Case	Description
UC-01	PremierOne Records shall submit inmate demographic data to DataWorks Mugshot Web Service.
UC-04	The PremierOne Record submitted to a mugshot machine shall be available to the mugshot user for import.
UC-05	Updated booking documents shall be submitted back to PremierOne upon completion of the photos.
UC-06	The updated records shall update the PremierOne Inmate Booking record.

A.4.2 Operational Considerations

A.4.2.1 Connectivity

The connectivity must be established between the PremierOne Records application server and the DataWorks Mugshot system.

A.4.2.2 Exception Handling and Logging

All PremierOne exceptions are logged in the Windows Event Log on the application server.

A.4.2.3 Security

Inmate Booking privileges need to be granted for each security group inside of PremierOne for use of this feature.

A.4.2.4 Performance

The Booking record data should be available in the mugshot queue within 5 minutes of submittal.

A.4.2.5 High Availability and Disaster Recovery

There are no additional High Availability or Disaster Recovery requirements for the interface, beyond the standard implementation for PremierOne Records.

A.4.2.6 System Administration

Customer is responsible for contacting Motorola Solutions when changes occur in Imageware or Customer Enterprise Network (CEN), which might affect the interface.

A.4.2.7 Maintenance

There are no explicit maintenance requirements for the interface.

Refer to the "Warranty and Support" and "Maintenance Agreement" documents for additional information.

A.4.3 Statement of Work

A.4.3.1 Overview

This section defines the principal activities and responsibilities of Motorola Solutions, the Customer, and applicable Third Parties during the interface deployment and test process. This SOW provides the most current understanding of the work required by all parties to ensure a successful interface implementation.

This Interface Specification Document (ISD) is a description of the capabilities of PremierOne and the interface between PremierOne Records and the Imageware system. It is not representative of the capabilities of the DataWorks system. The Customer must coordinate with Imageware to determine any necessary hardware, software licenses, or product upgrades required to support the PremierOne interface. Motorola Solutions will deploy the interface and verify the functionality described in this ISD.

A.4.3.2 Responsibilities

Motorola Solutions Responsibilities

- Develop and deploy this interface on the PremierOne Records system.
- Provide Customer with instructions required to maintain the interface.
- Provide the interface ATP and assist in testing the interface.
- Support the interface.

Customer Responsibilities

- Review the Interface Specification Document (ISD) and Acceptance Test Plan (ATP) for the interface.
- Provide necessary hardware, software and network connectivity on the Customer Enterprise Network (CEN) as needed to support the interface, prior to implementation.
- Conduct acceptance testing of the interface using the Motorola Solutions provided ATP.

Imageware Responsibilities

- Provide data structure and documentation for the web service.
- Configure the web service to consume PremierOne Inmate Booking documents.
- Assist with implementation and testing of the interface, as required.

A.4.3.3 Implementation Plan

Table A-9: Implementation Plan

Task	Owner
Establish network connectivity between PremierOne Records and DataWorks	Customer
Provision the Inmate Booking workflow and list management tables in PremierOne	Customer
Develop CSI component for the DataWorks interface	Motorola Solutions
Install and configure CSI service for the PremierOne application server	Motorola Solutions
Configure the DataWorks application to consume PremierOne Records data	DataWorks
Provide Inmate Booking data for testing	Customer
Provide the photos in a xml schema to be imported back into PremierOne Records	DataWorks

A.4.4 Appendix

A.4.4.1 Acronyms and Definitions

Table A-10: Acronyms & Definitions

Acronym	Definition
ACT	Advanced Configuration Tool
ATP	Acceptance Test Plan
CEN	Customer Enterprise Network
CSI	Common Service Interface

Acronym	Definition
ISD	Interface Specification Document
TCP	Transmission Control Protocol

A.5 PremierOne CAD - PMAM False Alarm Interface

A.5.1 Interface Description

A.5.1.1 Introduction

This Interface Specification Document provides a description of the capabilities of PremierOne, the interface between PremierOne and the PMAM False Alarm ("System"), and the scope of work involved in delivering an interface between System and the St. Johns County, FL ("Customer") PremierOne {CAD/Mobile/Records/Suite}. It is not representative of the capabilities of the System.
The Customer must coordinate with third party vendors and/or system administrators to determine any necessary hardware, software licenses, or product upgrades required to support the PremierOne interface. Motorola Solutions assumes no responsibility for training, installation, configuration, on-going support or warranty for any third-party systems and/or software not included as part of the contracted solution. Motorola Solutions will deploy the interface and verify the functionality described in this Interface Specification Document. If Customer desires any changes from this standard interface implementation, those changes can be address via the change provision of the contract.

A.5.1.2 Interface Overview

The PMAM False Alarm System is a part of the False Alarm Management Solution (FAMS) platform that is a robust interactive web based false alarm management and reduction solution that provides real time alarm data to mobile units, tracks alarm users and provides full service administration of the entire alarm reduction effort.

The PMAM False Alarm interface allows the PMAM False Alarm system to transfer alarm permit information to PremierOne CAD, and for PremierOne CAD to send false alarm related incidents to PMAM False Alarm, for tracking and billing. PMAM False Alarm also uses this information to determine the action PremierOne CAD should take when an alarm incident occurs at the location.

The PremierOne Common Services Interface (CSI) will be scheduled to extract closed false alarm incidents from PremierOne CAD. The CSI service will upload the data file to the PMAM False Alarm File Server. The CSI service has built-in connectors for File Transfer Protocol (FTP) and Secure File Transfer Protocol (SFTP) connection. The PMAM False Alarm System would monitor the PMAM False Alarm File Server and import the data.

The CSI service will be configured to monitor the PMAM False Alarm File Server for alarm permit files and import the data into the Alarm and Alarm Company tables, and then archive/delete the file. If additional files are received, PremierOne will process the files in the order they are received.

The interface diagram shows the connectivity and primary data flow across the system. Blue shaded box represents the new systems and software that will be deployed to implement the interface. Green shaded box represents existing systems required for the interface.

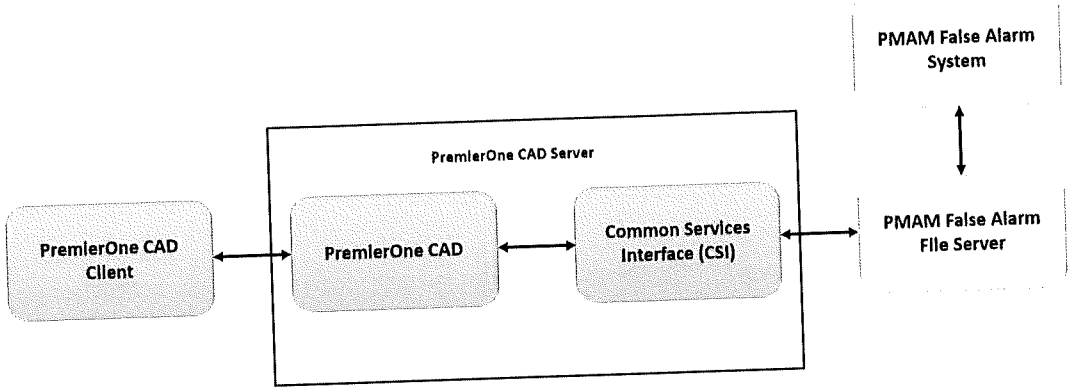


Figure A-15: PMAM False Alarm Interface Diagram

Details regarding the PMAM False Alarm System will be defined during the interface discovery phase, and will be documented in the Technical Specification Document. Any additional requirements gathered during the interface discovery phase will be provided to the Customer as a change order for Customer consideration.

A.5.1.3 Data Exchange

Incident Data

The CSI service will create the Incident Data file and place it on the file server. It will be schedule to run daily. The file includes all closed false alarm incidents, since the last data extract. The extract process can be configured to filter data based on agency, incident type, response type, priority, alarm level, disposition code or call source. The records in the file are sorted by incident creation time, in chronological order. The data in the file is in fixed format. The file name contains the extract date and is in text format (.txt).

Alarm Permit

The PMAM False Alarm System will create and place the Alarm Permit file on the file server. The file contains new, updated and deleted alarm permits, alarm company information and details on how to process incidents at the alarm location.

The data in the file is in fixed format. If the file name starts with "U", it is an update. If the file name starts with "R", it is a complete refresh of the PremierOne CAD Alarm tables. The rest of the file name is the timestamp (eg. U1017075.txt). The "update" Alarm Permit file is cumulative for the calendar day. That is, if the file is generated multiple times throughout the day, later files during the day will contain records from the earlier files in the day. Therefore, PremierOne CAD must process the records in the file from top to bottom.

Alarm Permit Processing Result

The Alarm Permit Processing Result file is generated by the PMAM False Alarm interface during the Alarm Permit data load process, and is placed on the file server. A record is generated for each failed record import only. The last record summarizes the number of successfully processed records.

The data in the file is in fixed format. The file name starts with "E" and the numeric portion of the file corresponds to the PMAM False Alarm file that was being processed (eg. E1017075.txt).

The data flow diagram captures the events, triggers and message exchange between the systems.

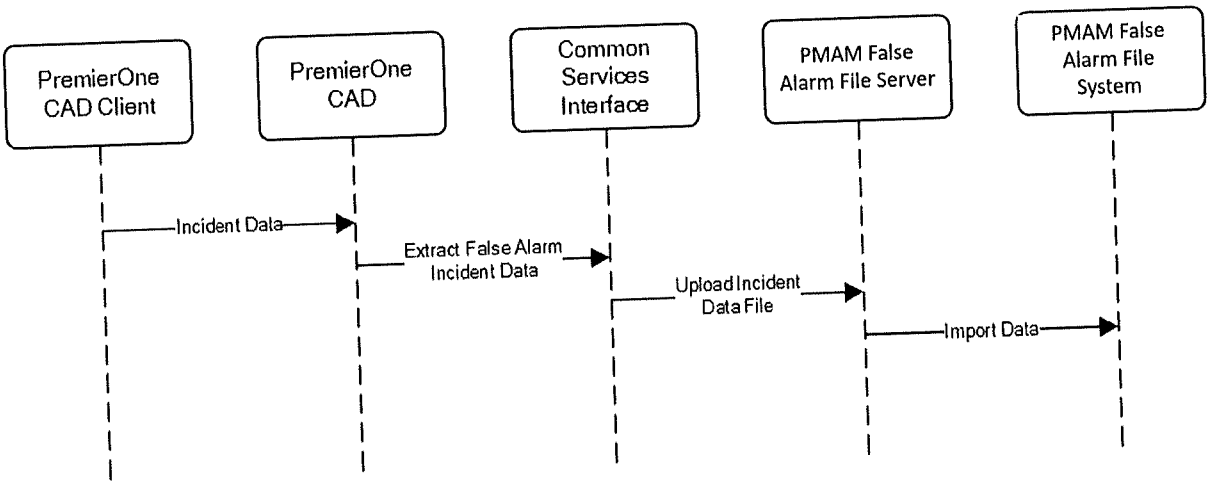


Figure A-16: PMAM False Alarm Incident Data Flow Diagram

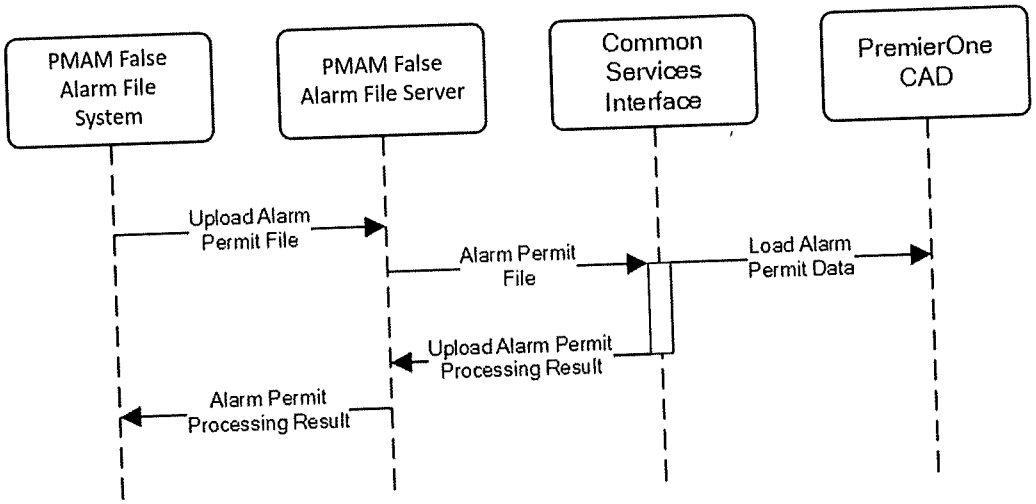


Figure A-17: PMAM False Alarm Incident Data Flow Diagram

A.5.1.4 Business Process

Address Verification

During the Alarm Permit import process, the address of the alarm permit location is verified against PremierOne CAD's Graphic Information System (GIS) data. If there are ambiguities in the alarm permit address (e.g., two or more "100 Main Street" in the city of "Manassas") or if the address does not match an address in PremierOne CAD's Graphic Information Service data, PremierOne will not import the record. To avoid address validation errors, both PremierOne and PMAM False Alarm should use the same Graphic Information System data.

Any processing error will result in the particular alarm permit record not being added or updated in PremierOne CAD, and the error being logged in the Alarm Permit Processing Result file. Even though the address is verified during the import process, the beat of the imported alarms is not stored with the alarm data, they are resolved when the alarm is used to create an incident.

Alarm Company Data

PremierOne CAD adds new alarm companies to its Alarm Company tables as it encounters them during the import of the Alarm Permit records. PremierOne CAD uses the Alarm Company Name as the key for the alarm companies. If an Alarm Company already exists and has a different phone number, PremierOne CAD adds the phone number to the existing Alarm Company entry.

If multiple Alarm Permit Records have the same Alarm Company Name with different phone numbers, all the numbers will be associated and displayed for all the Alarm Permits associated with that Company on PremierOne CAD.

A.5.1.5 User Experience

The data transfer occurs in the background and is transparent to PremierOne CAD user. PMAM False Alarm Administrator must review the Alarm Permit Processing Result file for errors.

Imported alarm permits are stored in the PremierOne CAD Alarm tables and can be viewed using the PremierOne CAD Provisioning Console. PremierOne CAD users should not make any changes to the Alarm tables, any changes made to the alarm permit data via PremierOne CAD will be overwritten by the next import process.

Alarm permit information can be viewed by PremierOne CAD user, when an alarm-related incident is created in PremierOne CAD incident form. Users have the option to search for alarm permit number in the incident form.

Table A-11 below are the step-by-step instructions for creating an alarm incident.

Table A-11: Alarm Incident Creation

Use Action	System Action	Notes
The user enters "#" followed by the alarm number in the Location field of the Initiate Incident screen and tabs away from the Location and City fields.	PremierOne CAD resolves the alarm number to the actual address and displays it on the client. PremierOne CAD verifies the address and also performs the "Potential Duplicate Incident" and "Previous Location" searches.	The user must use the alarm number. If the user enters the address (e.g. street address, common place name, lat/lon, etc.), the PremierOne CAD Alarm tables is not checked. Alternatively, the user can hit F12 instead of tabbing away from this field. The incident will be created with the incident type sent from PMAM False Alarm. PremierOne CAD does not allow the user to assign units on the initial submission of the incident when the alarm number is used. Alarm numbers are only valid for creating incidents on the

Use Action	System Action	Notes
		PremierOne CAD client. Mobile users cannot use alarm numbers to create incidents.
The user reviews the information on the form and hits F12 to submit the incident.	PremierOne CAD creates the incident. The Call Source of the incident is set to the code provisioned for alarm initiated incidents.	The incident is created regardless of the "Create Incident" setting from PMAM False Alarm. PMAM False Alarm sends different incident types based on the value of the Create Incident field and PremierOne CAD uses the type for the incident created. The alarm permit holder, contact information, company and alarm number can be viewed under the "INC CREATE" transaction type in the incident history.
The incident is handled and closed using the appropriate alarm related disposition code.	PremierOne CAD sends the incident information to its Reporting Data Warehouse (RDW).	The user must close the incident using a disposition code that the interface uses to select the incidents for PMAM False Alarm.
No user action needed	The interface extracts the incidents, based on the incident type and disposition code, and sends it to PMAM False Alarm daily.	The interface sends the selected incidents from the previous day nightly.

A.5.1.6 Use Case

Use Cases describe specific user and system interactions provided by the interface. They provide traceability for the Test Cases in the Interface Test Procedure.

Table A-12: Use Case

Use Case	Description
UC-01	PremierOne system can send false alarm data for closed incidents
UC-02	PremierOne system can import alarm permit data
UC-03	PremierOne system can send alarm permit processing result

A.5.2 Operations Considerations

A.5.2.1 Connectivity

Connectivity needs to be established between PremierOne CAD and the PMAM False Alarm File Server over the Customer Enterprise Network. PremierOne supports FTP and SFTP connection to the PMAM False Alarm File Server.

A.5.2.2 Exception Handling and Logging

PremierOne exceptions are logged in the Windows Event Log on the application server. CSI exceptions are logged in the PremierOne database.

Alarm Permit processing errors caused by invalid data will be logged in the "Alarm Permit Processing Result" file ("E*"). PMAM False Alarm Administrator will manually review the file and correct the problems on the PMAM False Alarm application. Changes made will be sent to PremierOne when the next Alarm Permit file is generated.

A.5.2.3 Security

A Windows Service Account with read/write access to the PMAM False Alarm File Server will be created for PremierOne CAD and PMAM False Alarm system.

A.5.2.4 Performance

There are no explicit performance requirements for the interface. The PMAM False Alarm data refresh process will be setup to run during off-peak hours, in PremierOne CAD.

A.5.2.5 High Availability and Disaster Recovery

There are no additional High Availability or Disaster Recovery requirements for the interface, beyond the standard implementation for PremierOne CAD.

If available, the PremierOne recovery servers will be setup to access the PMAM False Alarm File Server for the interface.

A.5.2.6 System Administration

Customer is responsible for contacting Motorola Solutions when changes occur in PMAM False Alarm system, PMAM False Alarm File Server or Customer Enterprise Network, which might affect the interface.

Customer is responsible for keeping the reference data synchronized between PremierOne CAD and the PMAM False Alarm system.

Customer is responsible for regularly archiving/purging files on the PMAM False Alarm File Server.

PMAM False Alarm Administrator is responsible for manually reviewing the "Alarm Permit Processing Result" file and resending fixed data in the Alarm Permit file, if required.

A.5.3 Statement of Work

A.5.3.1 Overview

This section defines the principal activities and responsibilities of Motorola Solutions, the Customer, and applicable Third Parties during the interface deployment. This Statement of Work provides understanding of the work required by all parties for a successful interface implementation.

A.5.3.2 Responsibilities

Motorola Solutions Responsibilities

- Conduct interface discovery session with the Customer subject matter experts and vendors to obtain details regarding the connection details and data elements.
- Implement the PMAM False Alarm interface for integration with a single file server destination
- Provide guidance on hardware, software and network connectivity as needed to support the interface, prior to implementation.
- Provide the Interface Test Procedure document and conduct functional demonstration validating the interface works in accordance with the Interface Specification Document.

Customer Responsibilities

- Participate in the interface discovery session and provide details for the Technical Specification Document, as mentioned in Motorola Solutions Responsibility (a).
- Familiarize themselves with the Interface Specification Document and Interface Test Procedure for the interface.
- Provide list of incident types associated with false alarm.
- Provide all hardware, software and network connectivity not specifically provided by Motorola Solutions, prior to implementation.
- Witness the functional demonstration of the interface and conduct additional testing of the interface as desired, using the Motorola Solutions provided Interface Test Procedure.
- Manage vendor and system administrator responsibilities to completion, enabling Motorola Solutions to complete its responsibilities.
- Manage communication between Motorola Solutions and vendors / system administrators, enabling Motorola Solutions to complete its responsibilities.

False Alarm Management Solution (FAMS) Responsibilities

- Participate in the interface discovery session and provide details for the Technical Specification Document, as mentioned in Motorola Solutions Responsibility (a).
- Configure PMAM False Alarm application to provide permit data and to consume PremierOne CAD data.

A.5.3.3 Implementation Plan

Table A-13: Implementation Plan

Task	Owner
Provide PMAM False Alarm File Server	Customer / Motorola Solutions
Provide PremierOne Service Account read/write privilege to the PMAM False Alarm File Server	Customer
Provide Windows Service Accounts with read/write privilege to the PMAM False Alarm File Server for the PMAM False Alarm System	Customer

Task	Owner
Establish network connectivity between PremierOne CAD and PMAM False Alarm File Server	Customer
Establish network connectivity between PMAM False Alarm System and the PMAM False Alarm File Server	Customer / Public Safety Corporation
Provide list of Incident Types associated with false alarm	Customer
Install and configure CSI component to extract and transfer PremierOne CAD data	Motorola Solutions
Configure PMAM False Alarm Interface in PremierOne	Motorola Solutions
Configure PMAM False Alarm to provide alarm permit data	Customer / Public Safety Corporation
Configure PMAM False Alarm to consume PremierOne CAD data	Customer / Public Safety Corporation

A.5.4 Appendix

A.5.4.1 Acronyms and Definitions

Table A-14: Acronyms & Definitions

Acronym	Definition
CAD	Computer Aided Dispatch
CSI	Common Services Interface
FTP	File Transfer Protocol
GIS	Graphic Information System
RDW	Reporting Data Warehouse
SFTP	Secure File Transfer Protocol

A.5.4.2 UI Field Mapping

The sample list of PMAM False Alarm data elements displayed on PremierOne CAD Provisioning Console and PremierOne CAD Incident Form.

Table A-15: UI Field Mapping

PMAM False Alarm Field	PremierOne CAD Provisioning Console Field	PremierOne CAD Incident Form Field	Notes
Owning Agency	Agency	Agency	
Alarm Number	General -> Alarm ID	History -> Inc Create -> Alarm ID	
Address	General -> Location - Address	Location	

PMAM False Alarm Field	PremierOne CAD Provisioning Console Field	PremierOne CAD Incident Form Field	Notes
Bldg-Apt	General -> Location - Bldg	Building	PremierOne CAD Apartment field is not used by this interface
City	General -> Location - City	City	
Create Incident	Not Displayed	Not Displayed	
Incident Type	Incident -> Incident Type	Incid Type	Indicates the action the user should take: respond account or a no-response account
Location	General -> Location - Loc. Name	Loc Name	Location of the address (e.g. Embassy Suites Marietta City or the actual street address)
Contact1	General -> Contacts -> First Name/Last Name	History -> Inc Create -> Contact	
Phone1	General -> Contacts -> Phone	History -> Inc Create -> Contact	
Contact2	General -> Contacts -> First Name/Last Name	History -> Inc Create -> Contact	
Phone2	General -> Contacts -> Phone	History -> Inc Create -> Contact	
Alarm Company	General -> Alarm Company	History -> Inc Create -> Company	
Alarm Company Phone	General -> [Alarm Company] Phone	History -> Inc Create -> Phone	
Permit Holder	General -> Permit Number	History -> Inc Create -> Permit Holder	

A.5.4.3 Data Element

Table A-16: Alarm Permit

PMAM False Alarm Field	Data Type	Start	Length	Comment
Operation Code	Char	1	1	A = Add, U = Update, D = Delete This flag is ignored for Refresh files.
Owning Agency	Char	2	4	
Alarm Number	Char	5	20	
Address	Char	26	44	

PMAM False Alarm Field	Data Type	Start	Length	Comment
Bldg-Apt	Char	70	10	
City	Char	80	15	
Create Incident	Char	95	1	PMAM False Alarm sets the field to "Y" or blank, based on whether the alarm should be responded to.
Incident Type	Char	96	10	PMAM False Alarm sets the field to one of two pre-configured system-wide Incident Type values, based on whether the alarm should be responded to.
Location	Char	106	50	Location of the address (e.g. Hilton Garden Inn Marietta City or the actual street address)
Contact1	Char	156	24	
Phone1	Char	180	15	
Contact2	Char	195	24	
Phone2	Char	219	15	
Alarm Company	Char	234	20	
Alarm Company Phone	Char	254	15	
Permit Holder	Char	269	33	Must be padded if less than 33 characters.
CR	Char	302	1	
LF	Char	303	1	

Table A-17: Incident Data

PMAM False Alarm Field	Start	Length	PremierOne CAD RDW Field	Comment
AlarmNo	1	50	N/A	Blank - Set by PMAM False Alarm
AlarmType	51	50	MV_Incident.IncidentTypeCode	PremierOne CAD Incident Type Code
Apt	101	10	MV_Incident.Building	Building, Not Apartment
BeatNo	111	50	MV_Incident.BeatName	Example: 1-12
CADAlarmCoName	161	50	MV_Incident.CallerName	Incident Primary Caller Name (Should be the alarm company)
CADAlarmCoPhone	211	50	MV_Incident.CallerPhone	Incident Primary Caller Phone

PMAM False Alarm Field	Start	Length	PremierOne CAD RDW Field	Comment
CADAlarmNo	261	50	MV_Incident.AlarmID	
CADName	311	250	MV_Incident.CommonPlace	Common Place Name
CallTakerInfo	561	250	MV_Incident.CreateUserID + "/" + MV_Incident.CreateUserName	PremierOne CAD Userid and provisioned Name of the user who created the incident separated by a slash
CaseNo	811	50	MV_Incident.IncidentNumber	Unique PremierOne CAD Incident Number
ClearanceCode	861	50	MV_Incident.AllDispositions	All Disposition Codes separated by commas
DateEntered	911	20	N/A	Blank - Set by PMAM False Alarm
DispatchCode	931	50	MV_Incident.IncidentTypeCode	Same as AlarmType - PremierOne CAD Incident Type Code
DispatcherInfo	981	250	MV_IncidentComment.Userid	UserIDs of all PremierOne CAD and Mobile users who have added comments to the incident separated by commas
FullAddress	1231	100	MV_Incident.StreetName	Full Street Name (e.g. 123 N Main ST NE)
IncidentDate	1331	20	MV_Incident.IncidentDate	Date of Incident, format: 2012-04-06
MonitoredBy	1351	50	N/A	Blank - Set by PMAM False Alarm
OfficerID	1401	30	MV_Incident.PrimaryUnitAgencyID + "/" + MV_Incident.PrimaryUnitID	The Agency ID and Unit ID of the Primary Unit separated by a slash
TimeCleared	1431	30	MV_Incident.RouteClosedTime	Local time, format: 2002-05-30T09:00:00
TimeDispatched	1461	30	MV_Incident.FirstUnitDispatchedTime	First unit dispatch time, local time, format: 2002-05-30T09:00:00
TimeOnScene	1491	30	MV_Incident.FirstUnitOnArrivedTime	First unit on-scene time, local time, format: 2002-05-30T09:00:00
TimeReceived	1521	30	MV_Incident.CallReceivedTime	Local time, format: 2002-05-30T09:00:00

PMAM False Alarm Field	Start	Length	PremierOne CAD RDW Field	Comment
UnitsAssigned	1551	250	MV_IncidentUnits.CallSign	All units assigned to the incident separated by commas
DisptchComments	1801	1200	MV_Incident.AllComments	All comments made by all PremierOne CAD users (both units and dispatchers) – the left most 1200 characters are sent
CR	3001	1	N/A	
LF	3002	1	N/A	

Table A-18: Alarm Permit Processing Result

PMAM False Alarm Field Name	Start	Length	Comment
Operation Code	1	1	E = Error, S = Successful
Owning Agency	2	2	
Alarm Number	4	20	
Address	24	44	
Permit Holder	68	20	First 20 characters of the alarm holder information
Location	88	50	
Blanks	138	10	
City	148	15	
Log Error Code	163	6	
Log Error Description	169	100	
CR	269	1	Carriage Return is not visible to the user
LF	270	1	Line Feed is not visible to the user

Sample "update" Alarm Permit file (U1122140.txt). The PremierOne CAD process will add ("A") record DC/810211 and update ("U") record DC/910210.

```
ADC  810211            100 W MAIN ST
ANYTOWN         YSMOKE
STRINGBEAN, LEROY       (757) 555-1234 STRINGBEAN, BUBBA        (757) 555-5678 ADT
ALARMS          (800) 555-3434 STRINGBEAN, LEROY

UDC  910210            125 E HIGH ST
ANYTOWN         YALARM
FLINTSTONE, FRED        (757) 555-1111 FLINTSTONE, WILMA        (757) 555-2222
BEDROCK ALARMS      (800) 555-3333 FLINTSTONE, PEBBLES
```

A.5.4.4 Error Code

List of error code and description sent by PremierOne CAD in the Alarm Permit Processing Result file ("E*") in the "Log Error Code" and "Log Error Description" fields.

Table A-19: Error Code

Error Code	Error Description	Comment
0	mm/dd/yy hh:mn 999999" (note: 999999 is the number of successful records processes)	Success, used on last record
100	** UNABLE TO ADD ALARM **	Unable to add record
200	** UNABLE TO UPDATE ALARM **	Unable to update record
300	** UNABLE TO DELETE ALARM **	Unable to delete record
400	** UNABLE TO FIND ALARM **	Unable to find record
500	** ADDRESS IS NOT UNIQUE, UNABLE TO DETERMINE ADDRESS USING VERI SERVER **	Address not unique
600	** OPERATION CODE NOT VALID, MUST BE U, A, OR D **	Operation is invalid
700	NOT A PERMIT FILE	Log file error

A.6 PremierOne Records -EvidenceOnQ Interface

A.6.1 Interface Description

A.6.1.1 Introduction

This Interface Specification Document provides a description of the capabilities of PremierOne, the interface between PremierOne and the FileOnQ EvidenceOnQ ("System"), and the scope of work involved in delivering an interface between System and the St. Johns County, FL ("Customer") PremierOne Records. It is not representative of the capabilities of the System. The Customer must coordinate with third party vendors and/or system administrators to determine any necessary hardware, software licenses, or product upgrades required to support the PremierOne interface. Motorola Solutions assumes no responsibility for training, installation, configuration, on-going support or warranty for any third-party systems and/or software not included as part of the contracted solution. Motorola Solutions will deploy the interface and verify the functionality described in this Interface Specification Document. If Customer desires any changes from this standard interface implementation, those changes can be address via the change provision of the contract.

A.6.1.2 Interface Overview

CSI service in PremierOne will send Property Sheet Detail information from PremierOne Records to the EvidenceOnQ system when a Property Sheet is completed.

This is a one-way interface, with data flowing from PremierOne Records to EvidenceOnQ. No information will be imported back into PremierOne Records.

When a property sheet has been successfully saved in PremierOne Records, it will be available for export through the CSI interface.

After property has been transferred from PremierOne Records to EvidenceOnQ, all management of that property will occur in EvidenceOnQ.

The interface diagram shows the connectivity and primary data flow across the system. Blue represents the new systems and software that will be deployed to implement the interface. Green represents existing systems required for the interface.

The interface diagram shows the connectivity and primary data flow across the system.

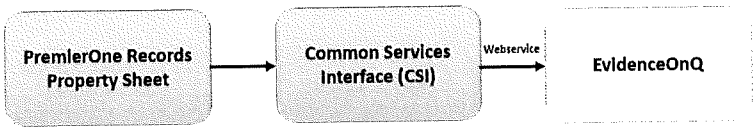


Figure A-18: EvidenceOnQ Interface Diagram

Details regarding the EvidenceOnQ will be defined during the interface discovery phase, and will be documented in the Technical Specification Document. Any additional requirements gathered during the

interface discovery phase will be provided to the Customer as a change order for Customer consideration.

A.6.1.3 Data Exchange

PremierOne CSI service will send Property Sheet information from PremierOne Records to EvidenceOnQ when a Property Sheet is created or updated.

PremierOne Property Sheet information will be sent utilizing EvidenceOnQ's web service.

There will be no information transferred from EvidenceOnQ into PremierOne Records.

EvidenceOnQ web service with all the potential fields P1 could send using the as-of-now field mapping we have. The link is: http://dev.fileonqsupport.com:8007/EoQPremierOneService.svc

The link to view the WSDL (technical description of the service) is: http://dev.fileonqsupport.com:8007/EoQPremierOneService.svc?singleWsdl

A.6.1.4 Business Process

A user in PremierOne Records will enter property into the property sheet for a case. Upon a successful save, this information will be transferred to EvidenceOnQ.

Inside of PremierOne, no further management of this property will be required. All management will occur in EvidenceOnQ once PremierOne CSI has exported this information to EvidenceOnQ.

If a Property Sheet has been updated inside of PremierOne Records, this updated information will also be sent to EvidenceOnQ.

A.6.1.5 User Experience

A PremierOne Records user will create a property sheet in a case folder by either manually entering the property detail or by bringing the existing property from the case report.

Once the property sheet has been saved, this is the end of the management of the property in PremierOne Records unless updates to the property sheet need to occur.

The user has the ability to make updates to the property sheet inside of PremierOne Records and these updates will be sent by CSI.

CSI will export the saved property sheet details into EvidenceOnQ. The property room personnel will manage the property exclusively in EvidenceOnQ from that point on.

A.6.1.6 Use Case

Use Cases describe specific user and system interactions provided by the interface. They provide traceability for the Test Cases in the Interface Test Procedure.

Table A-20: Use Case

Use Case	Description
UC-01	Property Sheets saved in Draft mode will not be sent to EvidenceOnQ.

Use Case	Description
UC-02	Property Sheets successfully saved will be sent to EvidenceOnQ.
UC-03	Updates to a previously saved Property Sheet are being sent to EvidenceOnQ.
UC-04	Evidence Transactions performed to property in PremierOne Records, are not sent over to EvidenceOnQ.

A.6.2 Operational Considerations

A.6.2.1 Connectivity

Connectivity needs to be established between PremierOne Records and the EvidenceOnQ over the Customer Enterprise Network. Firewall ports must be open to allow TCP communication.

A.6.2.2 Exception Handling and Logging

PremierOne exceptions are logged in the Windows Event Log on the application server. CSI exceptions are logged in the PremierOne database.

A.6.2.3 Security

There are no additional security requirements for the interface, beyond the standard implementation for PremierOne RMS.

A.6.2.4 Performance

There are no explicit performance requirements for the interface. The transfer of data from PremierOne production database to the PremierOne RDW is scheduled to run every 30 seconds. The transfer process only takes a couple of seconds under normal load condition. Analysis of prior PremierOne deployments shows that data arrives at the RDW in less than 60 seconds from the event occurring in Records.

A.6.2.5 High Availability and Disaster Recovery

There are no additional High Availability or Disaster Recovery requirements for the interface, beyond the standard implementation for PremierOne Records.

A.6.2.6 System Administration

Customer is responsible for contacting Motorola Solutions when changes occur in EvidenceOnQ or Customer Enterprise Network, which might affect the interface.

Customer is responsible for keeping the reference data synchronized between PremierOne RMS and EvidenceOnQ system.

A.6.3 Statement of Work

A.6.3.1 Overview

This section defines the principal activities and responsibilities of Motorola Solutions, the Customer, and applicable Third Parties during the interface deployment. This Statement of Work provides understanding of the work required by all parties for a successful interface implementation.

A.6.3.2 Responsibilities

Motorola Solutions Responsibilities

- Conduct interface discovery session with the Customer subject matter experts and vendors to obtain details regarding EvidenceOnQ System.
- Implement the interface for EvidenceOnQ System.
- Provide guidance on hardware, software and network connectivity as needed to support the interface, prior to implementation.
- Provide the Interface Test Procedure document and conduct functional demonstration validating the interface works in accordance with the Interface Specification Document.

Customer Responsibilities

- Participate in the interface discovery session and provide details for the Technical Specification Document, as mentioned in Motorola Solutions Responsibility (a).
- Familiarize themselves with the Interface Specification Document, Technical Specification Document and Interface Test Procedure for the interface.
- Provide all hardware, software and network connectivity not specifically provided by Motorola Solutions, prior to implementation.
- Witness the functional demonstration of the interface and conduct additional testing of the interface as desired, using the Motorola Solutions provided Interface Test Procedure.
- Manage vendor and system administrator responsibilities to completion, enabling Motorola Solutions to complete its responsibilities.
- Manage communication between Motorola Solutions and vendors / system administrators, enabling Motorola Solutions to complete its responsibilities.

EvidenceOnQ Responsibilities

- Participate in the interface discovery session and provide details for the Technical Specification Document, as mentioned in Motorola Solutions Responsibility (a).
- Assist with implementation and testing of the interface, as required.
- Configure the web service to consume PremierOne Property Sheet data.

A.6.3.3 Implementation Plan

Table A-21: Implementation Plan

Task	Owner
Establish network connectivity between PremierOne Records and EvidenceOnQ	Customer
Provision reference data in PremierOne Records List Management	Customer
Provide specifications on web service and xml schema	FileOnQ
Develop CSI component for the EvidenceOnQ interface	Motorola Solutions
Install and configure CSI service all PremierOne application servers	Motorola Solutions
Configure the EvidenceOnQ application to consume PremierOne Records data	FileOnQ
Provide Property data for testing	Customer

A.6.4 Appendix

A.6.4.1 Acronyms and Definitions

Table A-22: Acronyms & Definitions

Acronym	Definition
ATP	Acceptance Test Plan
CEN	Customer Enterprise Network
CSI	Common Services Interface
RMS	Records Management System
TCP	Transmission Control Protocol

A.7 PremierOne CAD - Outbound EPCR Interface

A.7.1 Interface Description

A.7.1.1 Introduction

This Interface Specification Document (ISD) provides a description of the capabilities of PremierOne CAD Outbound ePCR Interface (Interface) and the scope of work involved in delivering this Interface. Motorola Solutions will deploy the Interface and verify the functionality described in this ISD. If Customer desires any changes to this ISD scope, those changes can be addressed via the change provision of the contract.

A.7.1.2 Interface Overview

The Interface allows PremierOne CAD to provide incident data related to medical-incidents to a third-party ePCR system. The PremierOne CAD system is set up to post transactional updates to the RDW database within 30 seconds. The PremierOne Common Services Interface (CSI) will be scheduled to extract the required data from PremierOne CAD RDW. The CSI service can provide the data in a file format, update the external system database directly or call an Application Programming Interface (API) published by the third-party ePCR system. The CSI service has built-in connectors for Open Database Connectivity (ODBC), File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), REST Web Service and Transmission Control Protocol (TCP) connection.

In the file extract option, the CSI service will upload the data file to the ePCR File Server. The third-party ePCR system would monitor the ePCR File Server and import the PremierOne data. The CSI service can provide the data as fixed or delimited records or as XML messages.

Figure A-19 through Figure A-21 show the connectivity and primary data flow across the system.

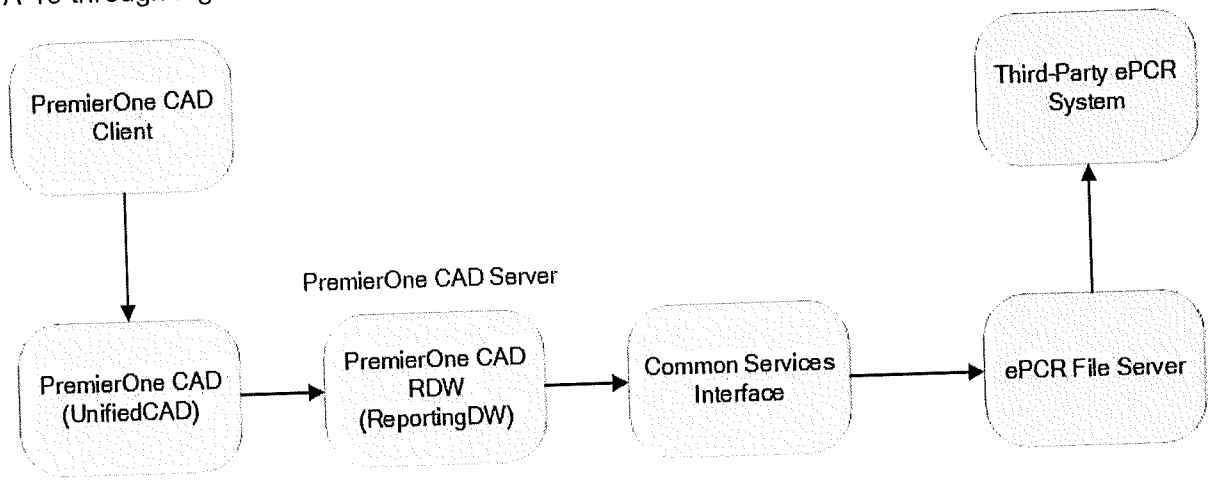


Figure A-19: File Extract Interface Diagram

In the database update option, the CSI service can be configured to call a Stored Procedure provided by the third-party ePCR system, to insert PremierOne data into the third-party ePCR system database.

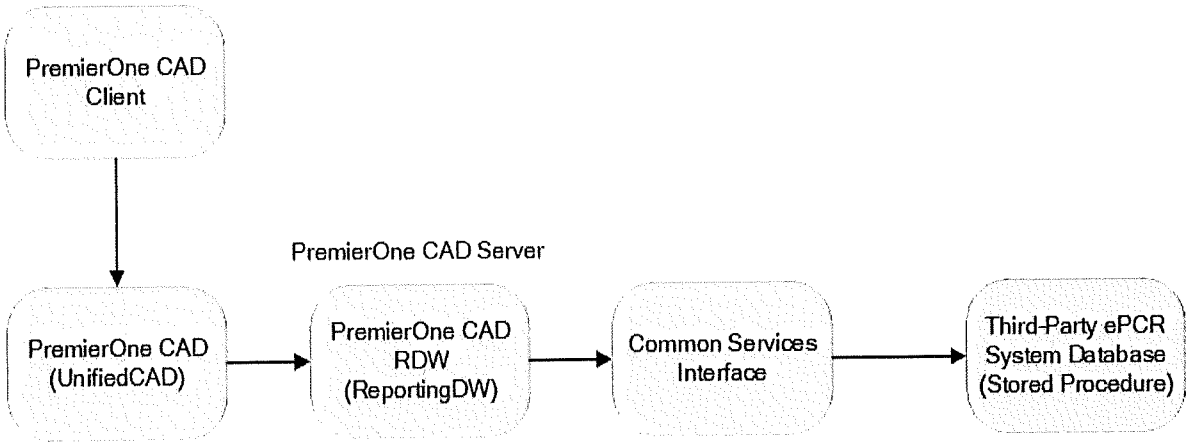


Figure A-20: Database Update Interface Diagram

In the API call option, the CSI service can be configured to call an API provided by the third-party ePCR system, to provide the PremierOne data to the third-party ePCR system.

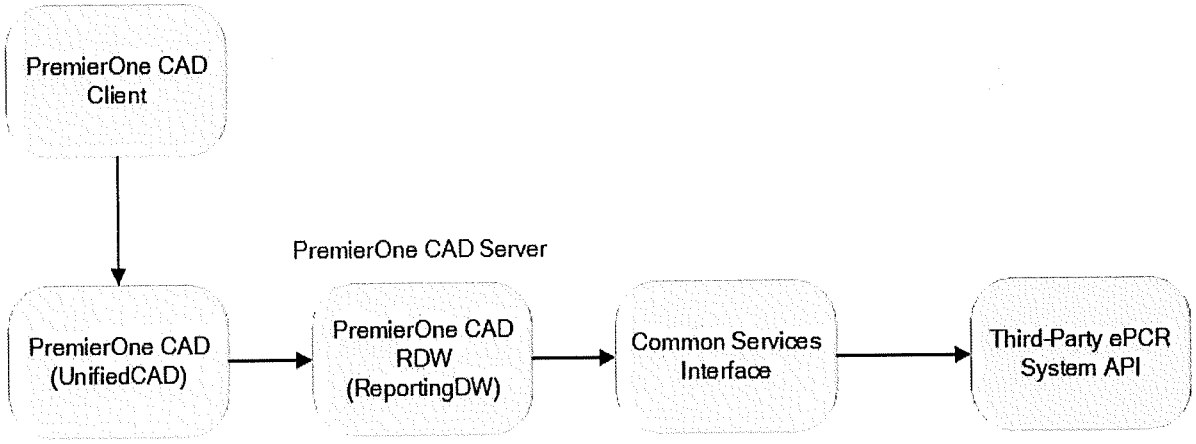


Figure A-21: API Call Interface Diagram

This Interface requires modification to PremierOne CSI service. Motorola Solutions is reliant on receipt of the API or Stored Procedure and the associated design documents from the Customer to implement the Interface.

The Interface provides data from PremierOne CAD Views (MV_* Views) and is based on the new, update or closed incident triggering criteria. PremierOne can also be configured to trigger the data extract based on specific agency, incident type, response type, priority or alarm level. The Interface only provides the current snapshot of the incident. Any additional data elements, data transformation or formatting requirements or triggering criteria beyond this will be gathered during the interface discovery phase and provided to the Customer as a change order for Customer consideration.

Information required for installation, configuration, test and support purposes regarding this Interface will be gathered during the ISD review.

A.7.1.3 Data Exchange

The PremierOne CSI service will manage the data extraction and transfer process.

The data flow diagram captures the events, triggers and message exchange between the systems.

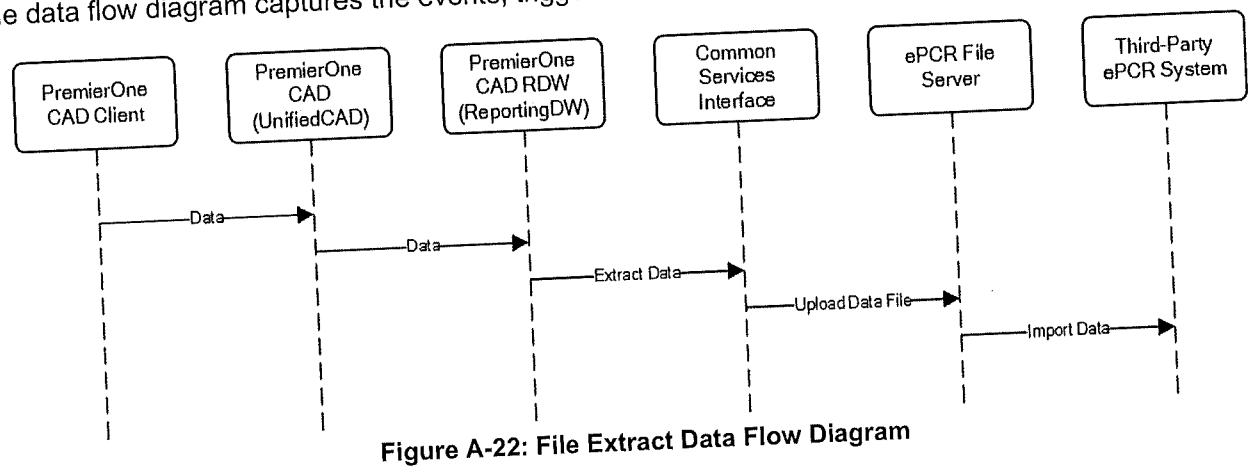


Figure A-22: File Extract Data Flow Diagram

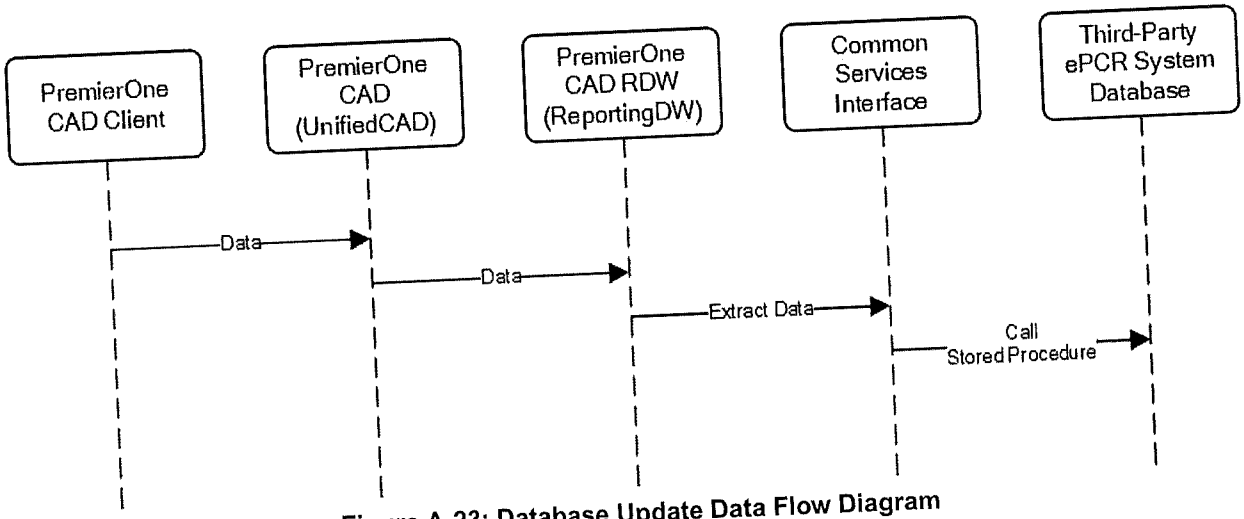


Figure A-23: Database Update Data Flow Diagram

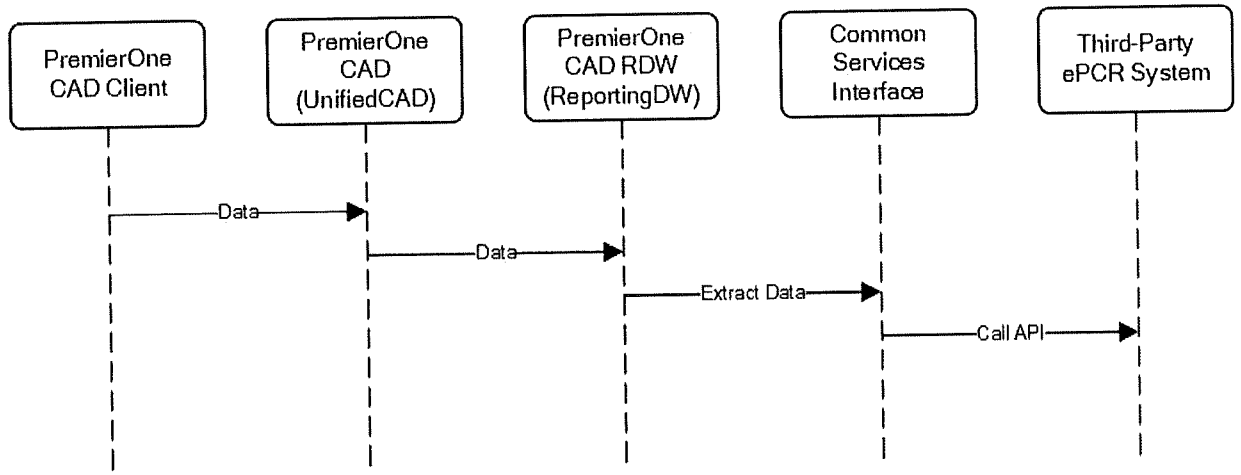


Figure A-24: API Call Data Flow Diagram

A.7.1.4 Business Process

None.

A.7.1.5 User Experience

The data transfer occurs in the background and is transparent to PremierOne CAD user. Third-party ePCR system users may view the information in their application.

A.7.1.6 Use Cases

Use Cases describe specific user and system interactions provided by the Interface. They provide traceability for the Test Cases in the Interface Test Procedure.

Table A-23: Use Cases

Use Cases	Description
UC-01	PremierOne CAD can export incident data.

A.7.2 Operational Considerations

A.7.2.1 Connectivity

Connectivity needs to be established between PremierOne CAD and the third-party ePCR system or the ePCR file server, over the Customer Enterprise Network. Connectors supported by PremierOne are ODBC, FTP, SFTP, REST Web Service and TCP.

A.7.2.2 Exception Handling and Logging

PremierOne exceptions are logged in both the Windows Event Log on the application server and the PremierOne database.

A.7.2.3 Security

For the file extract solution, a Windows Service Account with read/write access to the ePCR File Server will be created for PremierOne CAD and the third-party ePCR system.

Access needs to be provided to the third-party ePCR system API or Stored Procedure. For the database update solution, a SQL account will be created for PremierOne CAD with access to the Stored Procedure in the third-party ePCR system database.

Customer is responsible to ensure security and usage of patient data in accordance with Health Insurance Portability and Accountability Act (HIPAA).

A.7.2.4 Performance

There are no explicit performance requirements for the Interface.

PremierOne CAD is set up to post transactional updates to the RDW database within 30 seconds.

A.7.2.5 High Availability and Disaster Recovery

There are no additional High Availability or Disaster Recovery requirements for the Interface, beyond the standard implementation for PremierOne CAD.

A.7.2.6 System Administration

Customer is responsible for contacting Motorola Solutions when changes occur in the third-party ePCR system data source, API, ePCR file server, or Customer Enterprise Network, which might affect the Interface.

Customer is responsible for keeping the reference data synchronized between PremierOne and the third-party ePCR system.

For the file extraction solution, Customer is responsible for regularly purging data and files from the servers and maintaining optimal system performance.

A.7.3 Statement of Work

A.7.3.1 Overview

This section defines the principal activities and responsibilities of Motorola Solutions and the Customer, during the interface deployment. This Statement of Work provides understanding of the work required by all parties for the interface implementation.

Motorola Solutions assumes no responsibility for training, installation, configuration, on-going support or warranty for any third-party systems and/or software not included as part of the contracted solution.

A.7.3.2 Responsibilities

Motorola Solutions Responsibilities

- Conduct an ISD review session with the Customer subject matter experts to obtain details regarding the connector type, connection details, data elements and triggering criteria.

- Provide Customer with the PremierOne CAD - ePCR Integration Workbook template to capture the system mapping.
- Implement the Interface.
- Provide guidance on hardware, software and network connectivity that may be required of Customer to support the interface implementation use and maintenance, prior to implementation.
- Conduct a functional demonstration validating the Interface works in accordance with this ISD.

Customer Responsibilities

- Participate in the ISD review session and provide details required for interface installation, configuration, test and support.
- Provide updated PremierOne CAD - ePCR integration workbook and filter criteria list (agency, incident type, status) document for the data extract.
- Familiarize themselves with this ISD.
- Provide all hardware, software and network connectivity not specifically provided by Motorola Solutions, prior to implementation.
- Procure all customer third-party licenses and API documentation, as required.
- The customer's third-party system must be on a version supported by the customer third-party. Customer will procure any required upgrades.
- Coordinate Customer third-party involvement with the implementation and testing of the Interface, as required.
- Witness the functional demonstration of the Interface.
- Protect the Enterprise Network against unauthorized access.
- Provide secure connections between PremierOne and the third-party ePCR system.
- Manage customer third-party responsibilities to completion, as applicable, enabling Motorola Solutions to complete its responsibilities.
- Manage communication between Motorola Solutions and Customer third-party, enabling Motorola Solutions to complete its responsibilities.

A.7.3.3 Implementation Plan

Table A-24: File Extract Implementation Plan

Task	Owner
Provide ePCR File Server.	Customer
Provide PremierOne Service Account read/write privilege to the ePCR File Server.	Customer
Provide Windows Service Accounts with read/write privilege to the ePCR File Server for the third-party ePCR system.	Customer
Establish network connectivity between PremierOne CAD and the ePCR File Server.	Customer

Task	Owner
Establish network connectivity between third-party ePCR system and the ePCR File Server.	Customer
Develop and install CSI component to extract and transfer PremierOne CAD data.	Motorola Solutions
Configure the Interface in PremierOne.	Motorola Solutions
Configure third-party ePCR system to consume PremierOne CAD data.	Customer

Table A-25: Database Update Implementation Plan

Task	Owner
Provide Stored Procedure and connection information to access the third-party ePCR system Database.	Customer
Establish network connectivity between PremierOne CAD and the third-party ePCR system Database.	Customer
Develop and install CSI component to extract and transfer PremierOne CAD data.	Motorola Solutions
Configure the Interface in PremierOne.	Motorola Solutions

Table A-26: API Call Implementation Plan

Task	Owner
Provide API and connection information to access the third-party ePCR system.	Customer
Establish network connectivity between PremierOne CAD and the third-party ePCR system.	Customer
Develop and install CSI component to extract and transfer PremierOne CAD data.	Motorola Solutions
Configure the Interface in PremierOne.	Motorola Solutions

A.8 PremierOne™ Suite - External Query Interface

A.8.1 Interface Description

A.8.1.1 Introduction

This Interface Specification Document (ISD) provides a description of the capabilities of PremierOne Suite External Query Interface (Interface) and the scope of work involved in delivering this Interface. Motorola Solutions will deploy the Interface and verify the functionality described in this ISD. If Customer desires any changes to this ISD scope, those changes can be addressed via the change provision of the contract.

A.8.1.2 Interface Overview

The Interface allows PremierOne users to submit transactions to a third-party system. These transactions are most typically ones that perform inquiries, although transactions that enter, modify, locate, and clear information are also possible.

Query requests made on PremierOne CAD, Records or Mobile clients are routed to one of the PremierOne application servers. The PremierOne Query Service processes the request and determines which data source(s) can fulfill the request. This information is passed to the PremierOne Common Services Interface (CSI) component, which translates the request to a query string and handles the connection to the data source. When a structured response is received, CSI parses the response and forwards it to PremierOne Messaging Service, which handles the routing of the query response to the requestor.

The CSI service can call a Stored Procedure on the third-party system database or call an Application Programming Interface (API) published by the third-party system to get the data. CSI has built-in connectors for Open Database Connectivity (ODBC), REST Web Service and Transmission Control Protocol (TCP) connection.

Figure A-25 shows the connectivity and primary data flow across the system.

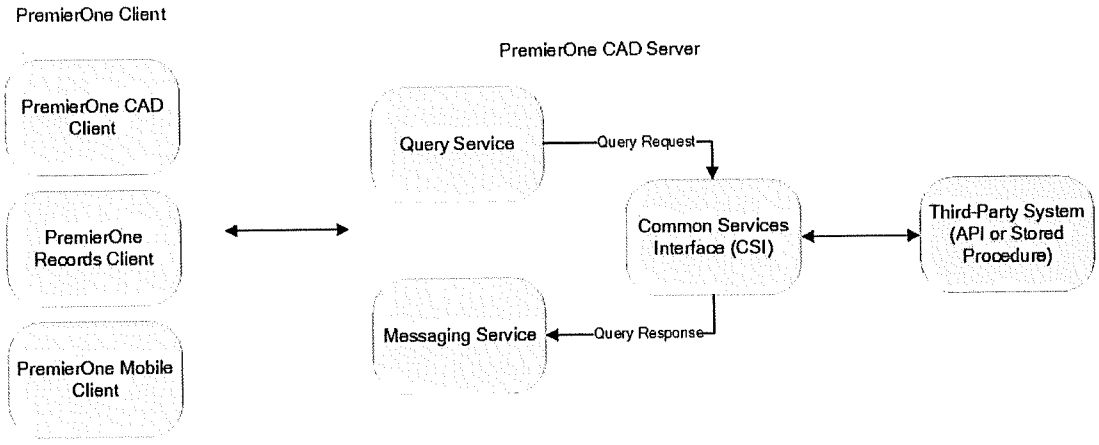


Figure A-25: External Query Interface Diagram

This interface implementation is limited to 6 forms with basic response formatting and 2 response types per request. Motorola Solutions will provide 8 hours of training and support for Customer to provision additional queries. This Interface requires modification to PremierOne CSI service. Motorola Solutions is reliant on receipt of the API or Stored Procedure and the associated design documents from the Customer to implement the Interface.

Information required for installation, configuration, test and support purposes regarding this Interface will be gathered during the ISD review.

A.8.1.3 Data Exchange

PremierOne services manage the data transformation and exchange process. CSI may direct a single query request to multiple systems, and each system will provide its own response.

The data flow diagram captures the events, triggers and message exchange between the systems.

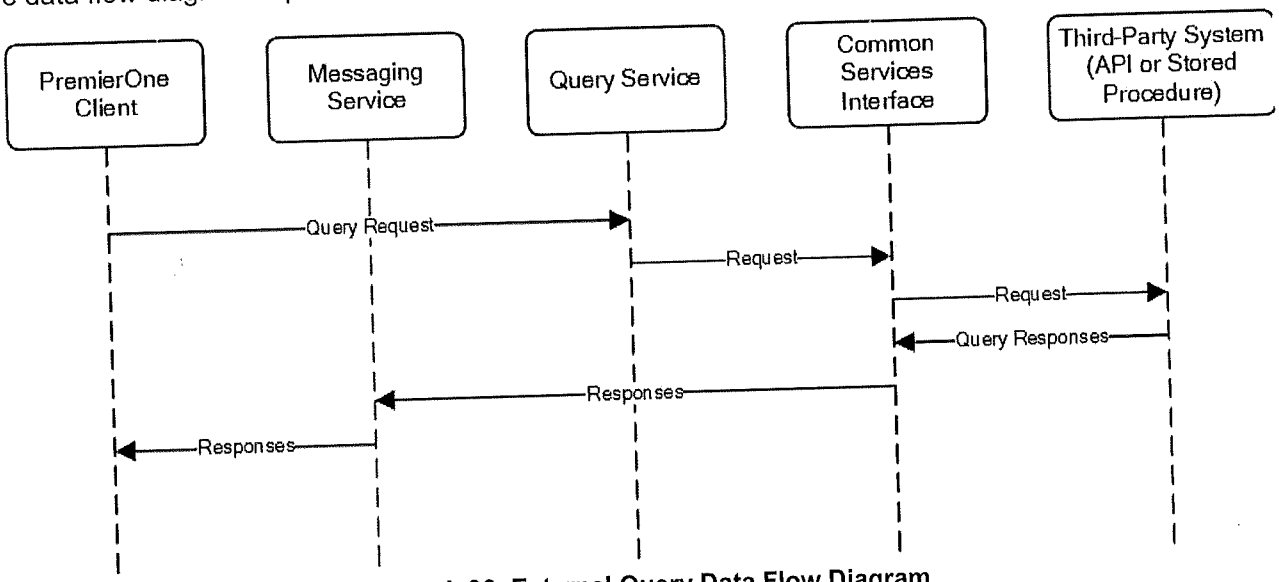


Figure A-26: External Query Data Flow Diagram

A.8.1.4 Business Process

None.

A.8.1.5 User Experience

PremierOne user can select a query type, enter the required query parameters and submit the query using a Query Request form similar to the sample in Figure A-27. The same query forms are available throughout the PremierOne Suite: CAD, Records and Mobile client. User access to the query forms is managed by the user roles provisioned in PremierOne.

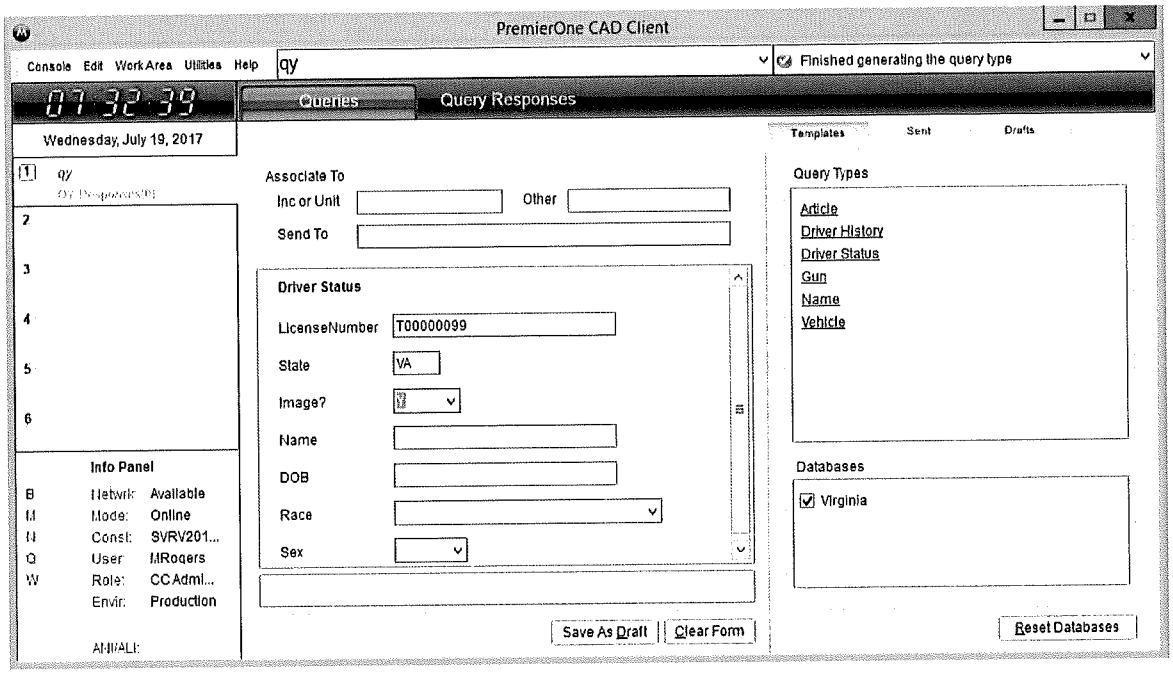


Figure A-27: Query Request Sample

PremierOne administrator may also create a command line version of a query form, similar to Figure A-28 command line query sample. This allows users to quickly submit frequently used queries. The administrator may also configure the system so queries can be submitted using person and vehicle information entered in an incident.

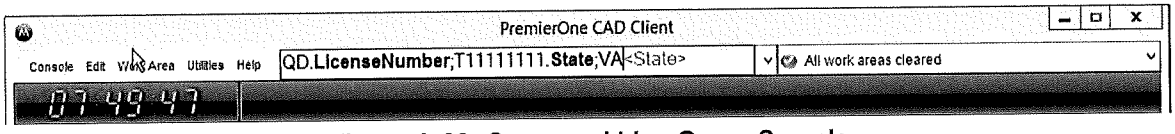


Figure A-28: Command Line Query Sample

Query Request forms are built upon the underlying data supplied by the third-party system. A form could use one or more underlying data sources. Thus, query responses from a particular form could be from multiple data sources.

Query responses are displayed in the Query Responses tab of the query window similar to the sample in Figure A-29. They may also be displayed in a dedicated window outside of the main CAD client window.

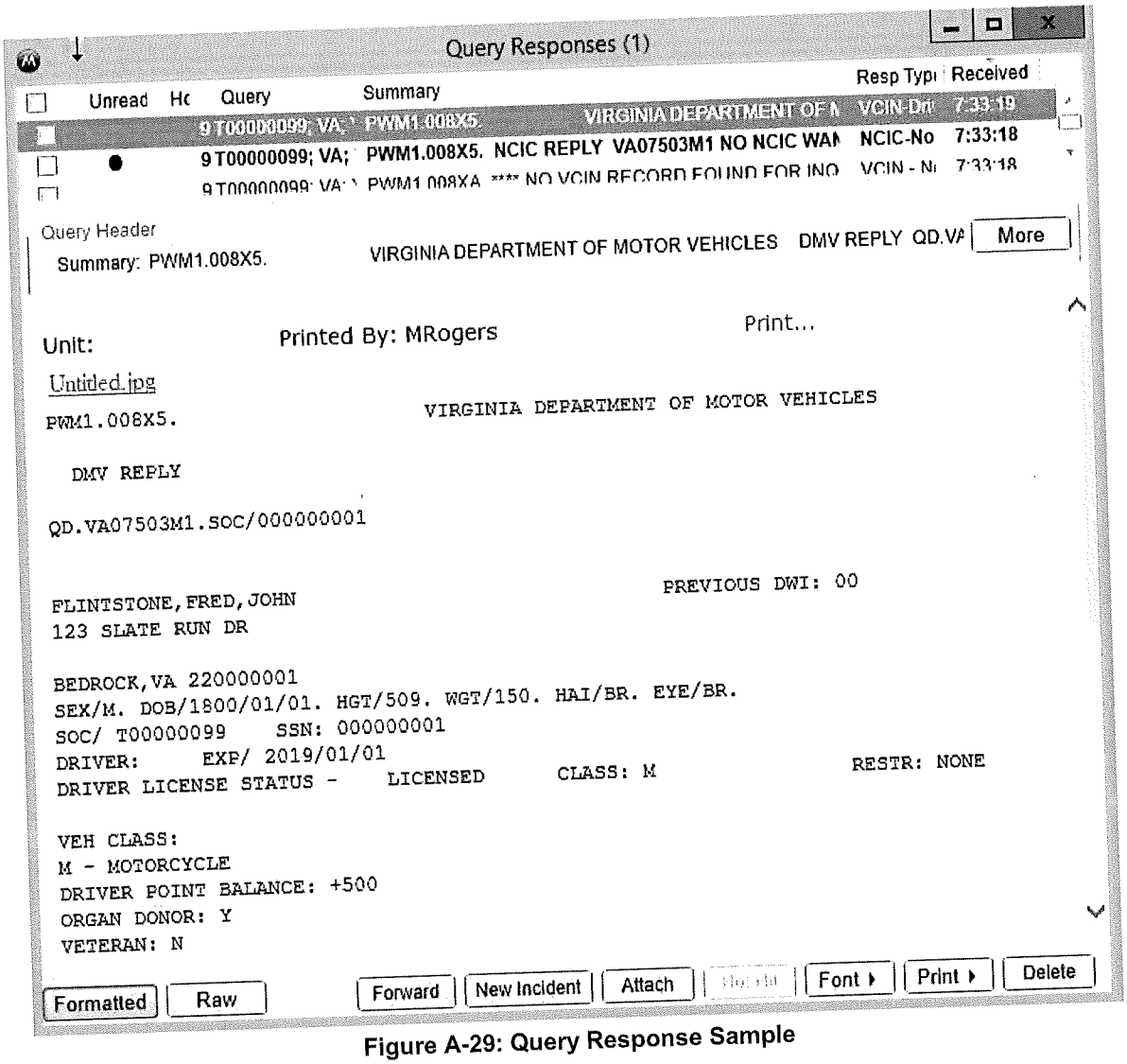


Figure A-29: Query Response Sample

If the third-party system provides a structured response, then this data is available as discrete values to PremierOne. This can be used to provide a visually formatted response that emphasizes key information. Figure A-30 provides a representative sample of a formatted query response.

Query Responses can be formatted for Workstations and Mobile clients. Query formatting is done using Extensible Stylesheet Language Transformations (XSLT) and the result is displayed using Hypertext Markup Language (HTML). The HTML transformation provides an enhanced level of formatting beyond the raw text that is returned in the query responses. The enhanced formatting can be helpful to call out specific data elements, or display images if they are included in the response from the third-party system.

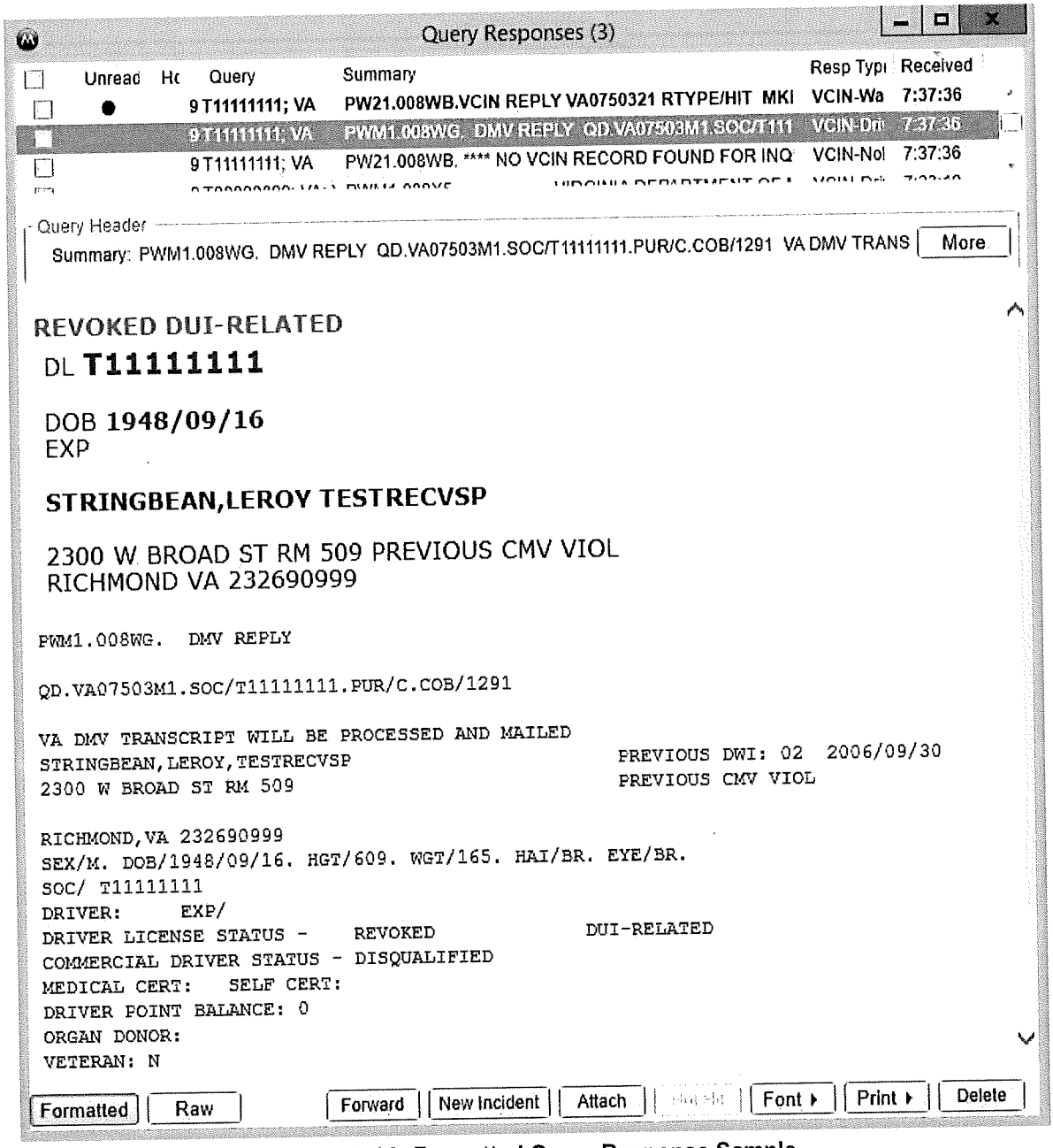


Figure A-30: Formatted Query Response Sample

A structured response may also be used to populate the person or vehicle information in an incident, without requiring the retyping of the information from a response. The user may run a query on a driver using their operator license number, and then use this feature to populate the person form with the person's details from the query response.

Cascading and drill-down queries can be provisioned by using details from the structured query response as input to subsequent queries. Cascading queries run automatically using these results and a drill-down query is run when the user clicks on the hyperlink on the response form.

The HTML transformation and structured response services are not in scope of the interface implementation. If these additional features are desired by the Customer, Motorola Solutions will provide a change order for Customer consideration for the enhanced response formatting.

A.8.1.6 Use Cases

Use Cases describe specific user and system interactions provided by the Interface. They provide traceability for the Test Cases in the Interface Test Procedure.

Table A-27: Use Cases

Use Cases	Description
UC-01	PremierOne user can submit a transaction from a form and view the responses.
UC-02	PremierOne user can submit a transaction from a command line and view the responses.
UC-03	PremierOne user can submit a transaction using the data in an incident and view the responses.
UC-04	PremierOne user can incorporate details from a response into an incident.

A.8.2 Operational Considerations

A.8.2.1 Connectivity

Connectivity needs to be established between PremierOne Suite and External Query Interface over the Customer Enterprise Network. Connectors supported by PremierOne are ODBC, REST Web Service and TCP.

A.8.2.2 Exception Handling and Logging

PremierOne exceptions are logged in both the Windows Event Log on the application server and the PremierOne database.

PremierOne logs query requests in the PremierOne reporting database.

A.8.2.3 Security

There are no additional security requirements for the Interface, beyond the standard implementation for PremierOne Suite. User access to the query forms are managed by user roles in PremierOne.

Access needs to be provided to the third-party system API or Stored Procedure. A SQL account with access to the Stored Procedure will be created in the third-party system database for PremierOne.

A.8.2.4 Performance

There are no explicit performance requirements for the Interface.

The query response is dependent on the third-party system connection and response time of the data sources. Query response is displayed as it is received from the third-party system.

A.8.2.5 High Availability and Disaster Recovery

There are no additional High Availability or Disaster Recovery requirements for the Interface, beyond the standard implementation for PremierOne Suite.

If available, the PremierOne recovery servers will be setup to access the third-party system for the Interface.

A.8.2.6 System Administration

Customer is responsible for contacting Motorola Solutions when changes occur in the Interface or Customer Enterprise Network, which might affect the Interface.

Customer is responsible for contacting Motorola Solutions when the third-party system changes the parameters or the response formats of the API or the Stored Procedure.

Customer is responsible for keeping the reference data synchronized between PremierOne and External Query Interface system.

Customer is responsible for regularly purging data and files from the servers and maintaining optimal system performance.

A.8.3 Statement of Work

A.8.3.1 General

The following Statement of Work (SOW) defines the scope of work involved in delivering an interface between Customer's Third-Party System and PremierOne CAD and Records System. This document includes the responsibilities of Motorola Solutions and the Customer.

A.8.3.2 Overview

This section defines the principal activities and responsibilities of Motorola Solutions and the Customer, during the interface deployment. This Statement of Work provides understanding of the work required by all parties for the interface implementation.

Motorola Solutions assumes no responsibility for training, installation, configuration, on-going support or warranty for any third-party systems and/or software not included as part of the contracted solution.

A.8.3.3 Responsibilities

Motorola Solutions Responsibilities

- Conduct an ISD review session with the Customer subject matter experts to obtain details regarding the Interface including connector type, connection details, transaction types, query criteria and response transformation.
- Implement the Interface for 6 forms with basic response formatting and 2 response types per request. Provide 8 hours of training and support for Customer to provision additional queries.
- Provide guidance on hardware, software and network connectivity that may be required of Customer to support the interface implementation use and maintenance, prior to implementation.

- Conduct a functional demonstration validating the Interface works in accordance with this ISD.

Customer Responsibilities

- Participate in the ISD review session and provide details required for interface installation, configuration, test and support.
- Familiarize themselves with this ISD.
- Provide all hardware, software and network connectivity not specifically provided by Motorola Solutions, prior to implementation.
- Provide the external database driver to enable ODBC connection, if required.
- Assist with provisioning Query Forms, Hot Hits, Pick Lists and Response Formats.
- Procure all customer third-party licenses and API documentation, as required.
- The customer's third-party system must be on a version supported by the customer third-party. Customer will procure any required upgrades.
- Coordinate Customer third-party involvement with the implementation and testing of the Interface, as required.
- Witness the functional demonstration of the Interface.
- Protect the Enterprise Network against unauthorized access.
- Provide secure connections between PremierOne and the Interface.
- Manage customer third-party responsibilities to completion, as applicable, enabling Motorola Solutions to complete its responsibilities.
- Manage communication between Motorola Solutions and Customer third-party, enabling Motorola Solutions to complete its responsibilities.

A.8.3.4 Implementation Plan

Table A-28: Implementation Plan

Task	Owner
Provide Stored Procedure or API to query the third-party system.	Customer / third-party system vendor
Provide associated user guide or design documentation for the Stored Procedure or API.	Customer / third-party system vendor
Establish network connectivity between PremierOne and the third-party system.	Customer
Provide the external database driver software and user's guide to enable ODBC access.	Customer
Develop and install CSI component to query the third-party system.	Motorola Solutions
Configure Query Interface in PremierOne.	Motorola Solutions
Provision Query Request Form in PremierOne.	Motorola Solutions / Customer
Configure Query Response in PremierOne for Workstation and Mobile.	Motorola Solutions / Customer
Provision user roles to access the query in PremierOne.	Customer

EXHIBIT C

Additional Terms and Conditions

1. Subscription Software Addendum

This Subscription Software Addendum (this "**SSA**") including its Exhibit, forms part of the Master Purchase Agreement ("MPA" or "Agreement") to reflect the parties' agreement with regard to the subscription services. Capitalized terms used in this SSA, but not defined herein, will have the meanings set forth in the MPA.

1. Addendum. This SSA governs Customer's purchase of Subscription Software (and, if set forth in the Proposal) from Motorola, and will form part of the Parties' Agreement. Additional Subscription Software-specific Addenda or other terms and conditions may apply to certain Subscription Software, where such terms are provided or presented to Customer.

2. Delivery of Subscription Software.

2.1. Delivery. During the applicable Subscription Term (as defined below), Motorola will provide to Customer the Subscription Software set forth in an Ordering Document, in accordance with the terms of the Agreement. Motorola will provide Customer advance notice (which may be provided electronically) of any planned downtime. Delivery will occur upon Customer's receipt of credentials required for access to the Subscription Software or upon Motorola otherwise providing access to the Subscription Software. If agreed upon in an Ordering Document, Motorola will also provide Services related to such Subscription Software.

2.2. Modifications. In addition to other rights to modify the products and services set forth in the MPA, Motorola may modify the Subscription Software, any associated recurring Services and any related systems so long as their functionality (as described in the applicable Ordering Document) is not materially degraded. Documentation for the Subscription Software may be updated to reflect such modifications. For clarity, new features or enhancements that are added to any Subscription Software may be subject to additional Fees.

2.3. User Credentials. If applicable, Motorola will provide Customer with administrative user credentials for the Subscription Software, and Customer will ensure such administrative user credentials are accessed and used only by Customer's employees with training on their proper use. Customer will protect, and will cause its Authorized Users to protect, the confidentiality and security of all user credentials, including any administrative user credentials, and maintain user credential validity, including by updating passwords. Customer will be liable for any use of the Subscription Software through such user credential (including through any administrative user credentials), including any changes made to the Subscription Software or issues or user impact arising therefrom. To the extent Motorola provides Services to Customer in order to help resolve issues resulting from changes made to the Subscription Software through user credentials, including through any administrative user credentials, or issues otherwise created by Authorized Users, such Services will be billed to Customer on a time and materials basis, and Customer will pay all invoices in accordance with the payment terms of the MPA.

2.4. Beta Services. If Motorola makes any beta version of a software application ("**Beta Service**") available to Customer, Customer may choose to use such Beta Service at its own discretion, provided, however, that Customer will use the Beta Service solely for purposes of Customer's evaluation of such Beta Service, and for no other purpose. Customer acknowledges and agrees that all Beta Services are

offered "as-is" and without any representations or warranties or other commitments or protections from Motorola. Motorola will determine the duration of the evaluation period for any Beta Service, in its sole discretion, and Motorola may discontinue any Beta Service at any time. Customer acknowledges that Beta Services, by their nature, have not been fully tested and may contain defects or deficiencies.

3. Subscription Software License and Restrictions.

3.1. Subscription Software License. Subject to Customer's and its Authorized Users' compliance with the Agreement, including payment terms, Motorola hereby grants Customer and its Authorized Users a limited, non-transferable, non-sublicenseable, and non-exclusive license to use the Subscription Software identified in an Ordering Document, and the associated Documentation, solely for Customer's internal business purposes. The foregoing license grant will be limited to use in the territory and to the number of licenses set forth in an Ordering Document (if applicable), and will continue for the applicable Subscription Term. Customer may access, and use the Subscription Software only in Customer's owned or controlled facilities, including any authorized mobile sites; provided, however, that Authorized Users using authorized mobile or handheld devices may also log into and access the Subscription Software remotely from any location. No custom development work will be performed under this Addendum.

3.2. End User Licenses. Notwithstanding any provision to the contrary in the Agreement, certain Subscription Software is governed by a separate license, EULA, or other agreement, including terms governing third-party software, such as open source software, included in the Subscription Software. Customer will comply, and ensure its Authorized Users comply, with such additional license agreements.

3.3. Customer Restrictions. Customers and Authorized Users will comply with the applicable Documentation and the copyright laws of the United States and all other relevant jurisdictions (including the copyright laws where Customer uses the Subscription Software) in connection with their use of the Subscription Software. Customer will not, and will not allow others including the Authorized Users, to make the Subscription Software available for use by unauthorized third parties, including via a commercial rental or sharing arrangement; reverse engineer, disassemble, or reprogram software used to provide the Subscription Software or any portion thereof to a human-readable form; modify, create derivative works of, or merge the Subscription Software or software used to provide the Subscription Software with other software; copy, reproduce, distribute, lend, or lease the Subscription Software or Documentation for or to any third party; take any action that would cause the Subscription Software, software used to provide the Subscription Software, or Documentation to be placed in the public domain; use the Subscription Software to compete with Motorola; remove, alter, or obscure, any copyright or other notice; share user credentials (including among Authorized Users); use the Subscription Software to store or transmit malicious code; or attempt to gain unauthorized access to the Subscription Software or its related systems or networks.

4. Term.

4.1. Subscription Terms. The duration of Customer's subscription to the first Subscription Software and any associated recurring Services ordered under this SSA (or the first Subscription Software or recurring Service, if multiple are ordered at once) will commence upon delivery of such Subscription Software (and recurring Services, if applicable) and will continue for a twelve (12) month period or such longer period identified in an Ordering Document (the "**Initial Subscription Period**"). Following the Initial Subscription Period, Customer's subscription to the Subscription Software and any recurring Services will automatically renew for additional twelve (12) month periods (each, a "**Renewal Subscription Year**"), unless either Party notifies the other Party of its intent not to renew at least thirty (30) days before the conclusion of the then-current Subscription Term. (The Initial Subscription Period

and each Renewal Subscription Year will each be referred to herein as a "**Subscription Term**".) Motorola may increase Fees prior to any Renewal Subscription Year. In such case, Motorola will notify Customer of such proposed increase no later than thirty (30) days prior to commencement of such Renewal Subscription Year. Unless otherwise specified in the applicable Ordering Document, if Customer orders any additional Subscription Software or recurring Services under this SSA during an in-process Subscription Term, the subscription for each new Subscription Software or recurring Service will (a) commence upon delivery of such Subscription Software or recurring Service, and continue until the conclusion of Customer's then-current Subscription Term (a "**Partial Subscription Year**"), and (b) automatically renew for Renewal Subscription Years thereafter, unless either Party notifies the other Party of its intent not to renew at least thirty (30) days before the conclusion of the then-current Subscription Term. Thus, unless otherwise specified in the applicable Ordering Document, the Subscription Terms for all Subscription Software and recurring Services hereunder will be synchronized.

4.2. Term. The term of this SSA (the "**SSA Term**") will commence once both parties execute this amendment two.

4.3. Termination. Notwithstanding the termination provisions of the MPA, Motorola may terminate this SSA (or any Addendum or Ordering Documents hereunder), or suspend delivery of Subscription Software or Services, immediately upon notice to Customer if (a) Customer breaches **Section 3 – Subscription Software License and Restrictions** of this SSA, or any other provision related to Subscription Software license scope or restrictions set forth in an Addendum or Ordering Document, or (b) it determines that Customer's use of the Subscription Software poses, or may pose, a security or other risk or adverse impact to any Subscription Software, Motorola, Motorola's systems, or any third party (including other Motorola customers). Customer acknowledges that Motorola made a considerable investment of resources in the development, marketing, and distribution of the Subscription Software and Documentation, and that Customer's breach of the Agreement will result in irreparable harm to Motorola for which monetary damages would be inadequate. If Customer breaches this Agreement, in addition to termination, Motorola will be entitled to all available remedies at law or in equity (including immediate injunctive relief).

4.4. Wind Down of Subscription Software. In addition to the termination rights in the MPA, Motorola may terminate any Ordering Document and Subscription Term, in whole or in part, in the event Motorola plans to cease offering the applicable Subscription Software or Service to customers.

5. Payment.

5.1. Payment. Unless otherwise provided in an Ordering Document (and notwithstanding the provisions of the MPA), Customer will prepay an annual subscription Fee set forth in an Ordering Document for each Subscription Software and associated recurring Service, before the commencement of each Subscription Term. For any Partial Subscription Year, the applicable annual subscription Fee will be prorated based on the number of months in the Partial Subscription Year. The annual subscription Fee for Subscription Software and associated recurring Services may include certain one-time Fees, such as start-up fees, license fees, or other fees set forth in an Ordering Document. Motorola will have the right to suspend the Subscription Software and any recurring Services if Customer fails to make any payments when due.

5.2. License True-Up. Motorola will have the right to conduct an audit of total user licenses credentialed by Customer for any Subscription Software during a Subscription Term, and Customer will cooperate with such audit. If Motorola determines that Customer's usage of the Subscription Software during the applicable Subscription Term exceeded the total number of licenses purchased by Customer, Motorola may invoice Customer for the additional licenses used by Customer, pro-rated for

each additional license from the date such license was activated, and Customer will pay such invoice in accordance with the payment terms in the MPA.

6. Liability.

6.1. ADDITIONAL EXCLUSIONS. IN ADDITION TO THE EXCLUSIONS FROM DAMAGES SET FORTH IN THE MPA, AND NOTWITHSTANDING ANY PROVISION OF THE AGREEMENT TO THE CONTRARY, MOTOROLA WILL HAVE NO LIABILITY FOR (A) INTERRUPTION OR FAILURE OF CONNECTIVITY, VULNERABILITIES, OR SECURITY EVENTS; (B) DISRUPTION OF OR DAMAGE TO CUSTOMER'S OR THIRD PARTIES' SYSTEMS, EQUIPMENT, OR DATA, INCLUDING DENIAL OF ACCESS TO USERS, OR SHUTDOWN OF SYSTEMS CAUSED BY INTRUSION DETECTION SOFTWARE OR HARDWARE; (C) AVAILABILITY OR ACCURACY OF ANY DATA AVAILABLE THROUGH THE SUBSCRIPTION SOFTWARE OR SERVICES, OR INTERPRETATION, USE, OR MISUSE THEREOF; (D) TRACKING AND LOCATION-BASED SERVICES; OR (E) BETA SERVICES.

6.2. Voluntary Remedies. Motorola is not obligated to remedy, repair, replace, or refund the purchase price for the disclaimed or excluded issues in the MPA or **Section 6.1 – Additional Exclusions** above, but if Motorola agrees to provide Services to help resolve such issues, Customer will reimburse Motorola for its reasonable time and expenses, including by paying Motorola any Fees set forth in an Ordering Document for such Services, if applicable.

7. Motorola as a Controller or Joint Controller. In all instances where Motorola acts as a controller of data, it will comply with the applicable provisions of the Motorola Privacy Statement at https://www.motorolasolutions.com/en_us/about/privacy-policy.html#privacystatement, as may be updated from time to time. Motorola holds all Customer Contact Data as a controller and shall Process such Customer Contact Data in accordance with the Motorola Privacy Statement. In instances where Motorola is acting as a joint controller with Customer, the Parties will enter into a separate Addendum to the Agreement to allocate the respective roles as joint controllers.

8. Survival. The following provisions will survive the expiration or termination of this SSA for any reason: **Section 4 – Term**; **Section 5 – Payment**; **Section 6.1 – Additional Exclusions**; **Section 8 – Survival**.

Subscription Services Addendum
Exhibit A: FirstNet and AT&T Service Terms
Public Safety Entity ("Customer") Responsibilities for access to and use of "First Net" Service as provided by
AT&T

General. The Customer is responsible for complying with AT&T Acceptable Use Policy found at att.com/aup and applicable AT&T Service Guides found at att.com/servicepublications.

Privacy. The Customer is responsible for complying with all applicable privacy laws. The Customer is responsible for obtaining consent from and giving notice to its Users regarding Motorola's and AT&T's collection and use of User information in connection with a Service. The Customer will only make accessible or provide Personal Data to Motorola and AT&T when it has the legal authority to do so.

User Eligibility. The Customer shall verify, or assist Motorola and AT&T in verifying, as stated below, the eligibility of its Users to use the Service. The Customer is required to verify and confirm that its Users are authorized and eligible to use Service. The Customer must perform periodic audits on a regular, but not less than once per year, basis to identify anyindividuals who are no longer eligible for Service. The Customer must produce such information as may be requested through AT&T by the FirstNet Authority and the United States Government to verify eligibility of its users.

Limitations on the Service. THE CUSTOMER ACKNOWLEDGES THAT SERVICE IS MADE AVAILABLE ONLY WITHINTHE OPERATING RANGE OF THE NETWORKS. SERVICE MAY BE TEMPORARILY REFUSED, INTERRUPTED, ORLIMITED BECAUSE OF: (A) FACILITIES LIMITATIONS; (B) TRANSMISSION LIMITATIONS CAUSED BY ATMOSPHERIC,TERRAIN, OTHER NATURAL OR ARTIFICIAL CONDITIONS ADVERSELY AFFECTING TRANSMISSION, WEAKBATTERIES, SYSTEM OVERCAPACITY, MOVEMENT OUTSIDE A SERVICE AREA OR GAPS IN COVERAGE IN A SERVICE AREA AND OTHER CAUSES REASONABLY OUTSIDE OF MOTOROLA OR AT&T'S CONTROL SUCH AS, BUT NOT LIMITED TO, INTENTIONAL OR NEGLIGENT ACTS OF THIRD PARTIES THAT DAMAGE OR IMPAIR THE NETWORK OR DISRUPT SERVICE; OR (C) EQUIPMENT MODIFICATIONS, UPGRADES, RELOCATIONS, REPAIRS, AND OTHER SIMILAR ACTIVITIES NECESSARY FOR THE PROPER OR IMPROVED OPERATION OF SERVICE.

Limitations on Service of Carrier Partners. CARRIER PARTNER NETWORKS ARE MADE AVAILABLE AS-IS AND MOTOROLA AND AT&T MAKES NO WARRANTIES OR REPRESENTATIONS AS TO THE AVAILABILITY OR QUALITY OF ROAMING SERVICE PROVIDED BY CARRIER PARTNERS, AND MOTOROLA AND AT&T WILL NOT BE LIABLE IN ANY CAPACITY FOR ANY ERRORS, OUTAGES, OR FAILURES OF CARRIER PARTNER NETWORKS. ROAMING ON CARRIER PARTNER NETWORKS OUTSIDE THE FIRSTNET SERVICE AREA (IF ANY) SHALL BE AVAILABLE AS DESCRIBIED IN THE SERVICE GUIDE.

User Disclosures. THE CUSTOMER UNDERSTANDS AND AGREES THAT IT: (1) HAS NO CONTRACTUAL RELATIONSHIP WITH THE UNDERLYING WIRELESS SERVICE CARRIER; (2) IS NOT A THIRD PARTY BENEFICIARY OF ANY AGREEMENT BETWEEN [CUSTOMER] AND THE UNDERLYING CARRIER; (3) THAT THE UNDERLYING CARRIER HAS NO LIABILITY OF ANY KIND TO [USER], WHETHER FOR BREACH OF CONTRACT, WARRANTY, NEGLIGENCE, STRICT LIABILITY IN TORT OR OTHERWISE; AND (4) THAT DATA TRANSMISSIONS AND MESSAGES MAY BE DELAYED, DELETED OR NOT DELIVERED, AND 911 OR SIMILAR EMERGENCY CALLS MAY NOT BE COMPLETED

Medical Devices (FDA and HIPAA Responsibilities). The Customer shall be responsible for FDA compliance as a "distributor" of the Device to its users. Except as necessary to provide the Service to the Customer, The Customer shall not convey any protected health information ("PHI") to AT&T, as that term is defined in the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health ("HITECH") Act regulations. Motorola and/or AT&T shall not function as the Customer's business associate in rendering the Services; such Services will be limited to providing conduit or mere data transmission services to the Customer in accordance

with guidance on the "conduit exception" under HIPAA. Each Party shall bear its own costs associated with regulatory compliance.

Audits. Customer may be subject to occasional audits by AT&T or its agents to verify compliance with this Exhibit A.

2. Data Processing Addendum

This Data Processing Addendum, including its Schedules and Annexes ("DPA"), forms part of the Master Purchase Agreement ("MPA" or "Agreement")) to reflect the parties' agreement with regard to the Processing of Customer Data, which may include Personal Data. In the event of a conflict between this DPA, the MPA or any Schedule, Annex or other addenda to the MPA, this DPA must prevail.

When Customer renews or purchases new Products or Services, the then-current DPA must apply and must not change during the applicable Term. When Motorola provides new features or supplements the Product or Service, Motorola may provide additional terms or make updates to this DPA that must apply to Customer's use of those new features or supplements.

1. Definitions.

All capitalized terms not defined herein must have the meaning set forth in the Agreement.

"**Customer Data**" means data including images, text, videos, and audio that are provided to Motorola by, through, or on behalf of Customer and its Authorized Users or their end users, through the use of the products and services. Customer Data does not include Customer Contact Data, Service Use Data, other than that portion comprised of Personal Information, or Third Party Data.

"Customer Contact Data" means data Motorola collects from Customer, its Authorized Users, and their end users for business contact purposes, including without limitation marketing, advertising, licensing, and sales purposes.

"Data Protection Laws" means all data protection laws and regulations applicable to a Party with respect to the Processing of Personal Data under the Agreement.

"Data Subjects" means the identified or identifiable person to whom Personal Data relates.

"Metadata" means data that describes other data.

"Motorola Data" means data owned by Motorola and made available to Customer in connection with the Products and Services.

"Personal Data" or **"Personal Information"** means any information relating to an identified or identifiable natural person transmitted to Motorola by, through, or on behalf of Customer and its Authorized Users or their end users as part of Customer Data. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Process" or **"Processing"** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, copying, analyzing, caching, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Security Incident" means an incident leading to the accidental or unlawful destruction, loss, alteration or disclosure of, or access to Customer Data, which may include Personal Data, while processed by Motorola. .

"**Service Use Data**" means data generated about the use of the Products and Services through Customer's use or Motorola's support of the Products and Services, which may include Metadata, Personal Data, product performance and error information, activity logs, and date and time of use.

"**Sub-processor**" means other processors engaged by Motorola to Process Customer Data which may include Personal Data.

"**Third Party Data**" means information obtained by Motorola from publicly available sources or its third party content providers and made available to Customer through the Products or Services.

2. Processing of Customer Data

2.1. Roles of the Parties. The Parties agree that with regard to the Processing of Personal Data hereunder, Customer is the Controller and Motorola is the Processor who may engage Sub-processors pursuant to the requirements of **Section 6** entitled "Sub-processors" below.

2.2. Motorola's Processing of Customer Data. Motorola and Customer agree that Motorola may use and Process Customer Data, including the Personal Information embedded in Service Use Data, only in accordance with Customer's documented instructions for the following purposes: (i) to perform Services and provide Products under the Agreement; (ii) analyze Customer Data to operate, maintain, manage, and improve Motorola products and services; and (iii) create new products and services. Customer agrees that its Agreement (including this DPA), along with the Product and Service Documentation and Customer's use and configuration of features in the Products and Services, are Customer's complete and final documented instructions to Motorola for the processing of Customer Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer's Agreement. Customer represents and warrants to Motorola that Customer's instructions, including appointment of Motorola as a Processor or sub-processor, have been authorized by the relevant controller. Customer Data may be processed by Motorola at any of its global locations and/or disclosed to Sub-processors. It is Customer's responsibility to notify Authorized Users of Motorola's collection and use of Customer Data, and to obtain any required consents, provide all necessary notices, and meet any other applicable legal requirements with respect to such collection and use. Customer represents and warrants to Motorola that it has complied with the terms of this provision.

2.3. Details of Processing. The subject-matter of Processing of Personal Data by Motorola hereunder, the duration of the Processing, the categories of Data Subjects and types of Personal Data are set forth on **Annex I** to this DPA.

2.4. Disclosure of Processed Data. Motorola must not disclose Customer Data to any third party except to Motorola's suppliers and channel partners as necessary to provide the products and services unless permitted under this Agreement, authorized by Customer or required by law. In the event a government or supervisory authority demands access to Customer Data, to the extent allowable by law, Motorola must provide Customer with notice of receipt of the demand to provide sufficient time for Customer to seek appropriate relief in the relevant jurisdiction. In all circumstances, Motorola retains the right to comply with applicable law.

2.5. Customer's Obligations. Customer is solely responsible for its compliance with all Data Protection Laws and establishing and maintaining its own policies and procedures to ensure such compliance. Customer must not use the Products and Services in a manner that would violate applicable Data Protection Laws. Customer must have sole responsibility for (i) the lawfulness of any transfer of Personal Data to Motorola, (ii) the accuracy, quality, and legality of Personal Data provided to Motorola; (iii) the means by which Customer acquired Personal Data, and (iv) the provision of any

required notices to, and obtaining any necessary acknowledgements, authorizations or consents from Data Subjects. Customer takes full responsibility to keep the amount of Personal Data provided to Motorola to the minimum necessary for Motorola to perform in accordance with the Agreement. Customer must be solely responsible for its compliance with applicable Data Protection Laws.

2.6. Customer Indemnity. To the extent allowed by law, Customer will defend, indemnify, and hold Motorola and its subcontractors, subsidiaries and other affiliates harmless from and against any and all damages, losses, liabilities, and expenses (including reasonable fees and expenses of attorneys) arising from any actual or threatened third-party claim, demand, action, or proceeding arising from or related to Customer's failure to comply with its obligations under this Agreement and/or applicable Data Protection Laws. Motorola will give Customer prompt, written notice of any claim subject to the foregoing indemnity. Motorola will, at its own expense, cooperate with Customer in its defense or settlement of the claim.

3. Service Use Data. Except to the extent that it is Personal Information, Customer understands and agrees that Motorola may collect and use Service Use Data for its own purposes, provided that such purposes are compliant with applicable Data Protection Laws. Service Use Data may be processed by Motorola at any of its global locations and/or disclosed to Sub-processors.

4. Third-Party Data and Motorola Data. Motorola Data and Third Party Data may be available to Customer through the Products and Services. Customer and its Authorized Users may use the Motorola Data and Third Party Data as permitted by Motorola and the applicable third-party data provider, as described in the Agreement or applicable Addendum. Unless expressly permitted in the Agreement or applicable Addendum, Customer must not, and must ensure its Authorized Users must not: (a) use the Motorola Data or Third-Party Data for any purpose other than Customer's internal business purposes or disclose the data to third parties; (b) "white label" such data or otherwise misrepresent its source or ownership, or resell, distribute, sublicense, or commercially exploit the data in any manner; (c) use such data in violation of applicable laws ; (d) use such data for activities or purposes where reliance upon the data could lead to death, injury, or property damage; (e) remove, obscure, alter, or falsify any marks or proprietary rights notices indicating the source, origin, or ownership of the data; or (f) modify such data or combine it with Customer Data or other data or use the data to build databases. Additional restrictions may be set forth in the Agreement or applicable Addendum. Any rights granted to Customer or Authorized Users with respect to Motorola Data or Third-Party Data must immediately terminate upon termination or expiration of the applicable Addendum, Ordering Document, or the MPA. Further, Motorola or the applicable Third Party Data provider may suspend, change, or terminate Customer's or any Authorized User's access to Motorola Data or Third-Party Data if Motorola or such Third Party Data provider believes Customer's or the Authorized User's use of the data violates the Agreement, applicable law or by Motorola's agreement with the applicable Third Party Data provider. Upon termination of Customer's rights to use of any Motorola Data or Third-Party Data, Customer and all Authorized Users must immediately discontinue use of such data, delete all copies of such data, and certify such deletion to Motorola. Notwithstanding any provision of the Agreement to the contrary, Motorola has no liability for Third-Party Data or Motorola Data available through the Products and Services. Motorola and its Third Party Data providers reserve all rights in and to Motorola Data and Third-Party Data not expressly granted in an Addendum or Ordering Document.

5. Motorola as a Controller or Joint Controller. In all instances where Motorola acts as a Controller it must comply with the applicable provisions of the Motorola Privacy Statement at https://www.motorolasolutions.com/en_us/about/privacy-policy.html#privacystatement as each may be updated from time to time. Motorola holds all Customer Contact Data as a Controller and must Process such Customer Contact Data in accordance with the Motorola Privacy Statement. In instances where

Motorola is acting as a Joint Controller with Customer, the Parties must enter into a separate addendum to the Agreement to allocate the respective roles as joint controllers.

6. Sub-processors.

6.1. Use of Sub-processors. Customer agrees that Motorola may engage Sub-processors who in turn may engage Sub-processors to Process Personal Data in accordance with the DPA. A current list of Sub-processors is set forth at **Annex III**. When engaging Sub-processors, Motorola must enter into agreements with the Sub-processors to bind them to obligations which are substantially similar or more stringent than those set out in this DPA.

7. Changes to Sub-processing. The Customer hereby consents to Motorola engaging Sub-processors to process Customer Data provided that: (i) Motorola must use its reasonable endeavors to provide at least 10 days' prior notice of the addition or removal of any Sub-processor, which may be given by posting details of such addition or removal at a URL provided to Customer in **Annex III**; (ii) Motorola imposes data protection terms on any Sub-processor it appoints that protect the Customer Data to the same standard provided for by this Addendum; and (iii) Motorola remains fully liable for any breach of this clause that is caused by an act, error or omission of its Sub-processor(s). The Customer may object to Motorola's appointment or replacement of a Sub-processor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, Motorola will either appoint or replace the Sub-processor or, if in Motorola's discretion this is not feasible, the Customer may suspend or terminate this Agreement. **Data Subject Requests.** Motorola must, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject, including without limitation requests for access to, correction, amendment, transport or deletion of such Data Subject's Personal Data and, to the extent applicable, Motorola must provide Customer with commercially reasonable cooperation and assistance in relation to any complaint, notice, or communication from a Data Subject. Customer must respond to and resolve promptly all requests from Data Subjects which Motorola provides to Customer. Customer must be responsible for any reasonable costs arising from Motorola's provision of such assistance under this Section. **Data Transfers**

Motorola agrees that it must not make transfers of Personal Data under this Agreement from one jurisdiction to another unless such transfers are performed in compliance with this Addendum and applicable Data Protection Laws. Motorola agrees to enter into appropriate agreements with its affiliates and Sub-processors, which will permit Motorola to transfer Personal Data to its affiliates and Sub-processors. Motorola agrees to amend as necessary its agreement with Customer to permit transfer of Personal Data from Motorola to Customer. Motorola also agrees to assist the Customer in entering into agreements with its affiliates and Sub-processors if required by applicable Data Protection Laws for necessary transfers.

8. Security. Motorola must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed by the Processing of Personal Data, taking into account the costs of implementation; the nature, scope, context, and purposes of the Processing; and the risk of varying likelihood and severity of harm to the data subjects. The appropriate technical and organizational measures implemented by Motorola are set forth in **Annex III**. In assessing the appropriate level of security, Motorola must weigh the risks presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise Processed.

9. Security Incident Notification. If Motorola becomes aware of a Security Incident, then Motorola must (i) notify Customer of the Security Incident without undue delay, (ii) investigate the

Security Incident and apprise Customer of the details of the Security Incident and (iii) take commercially reasonable steps to stop any ongoing loss of Personal Data due to the Security Incident if in the control of Motorola. Notification of a Security Incident must not be construed as an acknowledgement or admission by Motorola of any fault or liability in connection with the Security Incident. Motorola must make reasonable efforts to assist Customer in fulfilling Customer's obligations under Data Protection Laws to notify the relevant supervisory authority and Data Subjects about such incident.

10. Data Retention and Deletion.

Except for anonymized Customer Data, as described above, or as otherwise provided under the Agreement, Motorola must delete all Customer Data no later than ninety (90) days following termination or expiration of the MPA or the applicable Addendum or Ordering Document unless otherwise required to comply with applicable law.

11. Audit Rights

11.1 Periodic Audit. Motorola will allow Customer to perform an audit of reasonable scope and duration of Motorola operations relevant to the Products and Services purchased under the Agreement, at Customer's sole expense, for verification of compliance with the technical and organizational measures set forth in **Annex II** if (i) Motorola notifies Customer of a Security Incident that results in actual compromise to the Products and/or Services purchased; or (ii) if Customer reasonably believes Motorola is not in compliance with its security commitments under this DPA, or (iii) if such audit is legally required by the Data Protection Laws. Any audit must be conducted in accordance with the procedures set forth in **Section 11.3** of this DPA and may not be conducted more than one time per year. If any such audit requires access to confidential information of Motorola's other customers, suppliers or agents, such portion of the audit may only be conducted by Customer's nationally recognized independent third party auditors in accordance with the procedures set forth in **Section 11.3** of this DPA. Unless mandated by GDPR or otherwise mandated by law or court order, no audits are allowed within a data center for security and compliance reasons. Motorola must, in no circumstances, provide Customer with the ability to audit any portion of its software, products, and services which would be reasonably expected to compromise the confidentiality of any third party's information or Personal Data.

11.2 Satisfaction of Audit Request. Upon receipt of a written request to audit, and subject to Customer's agreement, Motorola may satisfy such audit request by providing Customer with a confidential copy of a Motorola's applicable most recent third party security review performed by a nationally recognized independent third party auditor, such as a SOC2 Type II report or ISO 27001 certification, in order that Customer may reasonably verify Motorola's compliance with national standards.

11.3 Audit Process. Customer must provide at least sixty days (60) days prior written notice to Motorola of a request to conduct the audit described in **Section 11.1**. All audits must be conducted during normal business hours, at applicable locations or remotely, as designated by Motorola. Audit locations, if not remote will generally be those location(s) where Customer Data is accessed, or Processed. The audit must not unreasonably interfere with Motorola's day to day operations. An audit must be conducted at Customer's sole cost and expense and subject to the terms of the confidentiality obligations set forth in the Agreement. Before the commencement of any such audit, Motorola and Customer must mutually agree upon the time, and duration of the audit. Motorola must provide reasonable cooperation with the audit, including providing the appointed auditor a right to review, but not copy, Motorola security information or materials provided such auditor has executed an appropriate non-disclosure agreement. Motorola's policy is to share methodology and executive summary

information, not raw data or private information. Customer must, at no charge, provide to Motorola a full copy of all findings of the audit.

12. Regulation Specific Terms

12.1. HIPAA Business Associate. If Customer is a "covered entity" or a "business associate" and includes "protected health information" in Customer Data as those terms are defined in 45 CFR § 160.103, execution of the MPA includes execution of the Motorola HIPAA Business Associate Agreement Addendum ("BAA"). Customer may opt out of the BAA by sending the following information to Motorola in a written notice under the terms of the Customer's Agreement.

12.2. FERPA. If Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA), apply, Motorola acknowledges that for the purposes of the DPA, Motorola is a "school official" with "legitimate educational interests" in the Customer Data, as those terms have been defined under FERPA and its implementing regulations, and Motorola agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials. Customer understands that Motorola may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer must be responsible for obtaining any parental consent for any end user's use of the Online Service that may be required by applicable law and to convey notification on behalf of Motorola to students (or, with respect to a student under 18 years of age and not in attendance at a post-secondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data in Motorola's possession as may be required under applicable law

12.3. CJIS. Motorola agrees to support the Customer's obligation to comply with the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy and must comply with the terms of the CJIS Security Addendum for the Term of this Agreement and such CJIS Security Addendum is incorporated herein by reference. Customer hereby consents to allow Motorola "screened" personnel as defined by the CJIS Security Policy to serve as an authorized "escort" within the meaning of CJIS Security Policy for escorting unscreened Motorola personnel that require access to unencrypted Criminal Justice Information for purposes of Tier 3 support (e.g. troubleshooting or development resources). In the event Customer requires access to Service Use Data for its compliance with the CJIS Security Policy, Motorola must make such access available following Customer's request. Notwithstanding the foregoing, in the event the MPA or applicable Ordering Document terminates, Motorola must carry out deletion of Customer Data in compliance with Section 10 herein and may likewise delete Service Use Data within the time frame specified therein. To the extent Customer objects to deletion of its Customer Data or Service Use Data and seeks retention for a longer period, it must provide written notice to Motorola prior to expiration of the 30 day period for data retention to arrange return of the Customer Data and retention of the Service Use Data for a specified longer period of time.

12.4. CCPA. If Motorola is Processing Personal Data within the scope of the California Consumer Protection Act ("CCPA"), Customer acknowledges that Motorola is a "Service Provider" within the meaning of CCPA. Motorola must process Customer Data and Personal Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in this DPA and as permitted under the CCPA, including under any "sale" exemption. In no event will Motorola sell any such data. If CCPA applies, Personal Data must also include any data identified with the CCPA definition of personal data.

13. **Motorola Contact.** If Customer believes that Motorola is not adhering to its privacy or security obligations hereunder, Customer must contact the Motorola Data Protection Officer at Motorola Solutions, Inc., 500 W. Monroe, Chicago, IL USA 90661-3618 or at privacy1@motorolasolutions.com.

ANNEX I

A. LIST OF PARTIES

1. **Data exporter(s):** Customer

   Role (controller/processor): Controller

2. **Data importer(s):** Motorola Solutions, Inc.

   Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data subjects include the data exporter's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by data importer. Motorola acknowledges that, depending on Customer's use of the Online Service, Customer may elect to include personal data from any of the following types of data subjects in the Customer Data:

- Employees, contractors, and temporary workers (current, former, prospective) of data exporter;
- Dependents of the above;
- Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of data exporter's services;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter;
- Stakeholders or individuals who passively interact with data exporter (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the data exporter);
- Minors; or
- Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).

Categories of personal data transferred

Customer's use of the Products and Services, Customer may elect to include personal data from any of the following categories in the Customer Data:

- Basic personal data (for example place of birth, street name, and house number (address), Agreement code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;
- Authentication data (for example user name, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
- Commercial Information (for example history of purchases, special offers, subscription information, payment history);
- Biometric Information (for example DNA, fingerprints and iris scans);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
- Photos, video, and audio;
- Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);
- Device identification (for example IMEI-number, SIM card number, MAC address);
- Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location, and organizations);
- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);

- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;
- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or
- Any other personal data identified under applicable law or regulation.

Sensitive data transferred *(if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

The frequency of the transfer *(e.g. whether the data is transferred on a one-off or continuous basis).*

Data may be transferred on a continuous basis during the term of the MPA or other agreement to which this DPA applies.

Nature of the processing

The nature, scope and purpose of processing personal data is to carry out performance of Motorola's obligations with respect to provision of the Products and Services purchased under the MPA and applicable Ordering Documents. The data importer utilizes a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors utilize such facilities

Purpose(s) of the data transfer and further processing

The nature, scope and purpose of processing personal data is to carry out performance of Motorola's obligations with respect to provision of the Products and Services purchased under the MPA and applicable Ordering Documents. The data importer utilizes a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors utilize such facilities

The period for which the personal data will be retained, *or, if that is not possible, the criteria used to determine that period*

Data retention is governed by Section 10 of this Data Processing Addendum

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Transfers to sub-processors will only be for carrying out the performance of Motorola's obligations with

respect to provision of the Products and Services purchased under the MPA and applicable Ordering Documents. The data importer utilizes a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors utilize such facilities. In accordance with the DPA, the data exporter agrees the data importer may hire other companies to provide limited services on data importer's behalf, such as providing customer support. Any such sub-processors must be permitted to obtain Customer Data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Customer Data for any other purpose.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Measures of pseudonymization and encryption of personal data

Where technically feasible and when not impacting services provided:

- We minimize the data we collect to information we believe is necessary to communicate, provide, and support products and services and information necessary to comply with legal obligations.
- We encrypt in transit and at rest.
- We pseudonymize and limit administrative accounts that have access to reverse pseudonymization.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

In order to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services, Motorola Solutions Information Protection policy mandates the institutionalization of information protection throughout solution development and operational lifecycles. Motorola Solutions maintains dedicated security teams for its internal information security and its products and services. Its security practices and policies are integral to its business and mandatory for all Motorola Solutions employees and contractors The Motorola Chief Information Security Officer maintains responsibility and executive oversight for such policies, including formal governance, revision management, personnel education and compliance. Motorola Solutions generally aligns to the NIST Cyber Security Framework as well as ISO 27001.

Some of the system configuration is under the control of the customer.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Security Incident Procedures Motorola Solutions maintains a global incident response plan to address any physical or technical incident in an expeditious manner. Motorola maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. For each security breach that is a Security Incident, notification will be made in accordance with the Security Incident Notification section of this DPA.

Business Continuity and Disaster Preparedness Motorola maintains business continuity and disaster preparedness plans for critical functions and systems within Motorola's control that support the Products and Services purchased under the Agreement in order to avoid services disruptions and minimize recovery risks.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Motorola periodically evaluates its processes and systems to ensure continued compliance with obligations imposed by law, regulation or contract with respect to the confidentiality, integrity,

availability, and security of Customer Data, including personal information. Motorola documents the results of these evaluations and any remediation activities taken in response to such evaluations. Motorola periodically has third party assessments performed against applicable industry standards, such as ISO 27001, 27017, 27018 and 27701.

Measures for user identification and authorization

Identification and Authentication. Motorola uses industry standard practices to identify and authenticate users who attempt to access Motorola information systems. Where authentication mechanisms are based on passwords, Motorola requires that the passwords are at least eight characters long and are changed regularly. Motorola uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

Access Policy and Administration. Motorola maintains a record of security privileges of individuals having access to Customer Data, including personal information. Motorola maintains appropriate processes for requesting, approving and administering accounts and access privileges in connection with the Processing of Customer Data. Only authorized personnel may grant, alter or cancel authorized access to data and resources. Where an individual has access to systems containing Customer Data, the individuals are assigned separate, unique identifiers. Motorola deactivates authentication credentials on a periodic basis.

Measures for the protection of data during transmission

Data is generally encrypted during transmission within the Motorola managed environments. Encryption in transit is also generally required of any sub-processors. Further, protection of data in transit is also achieved through the access controls, physical and environmental security, and personnel security described throughout this Annex II.

Measures for the protection of data during storage

Data is generally encrypted during storage within the Motorola managed environments. Encryption in storage is also generally required of any sub-processors. Further, protection of data in storage is also achieved through the access controls, physical and environmental security, and personnel security described throughout this Annex II.

Measures for ensuring physical security of locations at which personal data are processed

Motorola maintains appropriate physical and environment security controls to prevent unauthorized access to Customer Data, including personal information. This includes appropriate physical entry controls to Motorola facilities such as card-controlled entry points, and a staffed reception desk to protect against unauthorized entry. Access to controlled areas within a facility will be limited by job role and subject to authorized approval. Use of an access badge to enter a controlled area will be logged and such logs will be retained in accordance with Motorola policy. Motorola revokes personnel access to Motorola facilities and controlled areas upon separation of employment in accordance with Motorola policies. Motorola policies impose industry standard workstation, device and media controls designed to further protect Customer Data, including personal information.

Measures for ensuring personnel security

Access to Customer Data. Motorola maintains processes for authorizing and supervising its employees, and contractors with respect to monitoring access to Customer Data. Motorola requires its employees, contractors and agents who have, or may be expected to have, access to Customer Data to comply with the provisions of the Agreement, including this Annex and any other applicable agreements binding upon Motorola.

Security and Privacy Awareness. Motorola must ensure that its employees and contractors remain aware of industry standard security and privacy practices, and their responsibilities for protecting Customer Data and Personal Data. This must include, but not be limited to, protection against malicious software, password protection, and management, and use of workstations and computer system accounts. Motorola requires periodic Information security training, privacy training, and business ethics training for all employees and contract resources

Sanction Policy. Motorola maintains a sanction policy to address violations of Motorola's internal security requirements as well as those imposed by law, regulation, or contract.

Background Checks. Motorola follows its standard mandatory employment verification requirements for all new hires. In accordance with Motorola internal policy, these requirements must be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation and any additional checks as deemed necessary by Motorola.

Measures for ensuring events logging

Motorola maintains policies requiring continuous monitoring and event logging on all production information resources. Application audit trail logs must be captured on all production Motorola information resources. Audit trail logs of production Motorola information resources are regularly reviewed and appropriate remedial actions are taken when necessary.

Measures for ensuring system configuration, including default configuration

Motorola on-site systems are provided with a default secure configuration that may require Customer input to complete the secure configuration. For example, some default configurations must be changed by the Customer to maintain a secure system (e.g., default usernames and passwords, connecting to active directory, etc.). This completion of the default secure configuration is dependent on the Customer input for transitioning from the default secure configuration to a secure configuration.

Measures for internal IT and IT security governance and management

The Motorola Solutions Enterprise Information Security organization is structured as follows: Governance/ Risk/ Compliance, Threat Intelligence & Vulnerability Management, Detection, Protection, and Response. Motorola assesses organization's effectiveness annually via external assessors who report and share the assessment findings with Motorola Audit Services who tracks any identified remediations. For more information, please see the Motorola Trust Center at

https://www.motorolasolutions.com/en_us/about/trust-center/security.html

Measures for certification/assurance of processes and products

Motorola performs internal Secure Application Review and Secure Design Review security audits and Production Readiness Review security readiness reviews prior to service release. Where appropriate, privacy assessments are performed for Motorola's products and services. A risk register is created as a result of internal audits with assignments tasked to appropriate personnel. Security audits are performed annually with additional audits as needed. Additional privacy assessments, including updated data maps, occur when material changes are made to the products or services. Further, Motorola Solution has achieved AICPA SOC2 Type 2 reporting and ISO/IEC 27001:2013 certification for many of its development and support operations.

Measures for ensuring data minimization

Motorola Solutions policies require processing of all personal information in accordance with applicable law, including when that law requires data minimization. Further, Motorola Solutions conducts privacy assessments of its products and services and evaluates if those products and services support the principles of processing, such as data minimization.

Measures for ensuring data quality

Motorola Solutions policies require processing of all personal information in accordance with applicable law, including when that law requires ensuring the quality and accuracy of data. Further, Motorola Solutions conducts privacy assessments of its products and services and evaluates if those products and services support the principles of processing, such as ensuring data quality.

Measures for ensuring limited data retention

Motorola Solutions maintains a data retention policy that provides a retention schedule outlining storage periods for personal data. The schedule is based on business needs and provides sufficient information to identify all records and to implement disposal decisions in line with the schedule. The policy is periodically reviewed and updated.

Measures for ensuring accountability

To ensure compliance with the principle of accountability, Motorola Solutions maintains a Privacy Program which generally aligns its activities to both the Nymity Privacy Management and Accountability Framework and NIST Privacy Framework. The Privacy Program is audited annually by Motorola Solutions Audit Services.

Measures for allowing data portability and ensuring erasure

When subject to a data request to move, copy or transfer their personal data, Motorola Solutions will provide personal data to the Controller in a structured, commonly used and machine readable format. Where possible and if the Controller requests it, Motorola Solutions can directly transmit the personal information to another organization.

***For transfers to (sub-) processors**, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.*

If, in the course of providing products and services under the MPA, Motorola Solutions transfers information containing personal data to third parties, said third parties will be subjected to a security assessment and bound by obligations substantially similar, but at least as stringent, as those included in this DPA.

ANNEX III

LIST OF SUB-PROCESSORS

Not Applicable