INTERGOVERNMENTAL AGREEMENT

TO ESTABLISH A SCHOOL SAFETY INTEROPERABILITY PROGRAM

BETWEEN

THE CITY OF YUMA AND SOMERTON SCHOOL DISTRICT NO. 11

This Intergovernmental Agreement to Establish a School Safety Interoperability Program ("Agreement") is entered by the City of Yuma, Arizona ("City"), a municipal corporation of the State of Arizona, and the Somerton School District No. 11 ("District"), a public school district. The City and the District may be referred to individually as "Party" or collectively as "Parties".

RECITALS

WHEREAS, the Parties are authorized by A.R.S. § 11-952 *et. seq.*, Article III, Section 13, of the Yuma City Charter, and A.R.S. § 15-342.13 to enter into agreements for the joint exercise of any power common to the contracting parties as to governmental functions necessary to the public health, safety and welfare, and the proprietary functions of such public agencies; and,

WHEREAS, the enactment of A.R.S. § 41-1733 established a School Safety Interoperability Fund to distribute monies to the sheriff of a county or a city or town police department to establish a school safety program that meets the enumerated standards; and,

WHEREAS, the City accepted these monies from the Arizona Department of Administration ("ADOA") and has procured a School Safety Interoperability System that is compliant with A.R.S. § 41-1733 requirements; and,

WHEREAS, the Parties desire to work in cooperation with one another to further the goals of the School Safety Interoperability Program and shall accept the roles and responsibilities as established in the School Safety Interoperability Program guidelines; and,

WHEREAS, the Parties desire to jointly develop standard operating procedures and functional exercise test plans for the use of the School Safety Interoperability System; and,

WHEREAS, the City will assign software licenses to each school in the District to utilize the School Safety Interoperability System; and

NOW THEREFORE, in consideration of the mutual promises and undertakings contained herein, the City and District ("Parties") agree as follows:

SECTION 1 – Purpose: The purpose of this Agreement is to provide the terms and conditions for the joint use and operation of the School Safety Interoperability System.

SECTION 2 – Effective Date: This Agreement is effective and binding from the date of the last Party's governing board's signature.

SECTION 3 – Term: This Agreement is in effect for five (5) years commencing upon the Effective Date. There are no automatic renewals.

SECTION 4 – Services to be Provided: The City will provide the following services to the District via a software agreement the City procured with Motorola Solutions, Inc. ("Vendor") attached as Exhibit A:

- RAVE Panic Button application for District employees.
- RAVE Command View for District employees to manage panic button activations and collaborate with first responders.
- RAVE Link for automated notifications about priority computer aided dispatch (CAD) incidents occurring within the proximity of a school campus.
- Integration of Command Central Aware with District video management system (VMS).

SECTION 5 – Roles and Responsibilities:

A. City:

1. The City is responsible for administering funds and expenditures for the School Safety Interoperability System, except for items listed in Section 7.
2. The City will assign a project manager to oversee Vendor project activities, including any change orders to the software agreement.
3. The City will manage deployment of services to Yuma Regional Communications System member agencies.
4. The City will establish a School Safety Interoperability working group of all participating school districts and public safety agencies to develop policies, procedures, and functional exercise test plans for the regional system.
5. The City will provide all financial reporting to the ADOA for expenses and use of the School Safety Interoperability Fund.

B. District:

1. The District will communicate to the City what School Safety Interoperability System services it desires to utilize.
2. The District will assign a project manager to coordinate with the City and Vendor for all District project activities.
3. The District will manage the deployment of services to its employees.
4. The District will provide existing communications assets and networks, or acquire the communications assets or networks necessary, to implement the School Safety Interoperability System.
5. The District will load floorplans to the system and define geo-boundaries within District campuses to direct first responders to the location of a panic button activation.

6. The District will work collaboratively with the School Safety Interoperability working group.

SECTION 6 – School Safety Interoperability System Funding: The School Safety Interoperability Fund appropriation to the Yuma Police Department is expected to purchase five (5) years of software subscription and maintenance services for the items in Exhibit A. Items requested by the District outside of the scope of Section 4 and Exhibit A may require the District to contribute the costs.

SECTION 7 – Items Not Covered: This Agreement does not include costs associated with the acquisition, installation, replacement, or repair of District specific equipment such as mobile devices, laptop or desktop computers, associated accessories and software, communications networks, video cameras, VMS, and access control systems. This Agreement does not include system costs for school campuses or facilities beyond those actively in use as of the Effective Date. This Agreement does not include any contracts between a Party and a third-party vendor. The School Safety Interoperability System does not replace current wireline and wireless 9-1-1 services for emergencies.

SECTION 8 – Contracts and Procurement for School Safety Interoperability System: The City will maintain all purchasing and support contracts for the School Safety Interoperability System. Purchase of the School Safety Interoperability System will follow all applicable City and State procurement requirements.

SECTION 9 – Termination:

1. Any Party may terminate this Agreement, with or without cause, by providing sixty (60) days written notice of its intent to terminate to the other Party.

2. Pursuant to A.R.S. § 41-2546, both Parties are government entities, and the Agreement validity is based upon the availability of public funding under their authorities. If the public funds are unavailable and not appropriate for the performance of either Party's obligations under this Agreement, then this Agreement shall automatically expire without penalty to either Party, after written notice to the other of the unavailability and non-appropriations of public funds. It is expressly agreed that neither Party shall activate this non-appropriation provision for its convenience or to circumvent the requirements of the Agreement, but only as an emergency fiscal measure.

3. Pursuant to A.R.S. § 38-511, the provisions of which are incorporated herein by reference, this Agreement is subject to cancellation if any person significantly involved in initiating, negotiating, securing, drafting or creating the Agreement is, at any time while the Agreement is in effect, an employee or agent of any other Party to the Agreement in any capacity or a consultant to any other Party of the Agreement with respect to the subject matter of the Agreement.

SECTION 10 – Authorized Use: The School Safety Interoperability System, its interfaces, and user applications shall only be used by employees of a Party within the guidelines of the policies and procedures established by the School Safety Interoperability working group.

SECTION 11 – Relationship of the Parties: The employees, agents, officials, or representatives of the Parties will not, for any purpose, be considered employees, agents, officials, or representatives of the other Party. Each Party assumes full responsibility for the actions, inactions, negligence, or reckless acts of its personnel while performing services under this Agreement and shall be solely responsible for their supervision, direction and control, discipline, payment of salary (including withholding income taxes and social security), workers' compensation and disability benefits. Nothing in this Agreement constitutes a partnership or joint venture between any Party and neither Party is the principal or agent of the other.

SECTION 12 - Authorization: This Agreement has been approved by actions taken by each of the governing bodies of each Party. The persons executing this Agreement on behalf of the Parties hereby represent and guarantee that they have been authorized to do so, on behalf of themselves and the entity they represent. Further representation is made that due diligence has occurred, and that all necessary internal procedures and processes, including compliance with the open meeting law where necessary, have been satisfied to legally bind the Party to the terms of this Agreement.

SECTION 13 - Conflict of Interest: This Agreement is subject to the conflict of interest and cancellation provisions of Arizona Revised Statutes, § 38-511, as amended.

SECTION 14 - Attorney Fees and Costs: If any Party brings an action or proceeding for failure to observe any of the terms or provisions of this Agreement, the prevailing Party is entitled to reasonable attorney fees and costs as determined by the court.

SECTION 15 - Compliance with Law: The Parties must comply with all federal, state, and local laws and ordinances applicable to its performance under this Agreement.

SECTION 16 - Severability: If any terms, parts, or provisions of this Agreement are for any reason invalid or unenforceable, the remaining terms, parts, or provisions are nevertheless valid and enforceable.

SECTION 17 - Integration: This Agreement contains the entire agreement between the Parties, and no oral or written statements, promises, or inducements made by either Party or its agents not contained or specifically referred to in this Agreement is valid or binding. All modifications to this Agreement must be in writing, signed and endorsed by the Parties.

SECTION 19 - Indemnification: Each Party agrees to defend, indemnify, and hold harmless the other and its agents, officials, employees, and representatives from and against any and all claims, losses and expenses resulting from that Party's negligent or intentional acts, mistakes, or omissions in the performance of this Agreement. Unless otherwise expressly provided, the Parties shall be individually responsible for the conduct of its own operations and performance of obligations under the Agreement and for any accidents, injuries to or the death of persons or damage or loss of property arising out of negligent or wrongful acts or omissions by its officers, agents or employees acting in the course or scope of their employment and/or while performing duties

undertaken pursuant to this Agreement. To the extent allowed by law, the Parties shall each indemnify the other for the acts or omissions of its own officers, agents, or employees acting in the course or scope of their employment that may lead to any claims, liability, loss, or expense brought against the other Party, including reasonable costs, collection expenses, and attorney's fees incurred in the defense of the claim.

SECTION 20 – Insurance: The City and the District shall maintain adequate insurance to cover any liability arising from the acts and omissions of their respective employees and agents. The Parties each represent and warrant to the other that it will maintain liability insurance coverage with a minimum value of one-million dollars ($1,000,000.00) per occurrence and two-million dollars ($2,000,000.00) in the aggregate. Parties each agree they have had the opportunity to verify each Party's coverage prior to signing this agreement. In the event either Party is unable to maintain this insurance minimum, then other Party shall be notified in writing within ten (10) days and be given the opportunity to terminate this Agreement.

SECTION 21 - Notices: Any notice required or permitted by this Agreement shall be in writing and shall be deemed given if delivered in person, electronic mail with delivery receipt, or ten (10) days after mailing, by United States registered or certified mail, postage prepaid, and addressed to the following:

City of Yuma Attn: Jeremy Jeffcoat, Asst. IT Director of the Yuma Regional Communications System 190 West 14th Street Yuma, Arizona 85364	Somerton School District No. 11 Attn.: Omar Duron, Superintendent 343 North Carlisle Avenue Somerton, AZ 85350

Unless otherwise agreed to, all information-sharing between the Parties described in this Agreement will flow between these points of contact. The Parties agree to notify the other Party of any changes to their points of contact within five (5) days of the change.

SECTION 22 - Recording: This Agreement shall be recorded in the Office of the County Recorder of Yuma County Arizona and with the City of Yuma Clerk's Office.

SECTION 23 - Modifications: No modifications, waiver, amendment, discharge or change of this Agreement shall be valid unless the same is in writing and signed by the Party against whom the enforcement of such modification, waiver, amendment, discharge, or change is or may be sought.

SECTION 24 - Assignment: This Agreement is not assignable without the mutual written consent of both Parties.

SECTION 25 – Rights of Parties Only: The terms of this Agreement are intended only to define the respective rights and obligations of the Parties. Nothing expressed herein shall create any rights or duties in favor of any potential third-party beneficiary or other person, agency, or organization.

SECTION 26 - Dispute Resolution: In the event a dispute arises, to the extent required by A.R.S. §12-1518, the Parties agree to submit any dispute to mediation or arbitration.

SECTION 27 - Venue: The Parties must institute and maintain any legal actions or other judicial proceedings arising from this Agreement in the Superior Court of Yuma County, or the United States District Court of Arizona, Yuma County, as appropriate.

SECTION 28 - Applicable Law: This Agreement shall be governed by and construed in accordance with the laws of the State of Arizona.

SECTION 29 – No Boycott of Israel; Forced Labor of Ethnic Uyghurs: To the extent applicable under Ariz. Rev. Stat. §§ 35-393 through 35-393.03, each party certifies it is not currently engaged in and agrees that it will not engage in for the duration of this Agreement, a "boycott" of Israel, as that term is defined in Ariz. Rev. Stat. § 35-393. To the extent applicable under Ariz. Rev. Stat. § 35- 394, the parties warrant and certify that they do not currently, and agree that they will not, for the duration of this Agreement, use the forced labor, any goods or services produced by the forced labor, or any contractors, subcontractors, or suppliers that use the forced labor or any goods or services produced by the forced labor of ethnic Uyghurs in the People's Republic of China.

SECTION 30 - Employment Eligibility: Each Party warrants, and shall require its subcontractors to warrant, that it is in compliance with A.R.S. § 41-4401, A.R.S § 23-214(A), the Federal Immigration and Nationality Act (FINA), and all other Federal immigration laws and regulations at all times when operating in the State of Arizona. A breach of this warranty shall be deemed a material breach of the IGA and is subject to penalties up to and including termination of this IGA. The Parties retain the legal right to inspect the citizenship documents of any Party employee or subcontractor employee who works on this IGA to ensure that the other Party or its subcontractors are complying with this warranty.

SECTION 31 – Workers Compensation: For purposes of workers' compensation, an employee of a Party to this Agreement, who works under the jurisdiction or control of, or who works within the jurisdictional boundaries of another Party, is deemed to be an employee of both the Party who is his/her primary employer and the Party under whose jurisdiction or control or within whose jurisdictional boundaries he/she is then working, as provided in A.R.S. §23-1022(D). The primary employer of such employee shall be solely liable for payment of workers' compensation benefits for the purposes of this section. Each Party herein shall comply with the provisions of A.R.S. § 23-1022(E) by posting the notice required.

SECTION 32 – Nondiscrimination: The Parties shall comply with all applicable State and Federal employment laws, rules, and regulations, which require that all persons shall have equal access to employment and educational opportunities regardless of race, color, religion, disability, sex (including sexual preference/identity), age, national origin, veteran's status, genetic code, or political affiliation during the term of this Agreement.

SECTION 33 – Counterparts: This Agreement may be executed in multiple counterparts, each of which shall be deemed an original and which together shall constitute the Agreement.

SECTION 34 – Impossibility: Neither Party to this Agreement shall be deemed to be in violation of this Agreement if it is prevented from performing any of its obligations hereunder for any reason beyond its control, including without limitation, global or national pandemics, acts of God or of the public enemy, flood or storm, strikes or statutory regulation or rule of any federal, state, or local government, or any agency thereof.

SECTION 35 – Recordkeeping and Confidentiality:

1. All student identities, records and personally identifiable information shall be kept confidential in accordance with the Family Educational Rights and Privacy Act (FERPA) and regulations adopted pursuant to that Act; the Individuals with Disabilities Education Act as Amended (IDEA) and regulations adopted thereunder; the Section 504 of the Rehabilitation Act and the regulations adopted thereunder; and applicable District board policies regarding the disclosure of personally identifiable information from students' education records. The City, acting pursuant to this Agreement, may be granted access to educational records or information. As such, the City's designated authorized employees, when acting pursuant to this Agreement, are hereby designated as "school officials" for purposes of this Agreement to receive access to educational records of students participating in the Program that is the subject of this Agreement. Neither the City or its designated authorized employees will disclose student information it receives to any third party, except with the prior written consent of District and the adult student and/or parent or guardian, as applicable. The City agrees it will use student information received pursuant to this Agreement solely to accomplish its obligations under this Agreement and solely in a manner and for purposes consistent with the terms and conditions of this Agreement and District policies and procedures. Notwithstanding this Section, the City is governed by the Arizona Public Record Laws, pursuant to Title 39 of the Arizona Revised Statutes. In the event there is a conflict between the requirements of Title 39 and the terms of this Agreement, the City shall notify the District in writing to provide the District an opportunity to seek injunctive relief against disclosure. The District acknowledges any such injunctive action must be taken promptly, as Arizona law prevents the City from delay in the production of public records.
2. Each Party shall retain all books, accounts, reports, files, documents, and records relating to the performance of this Agreement for a period of five (5) years, or as long as required by the Arizona State Library records retention schedules, after the completion of this Agreement, and agrees to make such documents open to inspection and audit by the other Party upon written request.
3. In the event recorded video is transmitted to the City by the District as part of a criminal investigation, the video shall become the property of the City and shall be governed by the Arizona laws relating to public records, as well as any evidentiary and criminal procedural rules and court orders. The City agrees to act to always maintain student privacy, so long as maintaining such privacy does not violate any Arizona laws, court rules, or court orders.
4. All recorded video that is not transmitted to the City for the purposes of a criminal investigation shall remain the property of the District.

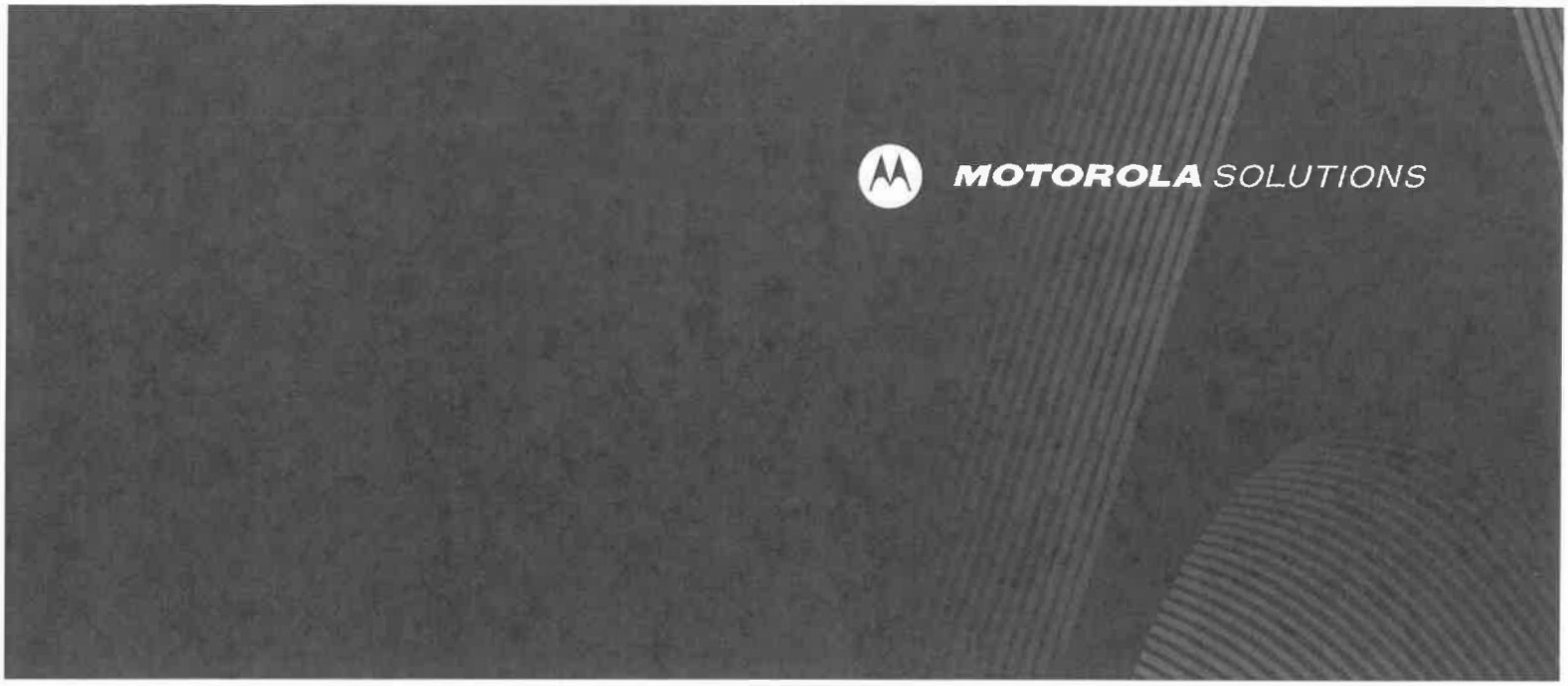
[Signature Blocks on Next Page]

Somerton School District No. 11	City of Yuma
_____ Omar Duron, Superintendent Date:_____	_____ John D. Simonton, City Administrator Date:_____
	ATTEST: _____ Lynda Bushong, City Clerk Date:_____

Pursuant to A.R.S. § 11-952, this Agreement has been reviewed by the undersigned attorney and is approved as to being in proper form and authority.

Somerton School District No. 11	City of Yuma
_____ [Attorney name] Date:_____	_____ Richard W. Files, City Attorney Date:_____

Exhibit A



Proposal

Yuma Police Department, City of AZ

CommandCentral Aware & Rave Proposal

24-180098/USAZ24P041

November 7, 2024

The design, technical, and price information furnished with this proposal is proprietary information of Motorola Solutions, Inc. (Motorola). Such information is submitted with the restriction that it is to be used only for the evaluation of the proposal, and is not to be disclosed publicly or in any manner to anyone other than those required to evaluate the proposal, without the express written permission of Motorola Solutions, Inc.

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2024 Motorola Solutions, Inc. All rights reserved.

PS-000183098

Motorola Solutions, Inc.
500 W Monroe Street, Ste 4400
Chicago, IL 60661-3781
USA

November 7, 2024

Yuma Police Department, City of AZ
Attn: Jeremy Jeffcoat
141 S Third Ave
Yuma, AZ 85364

Subject: Project 24-183098/USAZ24P041 CommandCentral Aware & Rave Proposal

Dear: Jeremy Jeffcoat

Motorola Solutions is pleased to present to the CITY OF YUMA POLICE DEPARTMENT ("City") with this quote for quality communications equipment and services. The development of this quote provided us the opportunity to evaluate your requirements and propose a solution to best fulfill your communications needs.

Motorola's Proposal is subject to the terms and conditions of the Maricopa County's Contract School Safety Pilot Program, 230076-RFP, executed on November 22, 2023, its Exhibits and applicable Addenda ("Contract"). The City of Yuma Police Department may accept this quote by signing and returning a signed copy of this proposal to Motorola.

Additionally, the City of Yuma Police Department's proposal to purchase via this Contract is contingent upon the City receiving approval from Maricopa County or executing an Intergovernmental Cooperative Purchasing Agreement ("ICPA") in accordance with Section 8.0 of the Contract.

This information is provided to assist you in your evaluation process. Our goal is to provide to the CITY OF YUMA POLICE DEPT with the best products and services available in the communications industry. Please direct any questions to Emily Dean at emily.dean@motorolasolutions.com.

We thank you for the opportunity to provide you with premier communications and look forward to your review and feedback regarding this quote. Sincerely,
Motorola Solutions, Inc.

Carrie Hemmen
MSSSI Sr. Vice President, Software Sales
Motorola Solutions Inc.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Table of Contents

Section 1
System Description 4
- **1.1 Overview** 4
- **1.2 Modules available with the CommandCentral Aware Plus** 6
- **1.3 Integrations** 7
- **1.4 Protected Places Package** 12
- **1.5 Cloud Security and Compliance** 13
- **1.6 Capacity and Latency** 14
- **1.7 Customer Provided Hardware** 16

Section 2
Functional Description 18
- **2.1 Tyler New World CAD to CC Aware** 18
- **2.2 System Diagram** 19

Section 3
Rave LINK+Panic Button- Statement of Work 21
- **3.1 Rave LINK Overview** 21
- 3.1.1 Product Specifications and Terms of Use 21
- **3.2 Features & Functions** 21
- **3.3 Terms of Use** 22
- **3.4 Rave Link Network Architecture & Hardware Minimum Requirements** 22
- **3.5 Rave Link Network Architecture and Requirements** 23
- **3.6 Self-Hosted MEP Compute & Network Resources** 23
- **3.7 Customer Obligations** 24
- **3.8 Access to Data - CAD Administration** 25
- **3.9 Information Technology (IT)** 25
- **3.10 Rave Panic Button Implementation** 25
- **3.11 Implementation** 26
- 3.11.1 Training and Support 27

Section 4
CommanCentral Aware: Statement of Work 29
- **4.1 Overview** 29
- 4.1.1 Contract Administration and Project Initiation 29
- 4.1.2 Completion and Acceptance Criteria 29
- 4.1.3 Project Roles and Responsibilities 30
  - 4.1.3.1 Motorola Roles and Responsibilities 30
  - 4.1.3.2 Customer Core Team, Roles and Responsibilities Overview 31
  - 4.1.3.3 General Customer Responsibilities 33

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

4.1.4 Project Planning and Pre-Implementation Review 34
4.2 CommandCentral Enablement 35
4.2.1 Agency and User Setup 35
4.2.2 Project Kickoff 35
4.3 Contract Design Review (CDR) 36
4.3.1 Contract Design Review 36
4.3.2 Interface Delivery Review 37
4.4 Environmental Design Considerations 38
4.5 Hardware/Software Installation and Configuration 38
4.5.1 CloudConnect Installation and Configuration 38
4.6 Interfaces and Integration 39
4.6.1 Interface Installation and Configuration 39
4.6.2 ASTRO 25 Location Integration 40
4.6.3 CommandCentral Solution Geospatial Mapping Configuration 40
4.7 CommandCentral Solution Provisioning 40
4.8 Functional Demonstration 41
4.9 CommandCentral Training 41
4.9.1 Learning eXperience Portal (LXP Online Training) 41
4.9.2 Instructor-Led Training Motorola Responsibilities 42
4.10 Completion Milestone 43
4.11 Transition to Support and Customer Success 43

Section 5
Pricing Summary 44
5.1 Pricing Summary 44
5.2 Standard Maintenance Annual Pricing Summary 45
5.3 Payment Milestones 45

Section 6
Terms and Conditions 47

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Section 1

System Description

1.1 Overview

CommandCentral Aware is a situational awareness software solution designed to deliver real-time intelligence across the public safety workflow. The Plus offering of CommandCentral Aware provides a map-based and list view of calls from VESTA® 9-1-1 and VESTA® NXT, incidents and units from CommandCentral, PremierOne or Flex computer-aided dispatch (CAD), locations from broadband and LMR radios, LRP hot hits, cameras location and panic alerts from Rave Mobile Safety, and ingests third-party data such as gunshot detection alerts from ShotSpotter. The offer includes device location and details from V300 and V700 body-worn cameras, 4RE and M500 in-car video systems, CAPE-equipped drones, license plate recognition (LPR) camera locations sourced from Vigilant VehicleManager, cameras registered in CommandCentral Community, compatible APX radios and smartphone applications. Devices can also send status information, such as from a radio entering an emergency state, a body-worn camera recording activation, or an LPR camera registering a hot hit, to CommandCentral Aware that can trigger an alert.

The Plus offer allows you to consolidate and view Motorola Solutions and third-party video management systems for an increased range of options for streaming, as well as connect to camera feeds in your community, to bring more real-time video feeds into your command center. This helps intelligence analysts in the command center gain valuable visibility to the field, quickly identify emergency situations and provide remote supervision.

CommandCentral Aware is hosted in the Microsoft Azure Government cloud and is offered as-a-service for an annual subscription cost.

Solution Elements

CommandCentral Aware consists of a series of core functional modules and integrated systems that power the solution. The CommandCentral Aware Plus offer includes the following:

Modules:

- Esri-based unified map
- Configurable event monitor
- Workflow automation rules engine
- Integrated video module

Integrations:

- Radio Location, Detail and Status
  - APX Next, XN, XE and N70 Radios
  - APX Portable and mobile radios
  - MOTOTRBO Portable and Mobile Radios
  - Broadband Vehicle Modems
- Smartphone App Location, Detail and Status

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

  - WAVE Broadband Push-to-Talk
  - CommandCentral Responder
- Body-Worn, In-Car and Drone Camera Location and Detail
  - V300 and V700 Body-Worn Cameras
  - 4RE and M500 In-Car Camera System
  - CAPE-Equipped Drones
- LPR Camera Location, Detail and Hot Hit Alerts
  - Vigilant VehicleManager
- CAD Incident and CAD-Provided Unit Location, Detail and Status
  - PremierOne CAD
  - Flex CAD
  - CommandCentral CAD
- Community and Business Registered Cameras on the Map
  - CommandCentral Community
  - Rave Facility
- Panic Button and Tip Location and Details*
  - CommandCentral Community
  - Rave Panic Button
- 9-1-1 Call Location and Details
  - VESTA 9-1-1, VESTA NXT and RapidSOS
- Fixed Video Location, Detail and Livestreaming
  - Motorola Video Management Systems
  - Third Party Fixed Video Management Systems
  - Real Time Streaming Video (RTSP)
  - Edge Appliance
- Third-Party Event Integrations** (e.g. Shotspotter)
- Documented Data Ingest API*

* Integration functionality dependent on third-party partner

**Other third-party apps available depending on region

Cloud anchor server hardware and required software is also available, if not already present, to establish a connection between on-premises systems and the Motorola cloud hosting environment.

Below is a high level representation of the solution for Yuma

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

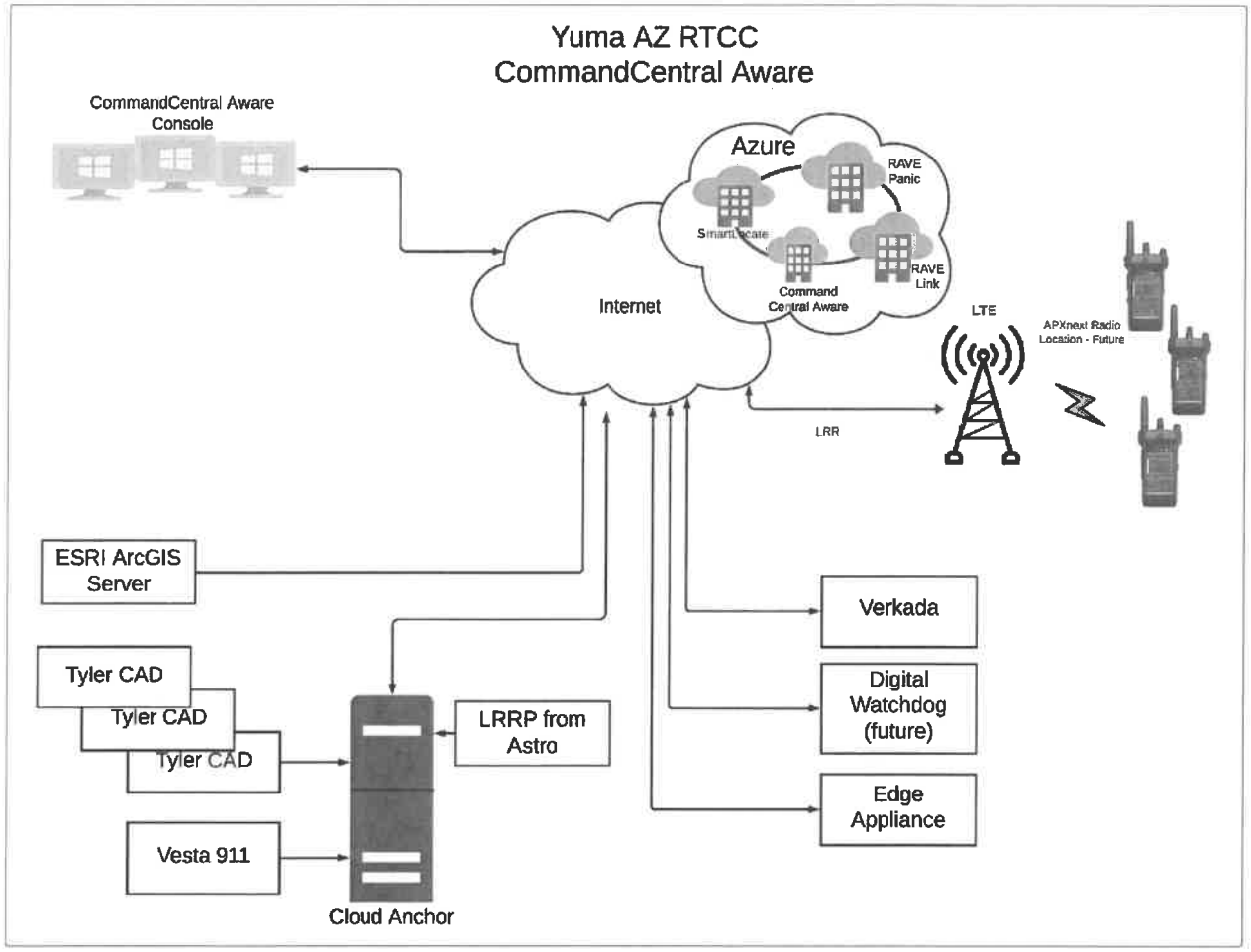


Figure 1: High Level System Diagram

1.2 Modules available with the CommandCentral Aware Plus

The CommandCentral Aware Plus offer includes the following modules.

Unified Map

CommandCentral Aware offers a unified mapping interface, powered by Esri, to display resources, event locations and alerts overlaid on detailed base maps and customer specific GIS layers. Users can view all location-based data on the map display. The CommandCentral Aware map includes the following:

- **Custom Map Layers** – Add your custom map layers from ArcGIS, Mapbox or GeoServer.
- **Map Layers Panel** – Show or hide event data and map layers to refine the map view.
- **Event Detail Display** – View details associated with each event on the map.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

- **Incident Recreation** – Replay a time lapse of mapped events over a set period of time for up to 90 days. This history can be exported and viewed in Google Earth or Esri ArcGIS Pro.
- **Traffic and Weather** – Overlay real-time traffic data and a weather radar map layer.
- **Building Floor Plans** – Enhance your map view with the addition of indoor floor plans using ArcGIS Indoor Floor plan layers.
- **Collaborative Drawing Tools** – Draw and save polygons, polylines and points onto the map to support planning for pre-planned events and provide tactical awareness during a real-time incident response. Annotations are visible by all users as a data layer.
- **Zones of Interest** – Create geofences that geographically filter information in a defined area.
- **Directed Patrol Alerts** – Specify geographic areas, set alerts and define rules for resources to enter and remain in for a user-determined period of time.
- **Unit Management** – From CommandCentral Admin, affiliate various resources such as radios and body worn cameras into units that can be named and intelligently tracked based on data from all affiliated resources.

Event Monitor

CommandCentral Aware offers an event monitor to display a running list of event and resource alerts. The event monitor is highly configurable to meet the needs and preferences of each user. Filter events by type, create separate tabs for different event types and show, hide or reorder columns of event information within the tabs. Pin an event to the top of your monitor as well as apply your event monitor filter to the map to maintain a consistent view of information. Details from any event can be opened in a dialogue box to give users all information about an event provided by the source system.

Rules Engine

The CommandCentral Aware rules engine allows users to create highly configurable rule sets to trigger actions based on the occurrence of events matching the rule criteria. For example, rows in the Event Monitor can be highlighted and audible alerts for critical events can be triggered. These visual or auditory triggers reduce the number of steps needed to support an incident. Rules are used to trigger scenarios. For example, if a panic button alert is received, Aware will pin and highlight the event in the Event Viewer, zoom and pan to the location on the map and play nearby cameras in the Video module.

1.3 Integrations

The CommandCentral Aware Plus offer the following integrations:

Radio Location, Detail and Status

APX Next, XN, XE and N70 Radios

The CommandCentral Aware Plus offer comes with integration to APX NEXT, XN, XE and N70 radios equipped with an active SmartLocate subscription. Once SmartLocate is activated, these APX radios can send device location, details and status over a broadband network. This data is available in CommandCentral Aware on the map and event monitor. Broadband connectivity via SmartLocate increases the frequency of location reporting beyond the capability of an LMR system to improve location accuracy and enable more devices to be tracked.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

APX Portable and Mobile Radios

The CommandCentral Aware Plus offer comes with the ability to integrate with APX portable and mobile radios. APX radios can send device location, details and status over an ASTRO network for locationing of radios when Push-To-Talk (PTT) is activated on the device or cadence-based locationing through the ASTRO data network, which uses integrated voice and data. This data is available in CommandCentral Aware on the map and event monitor. Alerts can be triggered when the radio registers "person down" status at an angle with no movement, when the emergency button is pressed on the radio or when a vehicle equipped with APX radios experiences significant impact.

APX Next, XN, XE and N70 Radios

The CommandCentral Aware Plus offer comes with the ability to integrate with APX radios equipped with an active SmartLocate subscription. Once SmartLocate is activated, these APX radios can send device location, details and status over a broadband network. This data is available in CommandCentral Aware on the map and event monitor. Broadband connectivity via SmartLocate increases the frequency of location reporting beyond the capability of an LMR system to improve location accuracy and enable more devices to be tracked. Alerts can be triggered when the radio registers "person down" status at an angle with no movement, when the emergency button is pressed on the radio or when a vehicle equipped with APX radios experiences significant impact.

MOTOTRBO Portable and Mobile Radios

The CommandCentral Aware Plus offer comes with the ability to integrate with MOTOTRBO radios. With this integration, MOTOTRBO radios can send device location, details and status information to CommandCentral Aware.

Broadband Vehicle Modems

The CommandCentral Aware Plus offer comes with the ability to integrate within-car broadband vehicle modems. These modems can send device location, details and status information to CommandCentral Aware. Examples include location via Sierra Wireless or Cradlepoint networks.

Broadband Application Location, Detail and Status

WAVE PTX Broadband Push-to-Talk

The CommandCentral Aware Plus offer comes with the ability to integrate with WAVE and Kodiak Broadband Push-to-Talk smartphone applications. With this integration, these smartphone applications can send device location, details and status information to CommandCentral Aware.

CommandCentral Responder

The CommandCentral Aware Plus offer comes with the ability to integrate with the CommandCentral Responder smartphone application. With this integration, CommandCentral Responder can send device location, details and status information to CommandCentral Aware.

Body-Worn, In-Car and Drone Camera

4RE and M500 In-Car Video Systems

The CommandCentral Aware Plus offer comes with the ability to integrate with M500 and 4RE in-car camera systems. With this integration, users can view real-time location, system details and livestreams from systems in the field that are actively recording. Your agency can provision up to 500

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

in-car camera systems in CommandCentral Aware, and administrators can add, edit or remove systems as needed.

When in-car cameras are active in the field and the in-vehicle modem is on, the CommandCentral Aware user can view the system's location on the map, see it listed in the event monitor and open up a video livestream upon recording being initiated in the field. CommandCentral Aware users can control the livestream to see front, cabin, rear, panoramic and side (depending on camera model) views of events both in and outside of the patrol car. CommandCentral Aware users can access up to ten simultaneous in-car camera livestreams.

V300 Body-Worn Cameras

The CommandCentral Aware Plus offer comes with the ability to integrate with V300 body-worn cameras. This integration brings V300 location, device details and the livestream from an actively recording camera into CommandCentral Aware on the map and in the event monitor. When the body-worn camera is on and within WiFi range of a vehicle or other agency authorized hotspot, the location of the V300 will be displayed on the CommandCentral Aware map. When the V300 is recording, you can view the video livestream remotely from CommandCentral Aware.

V700 Body-Worn Cameras

The CommandCentral Aware Plus offer comes with the ability to integrate with LTE-enabled V700 body-worn cameras. This integration brings V700 location device details and the livestream from an actively recording camera into CommandCentral Aware on the map and in the event monitor without needing to be within range of WiFi.

CAPE-Equipped Drones

The CommandCentral Aware Plus offer comes with the ability to integrate with CAPE-equipped drones. This integration brings in any active drone's location, device details and the livestream from a CAPE-equipped drone into CommandCentral Aware on the map and in the event monitor.

License Plate Recognition (LPR) Camera Location, Detail and Hot Hit Alerts

Vigilant VehicleManager

The CommandCentral Aware Plus offer comes with the ability to integrate with Vigilant VehicleManager. The locations of LPR cameras integrated with Vigilant VehicleManager can be viewed on the map in CommandCentral Aware as a data layer that can be toggled on or off. In addition to LPR camera locations, hits that match a hot list display on the map at the location of the camera that generated the scan. Hits also display in the event monitor and can trigger an alert.

Additionally, with the Vigilant VehicleManager, CommandCentral Aware users have the ability to initiate a search for historical license plate data directly from within CommandCentral Aware. By simply highlighting a license plate and right clicking, an option will be presented to run a search. This will open up a new window displaying the results directly within Vigilant VehicleManager. From there, users can conduct additional searches or analysis on the vehicle of interest.

CAD Incident and CAD-Provided Unit Location, Detail and Status

CommandCentral, PremierOne or Flex Computer Aided Dispatch (CAD)

The CommandCentral Aware Plus offer comes with the ability to integrate with CommandCentral CAD, PremierOne CAD and Flex CAD. This integration allows users to see incidents and details including incident type, location, narrative, priority and status on the map and event monitor. If Automatic Vehicle

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Location (AVL) status is reported through the CAD feed, the location of devices or units may also be displayed.

Community and Business Registered Cameras on the Registry Map

CommandCentral Community

The CommandCentral Aware Plus offer comes with the ability to display information and location of cameras registered in CommandCentral Community included in a map layer in CommandCentral Aware.

Rave Facility

The CommandCentral Aware Plus offer comes with the ability to support business cameras registered in Rave Facility via a data layer in CommandCentral Aware.

Panic Button, Tip Location and Details

CommandCentral Community

The CommandCentral Aware Plus offer comes with the ability to display tip submission details from CommandCentral Community. Users can access critical details submitted by the user including incident type and multimedia attachments via a data layer in CommandCentral Aware.

*Rave Mobile Safety Panic Button**

The CommandCentral Aware Plus offer comes with the ability to integrate with Rave Mobile Safety Panic Button. When a panic alert is initiated, an alert will be mapped in CommandCentral Aware and populated into the event monitor. Users can access critical details submitted by the user including activator's profile, incident type and multimedia attachments.

*Other third-party apps available depending on region.

9-1-1 Call Location and Details

VESTA 9-1-1 and VESTA NXT

The CommandCentral Aware Plus offer comes with the ability to integrate with the VESTA 9-1-1 and VESTA NXT call handling system. When a 9-1-1 call or text comes into VESTA 9-1-1, the CommandCentral Aware map has the ability to plot, center, and zoom upon answer and call updates. For each call or text, Class of Service icons will display with an uncertainty radius. Additionally, if available, CommandCentral Aware will display enhanced location data from RapidSOS associated with a wireless call. 9-1-1 calls and text will also populate in the event monitor.

Fixed Video Location, Detail and Livestreaming

The CommandCentral Aware Plus offer allows public safety agencies to expand their footprint of cameras by utilizing integrations with video management systems (VMS), real time streaming protocol (RTSP) connection and the Edge appliance.

Motorola Solutions Video Management Systems (Alta, Unity)

The CommandCentral Aware Plus offer provides the ability to integrate with Motorola video management systems and video streaming platforms. Camera feeds from connected video management system(s) can be streamed in the CommandCentral Aware web video viewer.

- View up to 16 feeds at once from across systems.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

- Playback recorded videos where available.
- Group cameras from across systems and open all livestreams available in a specific location.
- Ingest video analytic alerts from compatible VMS as events. View camera locations and simultaneously open cameras nearby to an event. Apply user permissions by camera groups to control who can view video streams, review historical footage, clip, snapshot and export.
- For Pan-Tilt-Zoom (PTZ)-enabled cameras, you can remotely control the PTZ. Access to PTZ features is only available for the surveillance systems and cameras that are configured and that support recorded content and PTZ.
- Share video clips and snapshots via embedded email sharing from within CommandCentral Aware.
- Video storage is provided by the integrated video management systems (VMS).

Third-Party Fixed Video Management Systems

The CommandCentral Aware Plus offer comes with the ability to integrate with select third-party video management systems (VMS). Camera feeds from connected video management system(s) are able to be streamed in the CommandCentral Aware video viewer.

- View up to 16 feeds at once from across systems.
- Playback recorded videos where available.
- Clip or snapshot video footage to share or save as evidence.
- Group cameras from across systems and open all livestreams available in a specific location.
- View camera locations and simultaneously open cameras nearby to an event. Apply user permissions by camera groups to control who can view video streams, review historical footage (when supported by the VMS), clip, snapshot and export.
- For Pan-Tilt-Zoom (PTZ)-enabled cameras, you can remotely control the PTZ. Access to PTZ features is only available for the surveillance systems and cameras that are configured and that support recorded content and PTZ.
- Share video clips and snapshots via embedded email sharing from within CommandCentral Aware.
- Video storage is provided by the integrated video management systems (VMS).

Real Time Streaming Protocol (RTSP) Video Connection

Stream publicly accessible IP cameras with supported media formats including WebRTC, HLS, RTSP, RTMP. This connection allows your agency to configure a secure connection to livestream third-party owned, public IP cameras. Direct connection enables livestreaming only; no video storage is provided by CommandCentral Aware.

Edge Appliance Video Connection

Connect up to 30 IP security cameras on a network for immediate access to camera data including live video, device information and location. Cameras that support ONVIF Profile S allow for automated discovery and provisioning for livestreaming in CommandCentral Aware. IP cameras that support WebRTC, HLS, RTSP, RTMP media formats on the network can be manually discovered and provisioned for livestreaming.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Third-Party Event Integrations

CommandCentral Aware Plus provides the ability to ingest alarms, events and location data through our ecosystem of third-party integrations powered by Aware's Event Ingest API. Aware offers a library of external connectors enabling the ability to ingest information from third-party CAD, LPR, mobile applications, devices, panic buttons and much more. Your Motorola representative can provide you with more information about third-party integrations available.

Developer Program with Documented Event Ingest API

Additional integrations with CommandCentral Aware Plus can be achieved via the CommandCentral Technology Developer Program which enables access to our Event Ingest APIs for third party partners and integrators. Your Motorola representative can provide you with more information about our API integrator program.

1.4 Protected Places Package

Protected Places is a program for community businesses, organizations or individuals to register their security cameras with the local law enforcement agency. Once registered, the camera's video footage can feed directly to CommandCentral Aware, providing vital information that can benefit the community with improved efficiency and faster response times.

The program includes a Motorola-hosted website that is customized and personalized for each agency. On this easy-to-use portal, customers can learn about the program, purchase devices via e-commerce and register their locations and agree to terms for camera sharing with public safety.

This portal can be linked on the agency website or it can be a standalone site, and it serves as:

- A marketing website for your agency to communicate with the community on the Protected Places program and how to get involved.
- A resource for users (businesses, organizations or residents) to learn about and purchase the Edge appliance (a device + subscription offer with an annual evergreen recurring sub), which connects security cameras to CommandCentral Aware.
- A resource for the community to explore Motorola's wider camera portfolio, including the ability to talk to an expert. Available cameras include:
  - Avigilon IP based cameras
  - The L6Q License Plate Recognition camera

To register for the program, users are sent to a customized page for your agency. The registration process is short and straightforward, with clear explanations of the process.

Users can provide facility information for each of their locations that is shared with their public safety agency based on the address zip code:

- Name
- Address
- Contact information (name, email address, phone number)
- Registered cameras
  - Camera name
  - Camera placement (indoor/outdoor)

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

  - Camera address
- Edge Appliance video streaming service
  - Device name
  - Device address
  - Cameras detected for streaming
    - Camera name
    - Camera address

From the registration webpage, customers can access your agency's privacy policies, MOUs and FAQs. They can also access your portal to explore Motorola cameras and create a lead to talk to an expert.

1.5 Cloud Security and Compliance

Proactive Security Design

Security is proactively incorporated into the design of our applications, not applied reactively when incidents occur. Applications undergo security reviews at each phase of their development and continue with ongoing assessments after deployment to find and repair vulnerabilities.

Compliance with Industry Best Practices

Our cloud solutions comply with key industry best practices for security, including NIST Security and Privacy Controls for Information Systems and Organizations (800-53), ISO 27001, 27017, 27018 - Specification for an Information Security Management System, Open Web Application Security Project (OWASP), and Center for Internet Security (CIS) and Criminal Justice Information System (CJIS) Security Policy. We are also annually audited for Service Organization Control (SOC) 1 and 2.

We conduct continuous and comprehensive risk assessments following the guidelines and best practices provided by NIST, OWASP, CIS and ISO.

Cybersecurity Champions Imbedded in Product and Service Teams

Over 350 specially trained and certified Cybersecurity Champions ensure that a culture of cybersecurity is instilled into the fabric of our product and services teams. Programmers receive ongoing security training and updates on the latest hacker tactics so they can layer security into every stage of the application development process.

FedRAMP Certified Cloud

The CommandCentral Aware Plus offer is available to be hosted on GovCloud meeting high impact status determined by the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB). U.S. government customers can safely deploy CommandCentral Aware backed by FedRAMP's highest impact level of security. Some of the Aware Plus modules described above are not currently available with the FedRAMP deployment option.

Canada CCCS, Canada and Australia and New Zealand (ANZ) Clouds

The CommandCentral Aware Plus offer is available to be hosted on Motorola's CCCS (Canadian Centre for Cybersecurity) cloud environment as well as the Azure Canada and Azure ANZ clouds.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Some of the Aware Plus modules described above are not currently available with the CCCS, Canada and ANZ clouds.

1.6 Capacity and Latency

CommandCentral Aware instances have the following capacity parameters:

- A maximum of 3,000 icons viewed on the CommandCentral Aware client at one time, per instance.
- A maximum of 100 updates per second on the CommandCentral Aware client.
- A maximum of 5,000 radios supported per server.
- A maximum of 32,000 total fixed cameras supported per CommandCentral Aware instance.

Low latency is critical for real-time operations. The speed with which data appears on the CommandCentral Aware display depends in large part on how quickly the information is presented to the CommandCentral Aware interface. Major contributors to the latency are network delays and the delay time from occurrence of an event to when that event information is presented to CommandCentral Aware from the source application (CAD, AVL, ALPR).

Although CommandCentral Aware strives to provide near real-time performance, Motorola provides no guarantees as to the speed with which an event (or video stream) appears in the application once the event is triggered.

Motorola will work with the Customer IT personnel to verify that connectivity meets requirements. The Customer will provide the network components.

Network Bandwidth Specifications

- **Network**: Customer provided internet access and remote access capability
- **Minimum bandwidth**: 1.1 Mbps between Cloud Anchor Server and CommandCentral Aware cloud platform

Networking Requirements

The following chart displays the requirements for accessing external network resources from within your Aware deployment. The final set of requirements will vary depending on the modules being deployed.

Box	Source IP	Destination IP	Protocol	Destination port
CloudConnect	<CloudConnect IP>	idm.imw.motorolasolutions.com	TCP	443
	<CloudConnect IP>	aware-api.usgov.commandcentral.com	TCP	443
	<CloudConnect IP>	admin-api.usgov.commandcentral.com	TCP	443
	<CloudConnect IP>	aware-publisher-ws.usgov.commandcentral.com	TCP	443
	<CloudConnect IP>	registry.commandcentral.com	TCP	443
	<CloudConnect IP>	s3-us-west-2-r-w.amazonaws.com	TCP	443
	<CloudConnect IP>	platformy-registry.s3.us-west-2.amazonaws.com	TCP	443

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Box	Source IP	Destination IP	Protocol	Destination port
	<CloudConnect IP>	oneinterfaceblobstore.blob.core.usgovcloudapi.net	TCP	443
	<CloudConnect IP>	ccinterfaces-ccbroker-prod.usgov.commandcentral.com	TCP	443
	<CloudConnect IP>	ccinterfaces-sasgen-prod.usgov.commandcentral.com	TCP	443
	<CloudConnect IP>	services.usgov.commandcentral.com	TCP	443
	<CloudConnect IP>	qrwbubhpaovhj-sbu.servicebus.usgovcloudapi.net	TCP	443
	<CloudConnect IP>	qrwbubhpaovhj-sbu.servicebus.usgovcloudapi.net	TCP	5671
	<CloudConnect IP>	loc-srvc-ingest-production.servicebus.usgovcloudapi.net	TCP	443
	<CloudConnect IP>	loc-srvc-ingest-2-production.servicebus.usgovcloudapi.net	TCP	443
One-time cloudconnect provisioning	Provisioning client (jumpbox)	<CloudConnect IP>	TCP	8080
	Provisioning client (jumpbox)	<CloudConnect IP>	TCP	22
VMS Proxy	<VMS Proxy IP>	<CloudConnect IP>	TCP	22
	<VMS Proxy IP>	<CloudConnect IP>	TCP	8080
	<VMS Proxy IP>	<Genetec VMS IP>	TCP	5500
	<CloudConnect IP>	<VMS Proxy IP>	TCP	40080
IMW	<CloudConnect IP>	<IMW Core IP (or IMW customer IP if IMW is redundant)>	TCP	65001
(assuming 5.2.3 and above)	<CloudConnect IP>	<IMW Core IP (or IMW customer IP if IMW is redundant)>	TCP	65002
	<CloudConnect IP>	<IMW Core IP (or IMW customer IP if IMW is redundant)>	TCP	65003
	<CloudConnect IP>	<IMW Core IP (or IMW customer IP if IMW is redundant)>	TCP	65005
	<CloudConnect IP>	<IMW Core IP (or IMW customer IP if IMW is redundant)>	TCP	65006
	<CloudConnect IP>	<IMW Core IP (or IMW customer IP if IMW is redundant)>	TCP	65008
	<CloudConnect IP>	<IMW Core IP (or IMW customer IP if IMW is redundant)>	TCP	9031
Aware clients	<Aware client IP(s)>	<VMS Proxy IP>	TCP	40080
	<Aware client IP(s)>	<Genetec VMS IP>	TCP	554
	<Aware client IP(s)>	<Genetec VMS IP>	TCP	560
	<Aware client IP(s)>	<Genetec VMS IP>	TCP	5004
	<Aware client IP(s)>	<Genetec VMS IP>	TCP	5500
	<Aware client IP(s)>	admin.commandcentral.com	TCP	443
	<Aware client IP(s)>	aware.commandcentral.com	TCP	443
	<Aware client IP(s)>	idm.imw.motorolasolutions.com	TCP	443

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

1.7 Customer Provided Hardware

Motorola recommends the following hardware specifications for customers providing their own hardware or Virtual Machine hosting. The Cloud Anchor server available through Motorola Solutions is typically an HP DL20 or similar grade server sized for up to 4 simultaneous VMs.

Cloud Anchor Server Specifications

Host Server CPU	Intel Xeon 3.4 GHz or greater
Host Server RAM	64GB DDR or greater
Host Server OS	VMWare ESXi 8.X
Host Server Hard Drive	1TB or greater (SSD or SAS)
Data Interface Virtual Machine	8GB RAM, 2 virtual CPUs, 20GB disk storage
Video Interface Virtual Machine	16GB RAM, 2 virtual CPUs, 64GB disk storage
Operating System	Windows 2022 and above installed
Network Interface Card	1GB NIC Port
IP Address	Two static IP addresses, corresponding subnet masks/default gateway, and available NTP and DNS IP to the Cloud Anchor Virtual Machines
Network Port	One network port for each VMS server One network port for each VMS analytics appliance

CommandCentral Aware Workstations PCs

Workstation PCs deployed to run CommandCentral Aware often display Aware modules over three separate monitors and require appropriate PC resources to display a variety of real-time data and videos across multiple displays, including the ability to stream up to 16 concurrent video feeds. Motorola does not sell PCs as part of the Aware deployment. Below are recommendations for customer provided PCs.

Processor	High-end Business or Server Grade Intel CPU ▪ Reference: o Intel Core i7 13700K 5.40 GHz (16 Cores) o Intel Xeon 3.0 GHz (12 cores) or greater
RAM Memory	32 GB DDR or greater
Hard Drive	512GB SSD or greater
Operating System	Windows 10 Professional or greater
Network Card	1 GB port
Graphics Card	NVIDIA T1000 8 GB or greater (support for 3 or 4 monitors)

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Display	Narrow Bezel IPS Display, 2560x1440
Monitor	27" monitor of larger
Web Browser	Google Chrome (latest version available)

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Section 2

Functional Description

2.1 Tyler New World CAD to CC Aware

The Tyler New World CAD to CommandCentral Aware Interface ("Interface") will receive CAD incident data from the Tyler New World CAD system and deliver it to the CommandCentral Event Ingest system. When incidents are delivered to the Event Ingest system, they will be available for display within the CommandCentral Aware ("Aware") user interface. When location information is available as part of the CAD incident, then the incident can be plotted on the Aware map. Additionally, a tabular list of incidents can be configured in the Aware interface.

Use Cases

ID	Description
UC-01	Active CAD incidents will be displayed in CommandCentral Aware

Technical Requirements

Target System Version	Target System Connection Protocol	Send Only	Receive Only	Bi-Directional	Acknowledge Received / Send
Tyler New World CAD (version unknown)	File poller (FTP/SFTP/SMB)		Yes		

Configuration

Configuration of the interface will be done via CommandCentral Admin (CC Admin) as well as locally on the CloudConnect platform.

Assumptions/Limitations

- Files representing CAD incident updates will be delivered to a file share by the CAD system. The Interface will retrieve the CAD incident update files, translate them, and send the translated results to CC Aware.
- No filtering or extra processing of the data or business logic (beyond what is necessary to convert it into CommandCentral format) will be performed. Each incident is expected to be received in a single message and no cross-referencing or secondary table lookups should be necessary.
- Bi-directional communications with Tyler New World CAD are not supported (i.e. there will be no ability to send messages, commands, etc. from the CommandCentral system back to Tyler New World CAD).
- All data fields described below to be imported into CommandCentral are subject to availability from the source system.
- Authentication is assumed to be done via provisioned, static credentials that do not expire.
- Polling intervals of less than 30 seconds may not be supported.
- The file server (FTP, SFTP, or SMB) is provided by and managed by the customer and/or Tyler.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

- Customer will provide access to developer documentation and API information for the Tyler New World system. Customer will provide access for MSI engineering (via VPN or another mechanism) to a Tyler New World sandbox environment for development and testing of the interface. If no sandbox system is available, Customer understands that final testing may need to be completed on their production Tyler New World system.

The Interface will be hosted on the CloudConnect platform located on the customer's premises. Customer will ensure that all applicable network access is available for the CloudConnect platform to communicate with the file server/Tyler New World system as well as the CommandCentral cloud.

2.2 System Diagram

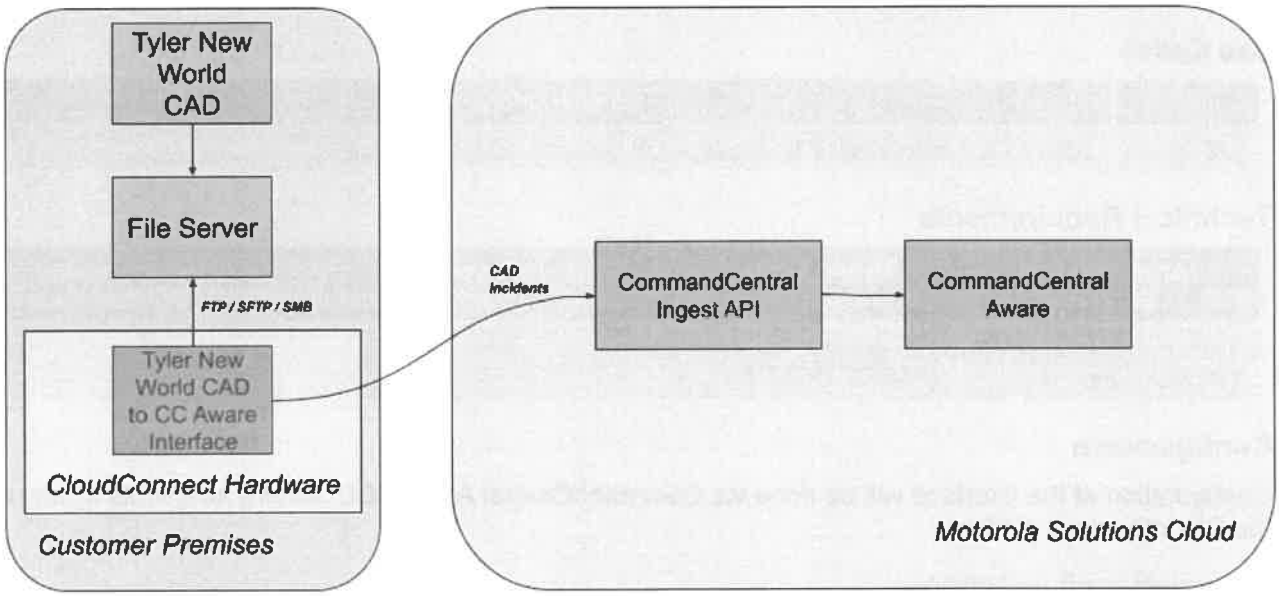


Figure 1: System Diagram

Data Elements sent to CommandCentral

CAD Incidents

- Incident ID
- Create Datetime Event Timestamp • Priority
- Call Type Description Label
- Problem Detailed Description
- Aware Details area:
  - Incident number
  - Call number
- Aware Comments:

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

  - Narrative creation time
  - Narrative text
  - Narrative Entered User
  - Narrative ID
- Latitude/Longitude
- Location Address display string
- Common Name Location description
- Icon: police

Motorola Solutions Responsibilities

- Implement the Interface according to the details specified in this document
- Configure and deploy the Interface to work with the customer's systems
- Conduct a functional demonstration validating the Interface works in accordance with this document

Customer Responsibilities

- Provide MSI access to API documentation and developer documentation for the Tyler New World system
- Provide MSI engineering access to an Tyler New World sandbox system for development and testing
- Perform any configuration necessary to permit MSI CommandCentral cloud-based systems to access Tyler New World API and/or file server (firewall configuration, etc.)
- Provide MSI the necessary credentials to access the Tyler New World API and/or file server with appropriate permissions configured • Coordinate meetings/discussions with 3rd party vendors as needed
- Participate in system and acceptance testing

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Section 3

Rave LINK+Panic Button- Statement of Work

3.1 Rave LINK Overview

3.1.1 Product Specifications and Terms of Use

RAVE LINK is a secure and interoperable solution for public safety agencies to speed response times by sharing CAD data, automating workflows, and more effectively collaborating across jurisdictions and on different CAD systems. Rave LINK provides data ingestion of Incidents and dynamic location of resources from an agency's CAD system, which can then be displayed within an agency or an adjacent agency's Radius EXCHANGE Map or LIGHTNING Mobile Application. RAVE LINK gives 9-1-1 dispatchers, first responders, and relevant emergency service agencies the information they need to respond more effectively and cohesively to critical incidents.

3.2 Features & Functions

- **Cross Agency Visibility** - Sharing CAD data with neighboring organizations enables both jurisdictions to see events and updates in real time, allowing both teams to give a faster response, and increasing situational awareness across jurisdictions.
  - **CAD Incidents** - Ingest, normalize and distribute CAD Data with advanced filter by incident type to Radius users within your agency and permission based access by authorized neighboring agencies.
  - **CAD AVL** - Ingest, normalize and distribute CAD AVL Unit Location with advanced filter by Discipline and Unit Type, to Radius users within your agency and permission-based access by authorized neighboring agencies.
- **Proximity Alerts** - Key data from an ongoing event, including locations indicated on an interactive map, are used to automate critical notifications and quickly get the right information to the right people.
- **Complex Incident Management** - During complex situations that require coordinated effort across multiple agencies or jurisdictions, an incident can automatically trigger a dedicated collaborative event, assign tasks for your team to complete, and offer easy mechanisms for tracking progress and updates.
- **Notifications** via SMS, voice, email, or applications based on automated rules leveraging CAD incident data.

Rave shall provide the customer with a deployment and configuration point of contact on the Rave Services team. This person will provide you with necessary operational and technical documentation, answer questions, configure operational rules, and provide access to additional technical or operational personnel within Rave, as necessary.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

- Product Interfaces - Configure and training for the operation of message template administrator interface for templated messages and automated rule-based sending by Rave Link to designated personnel.
- Incident action plan – Configure and train operation of administrator's interface for configuring event templates, tasks, assignments, and supplementary materials to guide your staff through manual or partly-manual processes.
- Documentation and Tools - Rave shall provide the necessary functional and technical documentation and tools necessary to facilitate deployment and train users on the Product Interfaces.
- Interface functional user guides for necessary interfaces including Rave Alert and Rave Admin View.
  - Technical integration manuals explaining options for conveying CAD data to Rave.
  - Data mapping spreadsheets to facilitate mapping your data into Rave's standard data model to enable rule-writing and inter-agency data sharing.

3.3 Terms of Use

- Acceptance of the Motorola Subscription Software Agreement is required for this option.
- Acceptance of the RAVE Aware Supplement

3.4 Rave Link Network Architecture & Hardware Minimum Requirements

As part of the Rave Link deployment, a CAD system must have the ability to use the Motorola Command Central Cloud API. If a CAD system does not have the ability to connect to the Motorola Command Central Cloud API, then the Motorola Edge Platform appliance needs to be installed to pass data securely. The appliance should be within the Public Safety Answering Point 's(PSAP's) environment behind a firewall with network access to the CAD system.

The virtual machine architecture reserves and isolates compute resources avoiding impact to CAD resources, provides observability metrics and logs that include system health monitoring and troubleshooting to Motorola Solutions (MSI) (system health monitoring and troubleshooting), and can be remotely patched and upgraded without adding overhead to the PSAP's IT team.

- Standardized MSI platform adhering to the Motorola cloud security policy that facilitates secure passes data between premise solutions and the MSI cloud to maintain CJIS compliance
- Facilitates a secure data handoff between CAD and the MSI cloud maintaining Criminal Justice Information Services (CJIS) compliance
- Monitoring services alerting on system health and data disruption events
- VM isolates resource impact from other applications (CAD, etc)

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

3.5 Rave Link Network Architecture and Requirements

Connecting Rave Link with a non MSI CAD solution requires a conveyance appliance to be deployed on premise to pass incident and AVL data to MSI's secure CAD cloud.

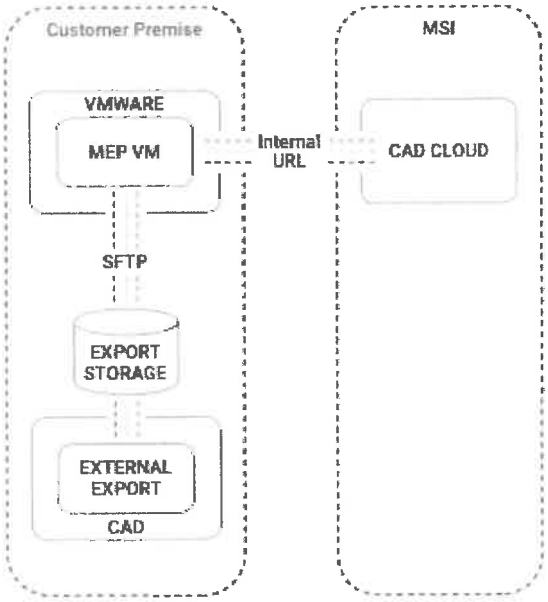


Figure 1: Rave Link Network Architecture

3.6 Self-Hosted MEP Compute & Network Resources

The MEP OVA should be installed on a ESXI hypervisor running ESXI 7.0 with the following settings:

- Deploy virtual machine with vTPM
- 1 TB disk size, thin provisioning
- 5 CPUs
- 9 GB RAM
- EFI firmware, with Secure Boot enabled
- Virtual hardware version: 13
- Guest OS type: rhel7-64 (Red Hat Enterprise Linux 8 is actual MEP operating system)
- Network Adapter Type: vmxnet3
- SCSI Adapter: VMware paravirtual SCSI

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

3.7 Customer Obligations

Rave Link provides powerful capabilities to optimize PSAP operations and reduce burdens on PSAP staff. To realize these benefits, an initial investment of effort is necessary to support the deployment and configuration of Rave Link. The efficiency of this deployment is dependent primarily on the PSAP's ability to provide relevant Information and Access to Data, via the involvement of necessary Personnel. Rave understands that the deployment of Rave Link is one of many important projects our customers are responsible for, and will work with you to deploy on a schedule realistic for your PSAP. However, experience has shown us that the customers who make a concerted effort to deploy as efficiently as possible derive the most benefit from the system.

The customer shall provide Rave two points of contact:

- A Project Owner: This person shall be invested in the success of the project and responsible for ensuring the timely provision of necessary Information and Access to Data, as described below.
- A Technical Lead: this person shall be responsible for the technical aspects of the product deployment.

The Project Owner and Technical Lead must possess information and expertise in the following areas, or else provide access to such people and ensure their cooperation:

- PSAP Operations
- CAD Administration
- Information Technology (IT)

Information - PSAP Operations

- Operational Rules - The customer is responsible for defining all operational rules desired and indicating which message templates or incident action plan should be automatically invoked by Rave Link when the rule is satisfied. For example, "Send template "Notify Chief" when an event of type Structure Fire is detected within Fire District 1 geo-boundary".
- Geo-Boundaries - The customer is responsible for providing all geo-boundaries necessary for automated rules in a supported format. For example, if different fire chiefs are to be notified about the same type of events in different towns, a boundary file must be provided for each relevant area.
- Message Template Content & Message Targets
  - The customer is responsible for managing the contact information for all people to be messaged via the system. Rave provides numerous ways to manage contact information manually or automatically - clearly documented in functional user guides.
  - The customer is responsible for creating all templated messages that the customer desires Rave Link to send automatically when a Rule is invoked.
- Incident Action Plans, Steps, Resources, & Assignees - The customer is responsible for creating all guided incident action plans, adding checklist steps, creating assignments, and adding supplemental resources like documents.
- Interagency Data Sharing
  - Rave Link can share data across agencies to improve situational awareness and inter-agency collaboration.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

- The customer is responsible for establishing relationships with other PSAPs and agencies with which you wish to share data. The customer is responsible for specifying which specific event types and event data fields are permissible to share with which other entities.

3.8 Access to Data - CAD Administration

- In order for Rave Link to function, the customer's CAD data fields must be mapped to Rave's NENA standards-based data model.
- The customer is responsible for understanding your CAD system's data schema, agency-specific configurations, and how your PSAP uses CAD operationally such that you can indicate to Rave which fields and data values contain the data necessary for Rave Link to function.
- If that knowledge is not available within the PSAP, the customer is responsible for working with your CAD company, consultants, or others to identify and indicate the necessary data fields.

3.9 Information Technology (IT)

- The customer is responsible for providing secure network access to the PSAP in order to transport the necessary CAD data to Rave.
- The customer is responsible for providing access to necessary CAD data via MSI connector and transport appliance, installed at Customer location, the customer makes the necessary data available to the tool through either:
  - XML or JSON files dropped in a location the tool reads from OR
  - creating a SQL Server view for the tool to read from.
- See 3.5 Rave Link Network Architecture & Hardware Minimum Requirements for additional details.

3.10 Rave Panic Button Implementation

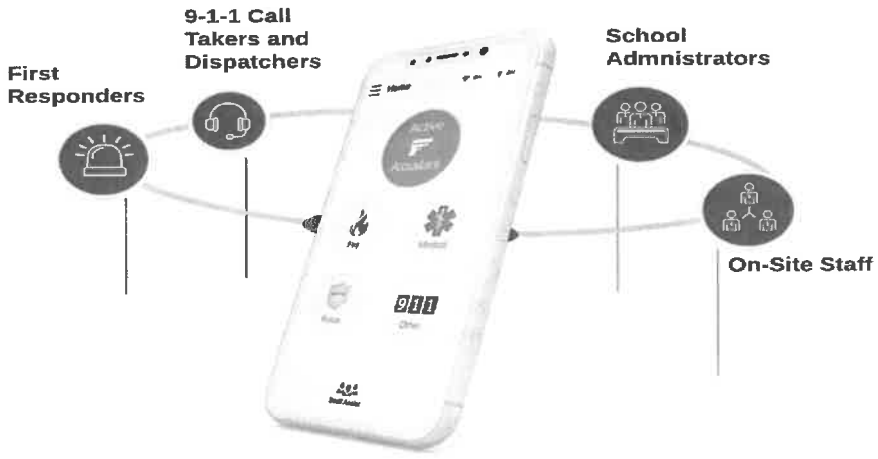


Figure 2: Rave Panic Button

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

3.11 Implementation

Easy Onboarding, Even for Large Districts

Having implemented thousands of schools in local, regional, and statewide adoption of Rave Panic Button, each school will find a successful path to onboarding with Rave Panic Button. Each new Rave customer is assigned a dedicated Implementation Manager. This is the single point of contact during implementation, who provides practical experience, expertise, and best practices.

Figure 3: Large State & Regional Deployments

Our implementation strategy is based on an agile methodology and service model in use by over 10,000 Rave customers. During the project kickoff, Rave will provide a customized project checklist that can be used to ensure that for each site all required project components are properly addressed.

Rave Implementation Manager Responsibilities

- Project Management
- Test plan development
- Resource allocation
- Configuration Management
- Change Management
- Issue Management
- Risk Management

Timetables may vary based on specific customer needs, implementation of optional integrations, or configuration needs for features requiring some customization. Rave completed a state-wide deployment in Arkansas in less than three months. In Brevard County, FL (110 school district)

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

implementation from date of purchase to fully initialized and functional was completed in under two weeks.

Upon completion of an agreement, Rave will work with you to establish a kick-off engagement for key stakeholders. The implementation manager will provide the access key for Panic Button Facility setup at this time, which outlines an easy-to-follow 5-step approach to deployment.

Client Responsibilities

This project requires operational support within the Client environment as well as awareness and training for authorized users, staff and other emergency response partners to ensure proper functioning of Rave Panic Button. The following outlines expected activities to be performed in support of the Panic Button deployment:

- **Project management** and executive support to coordinate the deployment of Rave Panic Button
- **Initial facility data entry and ongoing maintenance** to ensure that activations of the Panic Button app and other calls to 9-1-1 are appropriately recognized as originating from a covered location, as well as to deliver emergency notifications to the correct individuals / groups.
- **Integration of Panic Button functionality** into the applicable site-specific emergency response procedures and best practices as well as any training required to ensure proper implementation of those procedures.
- **Training for employees** through the use of the training materials provided by Rave
- **Regular exercising of emergency response** incorporating Rave Panic Button and in coordination with the local 9-1-1 center, police, fire and emergency medical services agencies.

For Each School Protected by Rave Panic Button

Upon completion of an agreement, Rave will work with you to set a time for a Kickoff Call, which will take roughly 30 minutes. The Kickoff Call will set the stage for the implementation, detailing who the Rave Implementation Manager will be and allow your team to be recognized as well. The implementation manager will provide the access key for Panic Button Facility setup at this time, which outlines an easy to follow 5 step approach to deployment:

- Understand what the solution is and does and allow you to share information to your assigned staff regarding the deployment.
- Creation of your facility profiles, including addition of details such as floor plans etc.
- Facility Approval coordination with 9-1-1, where applicable
- Addition of your contact data to the system, authorizing those users to receive notifications during an event, as well as download the Rave Panic Button app from their respective app store.
- Addition of Panic Button into your existing school safety protocols and testing.

3.11.1 Training and Support

To ensure successful operation of the system and integration into various security and emergency response workflows and processes, Rave will provide the following training and support services:

- **Provide training tools** PowerPoint decks, Administration Guide, videos, etc.
- **Provide remote access support** as needed for new feature deployments.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

- **Provide 24x7 phone and email technical support** as well as 8x5 phone and email support for non-critical support questions.
- **Provide sample SOPs** and FAQ documents.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Section 4

CommanCentral Aware: Statement of Work

4.1 Overview

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, Inc. (Motorola) system as presented in this offer to Yuma Police Department, City of AZ (hereinafter referred to as Customer). When assigning responsibilities, the phrase "Motorola" includes our subcontractors and third-party partners.

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

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

Motorola's Project Manager will use the SOW to guide the deployment process and coordinate the activities of Motorola resources.

The scope of this project is limited to supplying the contracted equipment and software as described in the Solution Description and system integration and or subscription services as described in this SOW and contract agreements.

4.1.1 Contract Administration and Project Initiation

After the contract is dually executed, the project is set up in Motorola's information and management systems, project resources are assigned, and Project Planning activities commence, Motorola 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 in order to avert delay.

4.1.2 Completion and Acceptance Criteria

Motorola's work is considered complete upon Motorola completing the last task listed in a series of responsibilities or as specifically stated in Completion Criteria. Customer task completion will occur in a way that enables Motorola to complete its tasks without delay.

The Customer will provide Motorola with written notification that it does not accept the completion of a task or rejects a Motorola deliverable within five business days of completion or receipt of a deliverable.

As CommandCentral Aware is provided as a subscription service, the subscription service period will begin upon activation of service.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Note - Motorola has no responsibility for the performance and/or delays caused by other contractors or vendors engaged by the Customer for this project, even if Motorola has recommended such contractors.

4.1.3 Project Roles and Responsibilities

4.1.3.1 Motorola Roles and Responsibilities

A Motorola team, made up of specialized personnel, will be assigned to the project under the direction of the Motorola 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's project team will provide services remotely via teleconference, webconference or other remote method in fulfilling its commitments as outlined in this SOW.

The personnel role descriptions noted below provide an overview of typical project team members. One or more resources of the same type may be engaged as needed throughout the project. There may be other personnel engaged in the project under the direction of the Project Manager.

Motorola has developed and refined its project management approach 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, our practices support the design, production and validation required to deliver a high-quality, feature-rich system.

Project Manager

A Motorola Project Manager will be assigned as the principal business representative and point of contact for the organization. The Project Manager's responsibilities include the following:

- Manage the Motorola responsibilities related to the delivery of the project.
- Maintain the project schedule and manage the assigned Motorola personnel and applicable subcontractors/supplier resources.
- Manage the Change Order process per the Agreement.
- Maintain project communications with the Customer.
- Identify and manage project risks.
- Manage 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 mutually agreed dates to discuss project status.
- Provide timely responses to issues related to project progress.

Consultant

If Consulting Services are included with this offer, the Motorola Consultant will work with the Customer project team on operationalizing the system into Customer's workflows and processes. The Consultant's responsibilities include the following:

- Provide training and guidance to the Customer on the use, operation and integration of the system.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Solutions Architect

The Solutions Architect is responsible for the delivery of the technical and equipment elements of the solution. Specific responsibilities include the following:

- Confirmation that the delivered technical elements and enablement of applications meets contracted requirements.
- Delivery of interfaces and integrations between Motorola products.
- Engagement throughout the duration of the delivery.

Customer Success Advocate

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

- Assist the Customer with maximizing the use of their Motorola 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.
- Liaise with the Customer on industry trends and Motorola evolutions.

Customer Support Services Team

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

4.1.3.2 Customer Core Team, Roles and Responsibilities Overview

The success of the project is dependent on early assignment of a Customer Core Team. During the Project Planning review, the Customer will be required to deliver names and contact information for the below listed roles that will make up the Customer Core Team. In many cases, the Customer will provide project roles that correspond with Motorola's project roles. It is critical that these resources are empowered to make decisions based on the Customer's operational and administration needs. The Customer Core 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 Customer Core Team must be committed to participate in activities for a successful implementation. In the event that the Customer is unable to provide the roles identified in this section, Motorola may be able to supplement Customer resources at an additional price.

Project Manager

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

- 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 Project Manager.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

- 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 Project Manager.
- Review the Project Schedule with the Motorola 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 staff as needed for the duration of the project, including at least one Application Administrator for CommandCentral Aware 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 Motorola personnel building access (and issue temporary identification to all Customer facilities where system equipment is to be installed during the project. Temporary identification cards are to be issued to Motorola personnel, if required for access to facilities.
- Ensure remote network connectivity and access to Motorola 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 personnel.
- Provide signatures of Motorola-provided milestone certifications and Change Orders within five business days of receipt.

System Administrator

The System Administrator manages the technical efforts and ongoing tasks and activities of their system, as defined in the Customer Support Plan (CSP).

Application Administrator(s)

The Application Administrator(s) manage the Customer-owned provisioning maintenance and Customer code tables required to enable and maintain system operation. The Application Administrator's involvement will start at the Project Kickoff and they will remain engaged throughout the

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

project to ensure they are able to maintain the provisioning post-handoff. The Application Administrator's responsibilities include the following:

- Participate in overall delivery activities to understand the software, interfaces and functionality of the system.
- 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.

Subject Matter Experts

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

IT Personnel

IT personnel provide required information related to LAN, WAN and wireless networks. They will provide required information about the devices and infrastructure related to servers, clients, radio, video and other devices ancillary to the implementation. They must also be familiar with connectivity to internal, external and third party systems to which the Motorola system will interface.

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 Customer Core Team if operations for these agencies differ from that of the Customer. The Customer will manage User Agency Stakeholder involvement, as needed, to fulfill Customer responsibilities.

4.1.3.3 General Customer Responsibilities

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

- All Customer-provided equipment, including hardware and third-party software, necessary for delivery of the system not specifically listed as a Motorola deliverable. This will include end user workstations, network equipment, telephone, radios, cameras, sensors and the like.
- Configuration, maintenance, testing and supporting the third-party systems that the Customer operates and will be interfaced as part of this project.
- Providing the Applications Programming Interface (API) or Software Development Kit (SDK) software licenses and documentation that details the integration process and connectivity for the level of custom third-party interface integration defined by Motorola.
- Communication and coordination between Motorola and Customer's third-party vendors, as required, to enable Motorola to perform its duties.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

- Active participation of Customer Core Team in project delivery meetings and working sessions during the course of the project. Customer Core Team 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 map services as requested by Motorola. 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 computer and audio-visual equipment for work sessions.
- Ability to participate in remote project meeting sessions using Google Meet or a mutually agreeable, Customer-provided, alternate remote conferencing solution.

4.1.4 Project Planning and Pre-Implementation Review

A clear understanding of the needs and expectations of both Motorola and the Customer are critical to the successful implementation and ongoing operation of CommandCentral. In order to establish initial expectations for system deployment and to raise immediate visibility to ongoing operation and maintenance requirements, Motorola will work with the Customer to help understand the impact of introducing a new solution and your preparedness for the implementation and support of the CommandCentral system.

Shortly after contract signing, Motorola will conduct a one-on-one teleconference with the Customer Project Manager to review the task requirements of each phase of the project and help to identify areas of potential risk due to lack of resource availability, experience or skill.

The teleconference discussion will focus on the scope of implementation requirements, resource commitment requirements, cross-functional team involvement, a review of the required technical resource aptitudes and a validation of existing skills and resource readiness in preparation for the Project Kickoff meeting.

Motorola Responsibilities

- Make initial contact with the Customer Project Manager and schedule the Pre-Implementation Review.
- Discuss the overall project deployment methodologies, inter-agency/inter-department decision considerations (as applicable), and third-party engagement/considerations (as applicable).
- Discuss Customer involvement in system provisioning and data gathering to understand scope and time commitment required.
- Discuss the Learning eXperience Portal (LXP) training approach.
- Obtain mutual agreement of the Project Kickoff meeting agenda and objectives.
- Review the Implementation Packet.
- Coordinate enabling designated Customer Application Administrator with access to the LXP and CommandCentral Admin Portal.

Customer Responsibilities

- Provide Motorola with the names and contact information for the designated LXP and application administrators.
- Acknowledge understanding of the Implementation Packet.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

- Collaborate with the Motorola Project Manager and set the Project Kickoff meeting date.

4.2 CommandCentral Enablement

The Customer will work with Motorola on setup and configuration of the Customer's firewall in order to allow traffic from CommandCentral.

4.2.1 Agency and User Setup

The Customer's agency(ies) and CommandCentral users must be provisioned within the CommandCentral cloud platform using the CommandCentral Admin application. The provisioning process allows the agency(ies) to define the specific capabilities and permissions of each user.

Motorola Responsibilities

- Use the CommandCentral Admin application to establish the Customer and the Customer's agency(ies) within the CommandCentral cloud platform. This activity is completed during the order process.
- Provision agency's CommandCentral initial users and permissions.

Customer Responsibilities

- Identify a System Administrator(s).
- Ensure all System Administrators complete the CommandCentral Admin training.
- Use the CommandCentral Admin application to set up CommandCentral administration and user passwords, and provision agency's CommandCentral users and permissions.

Completion Criteria

Initial agencies and users have been configured.

4.2.2 Project Kickoff

The purpose of the project kickoff is to introduce project participants and review the overall scope of the project.

Motorola Responsibilities

- Conduct a project kickoff meeting.
- Validate that key project team participants attend the meeting.
- Introduce all project participants.
- Review the roles of the project participants to identify communication flows and decision-making authority between project participants.
- Review the overall project scope and objectives.
- Review the resource and scheduling requirements.
- Review the teams' interactions (meetings, reports, milestone acceptance) and Customer participation.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

- Verify that Customer Administrator(s) (as defined during Pre-Implementation Review) have access to the LXP and CommandCentral Admin application.
- Obtain from Customer all paperwork and/or forms (i.e. fingerprints, background checks, card keys and any other security requirement) required of Motorola resources to obtain access.
- If third-party interfaces are included, request API, SDKs, data schema and any internal and third- party documents necessary to establish interfaces with local and remote systems.

Customer Responsibilities

- Validate that key project team participants attend the meeting.
- Introduce all project participants.
- Review the roles of the project participants to identify communication flows and decision-making authority between project participants.
- Provide VPN access to Motorola staff to facilitate delivery of services described in this SOW.
- Validate that any necessary non-disclosure agreements, approvals and other related issues are complete in time so as not to introduce delay in the project schedule. Data exchange development must adhere to third-party licensing agreements.
- Provide all paperwork and/or forms (i.e. fingerprints, background checks, card keys and any other security requirements) needed for Motorola resources to obtain access to each of the sites identified for this project.
- Provide the contact information for the license administrator for the project; i.e., IT Manager, CAD Manager and any other key contact information as part of this project.
- Validate access to the LXP and CommandCentral Admin application.
- Provide the information required in the Implementation Packet.

4.3 Contract Design Review (CDR)

4.3.1 Contract Design Review

The objective is to review the contracted applications, project schedule, bill of materials, functional demonstration approach, validation plan and contractual obligations of each party. Any changes to the contracted scope can be initiated via the change provision of the Agreement.

Motorola Responsibilities

- Review the contract exhibits: Solution Description, Statement of Work and Project Schedule.
- Review the technical, environmental and network requirements of the system.
- If Motorola is providing hardware, request shipping address and receiver name.
- Provide completed paperwork, provided to Motorola during project kickoff that enables Motorola resources to obtain site access.
- Review the information in the complete Implementation Packet.
- Grant Customer Administrator access to CommandCentral Admin application.
- Grant Customer LXP Administrator access to the LXP.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

- Generate a CDR Summary report documenting the discussions, outcomes and any required change orders.

Customer Responsibilities

- Project Manager and key Customer project team attend the meeting.
- Provide network environment information as requested.
- If Motorola is providing hardware, provide shipping address and receiver name.
- Provide locations and access to the existing equipment that will be part of the CommandCentral system per contract.

Completion Criteria

Delivery of CDR Summary report.

4.3.2 Interface Delivery Review

The objective of the interface delivery review is to discuss the user experience presented by each contracted interface, collect network information, API and access credentials required to connect to third-party systems, and document specific configuration parameters.

Motorola Responsibilities

- Discuss the need for additional information such as third party API, SDKs, data schema and any internal and 3rd party documents necessary to establish interfaces.
- Conduct reviews of the interface(s) to explain how each function as well as any dependency on third party API, SDKs, data schema and any internal and third party documents necessary to establish interfaces with local and remote systems.
- Review the functional interface demonstration process.
- Add interface related details to the CDR Summary report.

Customer Responsibilities

- Provide all required third party API and SDK licensing and documentation for Customer's existing systems such as CAD and Video Management Systems.
- Make knowledgeable individuals available for the interface reviews.
- As applicable, test any existing equipment and/or any third party equipment with which Motorola equipment will interface to validate connectivity with the Motorola system.
- Discuss information on third party API, SDKs, data schema and any internal and third party documents necessary to establish interfaces with all local and remote systems and facilities within ten days of the Project Kickoff Meeting so as not to impact the project schedule.
- Establish network connectivity between the CloudConnect Virtual Machine and all third party interface demarcations included as part of this project.

Completion Criteria

Delivery of CDR Summary Report.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

4.4 Environmental Design Considerations

The following environmental requirements must be met by Customer no later than the completion of the CDR in order to enable Motorola to complete installation activities presented in this SOW:

- Provide connectivity between the various networks.
- Provide VPN remote access for Motorola deployment personnel to configure the system and for Customer Support to conduct diagnostics.
- Provide backup power, as necessary.
- Provide Internet access to CommandCentral Aware server(s). This includes software licenses and media and installation support from the Customer's IT personnel.
- Provide for any electrical or infrastructure improvements required at the Customer's facility.
- Provide backhaul equipment, installation and support costs.
- Provide devices such as workstations, tablets and smartphones with Internet access in order to use the CommandCentral Aware solution. Chrome Browser is required for optimal performance. CommandCentral Aware workstations must support MS Windows 10 Enterprise or greater. Customer will provide Antivirus software for the CommandCentral Aware client.
- Existing APX subscribers will be at software version R15.00.00 or later and equipped with GPS and IV&D options in order to use the Location on PTT feature.
- Provide Motorola access with administrative rights to Active Directory for the purpose of installation/configuration and support.
- If interfaces are being included in this offer, the Customer is responsible for all necessary third-party upgrades of their existing system(s) as may be required to support the CommandCentral solution. Our offer does not include any services, support or pricing to support Customer third-party upgrades.
- If interfaces are being included in this offer, the Customer is responsible to mitigate the impact to third-party systems, to include CommandCentral interfaces that result from the customer upgrading a third-party system. Motorola strongly recommends you work with our team to understand the impact of such upgrades prior to taking any upgrade action.
- Provide all environmental conditions as outlined in the Aware Solution Description, such as power and network requirements.

4.5 Hardware/Software Installation and Configuration

4.5.1 CloudConnect Installation and Configuration

Motorola Responsibilities

- Verify remote access capability.
- If Motorola is providing hardware, perform physical installation of the Cloud Anchor Server on existing equipment rack, connect to power and network, and assign IP addresses for the network.
- Remotely configure CloudConnect Virtual Machine within the Cloud Anchor Server.
- Configure network connectivity and test connection to the CloudConnect Virtual Machine.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Customer Responsibilities

- If Customer is providing hardware, install Cloud Anchor Server in Customer's existing equipment rack and conduct a power on test demonstrating its availability to Motorola to commence with software installation and configuration activities.
- Give Motorola two static IP addresses, corresponding subnet masks/default gateway, and available NTP and DNS IP to the CloudConnect Server.

Completion Criteria

CloudConnect Virtual Machine configuration is complete.

4.6 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 project schedule. Integrations of functionality between Motorola developed products will be completed through software installation and provisioning activities in accordance with the Project Schedule dates. Integration activities that have specific requirements will be completed as outlined in this SOW.

4.6.1 Interface Installation and Configuration

Installation and configuration of interfaces will be completed in accordance with the System Description. Connectivity will be established between the Motorola system and the external and/or third party systems to which the contracted software will interface. Motorola 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 validating of the interfaces.

Motorola Responsibilities

- Establish connectivity to external and third-party systems.
- Configure interfaces to support the functionality described in the Solutions Description.
- Demonstrate the interface usability in accordance with the Project Validation Plan.

Customer Responsibilities

- Act as liaison between Motorola and third-party vendors or systems as required to establish interface connectivity with the Motorola system.
- Provide personnel who are proficient with and authorized to make changes to the network and third-party systems to support Motorola's interface installation efforts.
- Provide network connectivity between CommandCentral Solution and the third-party systems for interface installation and configuration. Act as liaison between Motorola and third-party vendors or systems as required to establish connectivity with CommandCentral Solution.

Completion Criteria

Interface and integration tasks are considered complete upon demonstration of the functionality.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Unknown circumstances, requirements and anomalies at the time of initial design can present difficulties in interfacing CommandCentral Solution to some third-party applications. These difficulties could result in a poorly performing or even a non–functional interface. At such time that Motorola is provided with information and access to systems, Motorola will be able to mitigate these difficulties. If Motorola 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 provision of the contract.

4.6.2 ASTRO 25 Location Integration

If Astro Location is being used by another application, the following responsibilities are applicable:

Motorola Responsibilities

- Configure connection between CloudConnect Virtual Machine and the existing ASTRO 25 Intelligent Middleware (IMW) system.
- Perform a remote IMW software upgrade (if required for compatible version).
- Configure IMW location reporting parameters. The location reporting configuration will include location on PTT, location on emergency and location on demand.
- Install core and site licenses for enhanced data, if enhanced data is selected.

Customer Responsibilities

- Provide IMW system.
- Program the subscriber fleet to support the Location on PTT functionality.

4.6.3 CommandCentral Solution Geospatial Mapping Configuration

Motorola Responsibilities

- Installation and configuration of the connection to the Customer-provided mapping system (ArcGIS Online, ESRI ArcGIS Server or ArcGIS Portal).
- Validate mapping layers and links to validate CommandCentral Solution is accessing and using Customer-published GIS data.

Customer Responsibilities

- Provide access to ESRI/GIS system and/or GIS personnel.
- Provide published GIS map services.
- Publish specific maps beneficial to the Customer analysts.

4.7 CommandCentral Solution Provisioning

Motorola will discuss industry best practices, current operations environment and subsystem integration in order to determine the optimal configuration for CommandCentral Solution.

Motorola Responsibilities

- Using the CommandCentral Admin application, provision users and groups based on Customer Active Directory data.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Customer Responsibilities

- Supply the access and credentials to Customer's Active Directory for the purpose of Motorola conducting CommandCentral Solution provisioning.
- Respond to Motorola inquiries regarding users/groups/agency mapping to CommandCentral Solution functionality.

Completion Criteria

CommandCentral Solution provisioning is complete upon Motorola completing provisioning activities.

4.8 Functional Demonstration

The objective of functional demonstration is to validate Customer access to the CommandCentral features and functions and system integration via configured interfaces (as applicable).

Motorola Responsibilities

- Update functional demonstration script.
- Provide script to Customer for review and acknowledgement.
- Conduct functional demonstration.
- Correct any configuration issues impacting access to cloud based features (i.e., map display, location updates, video display and/or interface and integrations).
- Document, in the Implementation Packet, any corrective actions taken by Customer or Motorola during the demonstration
- Provide Customer instruction on using the Customer Feedback Tool for feature/enhancement requests.

Customer Responsibilities

- Review and agree to the scope of the demonstration script.
- Witness the functional demonstration and acknowledge its completion.
- Resolve any provisioning impacting the functional demonstration.

Completion Criteria

Conclusion of the functional demonstration.

4.9 CommandCentral Training

The objective of this task is to prepare for and deliver the contracted training. Motorola training consists of both computer-based (online) and instructor-led. Training delivery methods vary depending on course content and offer.

4.9.1 Learning eXperience Portal (LXP Online Training)

This subscription service provides you with continual access to our library of online learning content and allows your users the benefit of learning at times convenient to them. Content is added and

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

updated on a regular basis to keep information current. This training modality allows the Customer to engage in training when convenient. All training, unless explicitly specified and defined, is online, computer-based, self-paced learning.

Motorola Responsibilities

- Designate a LXP Administrator to work with the Customer.
- Establish an accessible instance of the LXP for the Customer.
- Organize content to align with the Customer's selected technologies.
- Create initial Customer user accounts and a single Primary Administrator account.
- During on-boarding, assist the Customer with LXP usage by providing training and job aids as needed.
- Provide technical support for user account and access issues, base system functionality and Motorola-managed content.

Customer Responsibilities

- Provide user information for the initial creation of accounts.
- Provide network and internet connectivity for the Customer's users to access the LXP.
- The customer's primary LXP administrator should complete the following self-paced training: Learning Experience Portal (LXP) Introduction online course (LXP0001), LXP Primary Site Administrator Overview online course (LXP0002) and LXP Group Administrator Overview (LXP0003).
- Advise agency learners of the availability of training via the LXP.
- Ensure users complete LXP training in accordance with the Project Schedule.
- Order and maintain subscriptions to access Motorola's LXP.
- Contact Motorola to engage Technical Support when needed.

4.9.2 Instructor-Led Training Motorola Responsibilities

Motorola Responsibilities

- Deliver training materials in electronic format.
- Deliver Two Days On-site Training.
- Provide Customer with training attendance rosters and summarize any pertinent observations.

Customer Responsibilities

- Supply classroom, one login per attendee and one workstation per attendee.
- Designate a single point of contact who will work with Motorola to ensure the training environment is ready for training delivery.
- Facilitate training of all Customer end users in accordance with Customer's training delivery plan.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

4.10 Completion Milestone

Following the conclusion of the delivery of the functional demonstration, the project is considered complete and the completion milestone will be recognized.

4.11 Transition to Support and Customer Success

Customer Success is the main point of contact as you integrate this solution into your agency's business processes. Our Customer Support team will be the point of contact for technical support concerns you might have and can be reached either by phone or by emailing support.

Motorola Responsibilities

- Transition Customer to Motorola Customer Support.
- Supply Customer with instructions when engaging support.

Customer Responsibilities

- Provide Motorola with specific contact information for those users authorized to engage Motorola's support.
- Engage the Motorola support organization as needed.

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Section 5

Pricing Summary

5.1 Pricing Summary

Proposal Item Description	Price Year 1 USD
COMMANDCENTRAL AWARE	
CommandCentral Aware Plus Subscription #Video Devices 300 #Location Devices 300	$59,280
Integration: Vesta 911-QTY 4 LRRP Rave Alert Vehicle Manager	$0
Inteface: Tyler New World CAD to CC Aware –QTY 3	$4,590
Interface: Verkada- QTY 3	$9,000
Integration: CommandCentral Edge Appliance & HW Box	$1,655
CommandCentral Cloud Anchor Server	$20,226
CommandCentral Onsite *2 Days	$14,057
Implementation/Installation Services	$66,860
CommandCentral Aware Year 1 Total	$175,668
CommandCentral Aware Discount	$99,629
CommandCentral Aware Discounted Year 1 Total	**$76,039**
RAVE	
Rave Licenses Subscription	$160,380
Safety & Protection Set-up fee & Rave Aware One-time Fee	$17,500
One time Professional Service Fee	$5,000
Rave Year 1 Total	**$182,880**
CommandCentral Aware & RAVE Grand Total Year 1	**$258,919**

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

5.2 Standard Maintenance Annual Pricing Summary

Standard Maintenance Summary	CommandCentral Aware	Rave Solution	Total
Year 1	$76,039	$182,880	$258,919
Year 2	$66,822	$160,380	$227,202
Year 3	$66,822	$160,380	$227,202
Year 4	$66,822	$160,380	$227,202
Year 5	$66,822	$160,380	$227,202
	5-year Grand Total (exclusive of tax)		$1,167,727

Motorola Customer Loyalty Discount with signed contract- Discount Expires 12/15/2024

5.3 Payment Milestones

Payment

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 Milestones

Payment Milestone	Payment
Execution of Contract	50%
Final Acceptance	50%

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. Overdue invoices will bear simple interest at the maximum allowable rate by state law.

For Maintenance and Support Plan and Subscription Based Services: Motorola will invoice Customer annually in advance of each year of the plan.

Motorola will invoice Customer annually in advance of each year of the plan. For multi-year service 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

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

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. Measurement will take place once the annual average for the new year has been posted by the Bureau of Labor Statistics. 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).

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted

Section 6

Terms and Conditions

Motorola's Proposal is subject to the terms and conditions of the Maricopa County's Contract School Safety Pilot Program, 230076-RFP, executed on November 22, 2023, its Exhibits and applicable Addenda. Additionally, the City of Yuma Police Department's proposal to purchase via this Contract is contingent upon the City receiving approval from Maricopa County. The City of Yuma Police Department may accept this quote by signing and returning a signed copy of this proposal to Motorola.

Additionally, the City of Yuma Police Department's proposal to purchase via this Contract is contingent upon the City receiving approval from Maricopa County or executing an Intergovernmental Cooperative Purchasing Agreement ("ICPA") in accordance with Section 8.0 of the Contract.

Unless otherwise agreed upon in writing, invoices will be billed based on equipment shipped, services rendered, and standard payment terms and milestones.

By signing and returning this proposal to Motorola, this serves as authorization for Motorola Solutions to place an order and invoice for the communication equipment and services as referenced on Proposal / Quote 2834325 dated 10/8/24 for the purchase price of $1,167,727.33 (exclusive of tax), subject to the terms and conditions of Maricopa County's Contract School Safety Pilot Program, 230076-RFP, executed on November 22, 2023.

Customer affirms they have signatory authority to execute this contract. The contract price is fully committed and identified, including all subsequent years of contracted services, if applicable. 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.

Motorola acknowledges the Customer may require the issuance(s) of a purchase order or notice to proceed as part of the Customer's procurement process. However, Customer agrees that the issuance or non-issuance of a purchase order or notice to proceed does not preclude the Customer from its contractual obligations as defined in this Agreement.

The Parties hereby enter into this agreement of the above statement (Agreement) as of the last signature date below.

Motorola Solutions, Inc.

By: Carrie Hemmen

Name: Carrie Hemmen

Title: MSSSI Sr. Vice President, Software Sales

Date: November 7, 2024

Yuma Police Department, City of AZ

By:

Name: John D. Simonton

Title: City Administrator

Date: 12/16/2024

ATTEST:

Yuma City Clerk

Approved at the City Council Meeting of:

DEC 4 2024

City Clerk:

Use or disclosure of this proposal is subject to the restrictions on the cover page.
Motorola Solutions Confidential Restricted