

GUARDIAN MOBILE

SERVICE DEFINITION



DOCUMENT VERSION

Framework	G-Cloud 15
Document Version	1.0
Valid From	1 st January 2026

TABLE OF CONTENTS

1. Foreword	5
2. About Motorola Solutions	6
3. ITIL	7
4. Guardian Mobile Overview	8
4.3 Key Features & Operational Benefits	8
5. Guardian Mobile Modules	11
5.2 Core Applications & Clients	11
5.3 Operational Command Modules	11
5.4 Data Management Infrastructure	12
5.5 Integration Services	12
5.6 Administration	13
6. Solution Scope	14
6.5 Operational End-User Software	14
6.7 Connectivity & Security Layer	14
6.8 Data Management & Back-Office Layer	15
6.9 Configuration and Diagnostic Tools	15
7. Professional Services	17
8. Scalability & Optional Enhancements	19
8.2 Advanced Incident Command & Control	19
8.3 Guardian Fire Survival Guidance (FSG): [Prerequisite: Incident Command Module]	19
8.4 Mobilisation & Alerting Extensions	19
8.5 Agile Workforce	20
8.6 Satellite Navigation Engine	20
8.7 Guardian Training Simulators:	20
9. Implementation Model	22
9.3 Comprehensive Delivery Plan	22
9.4 Expert Delivery Team	22
9.5 Management of Implementation & Testing	22
9.6 Programme Milestones & Schedule	23
9.7 Go-Live	23
9.8 Agency Dependencies	23
9.9 Stakeholder Management & Governance	24
9.10 Train-the-Trainer	24
9.11 Administrative Training	24
10. Assumptions	25
10.2 Hosting & Infrastructure	25
10.3 Data, Mapping & Integration	25
10.4 Technical Prerequisites & Infrastructure	26

10.5 Agency Responsibilities & Dependencies	26
10.6 Commercial & Licensing	27
10.7 Delivery Approach	27

1. FOREWORD

- 1.1 This Service Definition document has been prepared by Motorola Solutions Limited (“Supplier” or “Motorola”) and submitted to the Crown Commercial Service for the G-Cloud 15 procurement and for publication on the Digital Marketplace. The information contained herein is proprietary and must only be used for the purpose of assessment and selection of Software as a Service for organisations eligible to procure cloud services through G-Cloud 15 Framework Agreement and Call-Off Contract. Use of any of the information for any other purpose must at first be authorised in writing by Motorola.

2. ABOUT MOTOROLA SOLUTIONS

- 2.1 Motorola Solutions creates innovative, mission-critical communication solutions and services that help Customers build safer cities and thriving communities by connecting people through technology.
- 2.2 Customers around the world turn to Motorola Solutions for our innovative solutions when they want highly connected teams that have the information they need throughout their workdays and in the moments that matter most to them.
- 2.3 Our Customers rely on us for the expertise, services and solutions we provide, trusting our years of invention and innovation experience. By partnering with Customers and observing how our products can help in their specific industries, we are able to enhance our Customers' experience every day.

3. ITIL

- 3.1 The Supplier has developed managed services and service management processes in line with the best practice ITIL Service Management Model. This systematic approach to service delivery and improvement provides us with the ability to deliver high quality, mature and robust services that are consistent with the expectations of our Customers.

4. GUARDIAN MOBILE OVERVIEW

4.1 Guardian Mobile is a fully integrated mobile data solution designed specifically to empower the Agency with mission-critical intelligence and seamless connectivity. This ecosystem unifies the operational picture across Control Rooms, Mobile Data Terminals (MDTs), and handheld devices, ensuring that commanders and crews have instant access to accurate data from mobilisation to incident closure. By combining robust GIS mapping, dynamic incident command tools, and flexible data capture, Guardian Mobile delivers a reliable, compliant platform that transforms how operational information is managed and shared between on scene responder, other agencies, tactical and strategic support groups.

4.2 Our proposed solution addresses the agency's core requirements through three strategic themes:

4.2.1 **Real-Time Situational Awareness:** Guardian Mobile establishes a Common Operating Picture (COP) that synchronises live data including resource locations (AVL), safety critical information, and incident management across Guardian Mobile Web, Guardian Mobile Pro, and Guardian Mobile Response, ensuring all stakeholders act on a dynamic, synchronised version of the truth.

4.2.2 **Operational Efficiency:** The solution replaces manual processes with intelligent automation, such as the Station Notifier for immediate crew visualisation of the mobilisation, presentation of safety critical information and other key data sets, integrated satellite navigation for optimal routing, and the digital forms to eliminate paper-based workflows.

4.2.3 **Safety & Compliance:** Guardian Mobile embeds safety into the workflow through the Incident Command Module, which provides auditable decision logs, dynamic risk assessments, and tactical mode status updates, ensuring statutory compliance, adherence to National Operation Guidance and robust firefighter safety management.

4.3 KEY FEATURES & OPERATIONAL BENEFITS

4.4 The following table details how the specific capabilities of the Guardian Mobile ecosystem translate into tangible operational value for your agency.

Feature / Capability	Operational Benefit for Fire & Rescue
Smart Mobilisation & Navigation Integrated resource-specific satellite navigation with live traffic feeds and automatic status updates.	Reduced Response Times: Appliances are routed via the fastest most appropriate route automatically. Automatic status updates (Mobile, On-Scene etc.) help manage radio traffic more effectively allowing control staff to manage work load effectively especially during spate conditions.
Common Operating Picture (COP) Real-time synchronisation of incident data	Unified Command: Eliminates information silos. An Incident Commander on the ground

Feature / Capability	Operational Benefit for Fire & Rescue
across MDTs, tablets, and Control Room screens.	sees the exact same risk data and resource locations as the Control Room, preventing miscommunication during major incidents.
Geographic Information System (GIS) & Site-Specific Risk Information (SSRI) Includes critical overlay data such as hydrants, building plans superimposed on OS MasterMap and other available map layers.	Pre-Arrival Intelligence: Crews arrive knowing exactly where water sources and hazards (e.g., gas mains, chemical stores) are located, allowing for faster, safer deployment of resources e.g. main jets, breathing apparatus etc.
Incident Command Module Includes Decision Logs, Dynamic Risk Assessments (DRA), and Analytical Risk Assessments (ARA).	Legal & Safety Compliance: Provides a robust digital timeline of decisions. This supports the "Decision Control Process" and supports Incident Commanders by proving due diligence was followed.
Cordon & Sector Management Digital tools to create geo-fenced areas, draw exclusion zones, assign sectors, and designate sector commanders on the map.	Scene Safety: Visually defines hot/warm zones and spans of control in real-time. This ensures every responder knows the safe working limits, reducing the risk of crews straying into unmanaged hazards.
Station Notifier Visualisation of incident details and key risks displayed on station screens immediately upon mobilisation.	Immediate Mental Preparedness: Crews absorb critical risk information (e.g., "Chemical Spill," "Persons Reported") and topographical detail while donning PPE, improving situational awareness before the appliance leaves the engine bay.
Multi-Bearer Connectivity Seamless switching between Airwave, 4G/5G, and Wi-Fi networks without user intervention.	Mission-Critical Reliability: Ensures that risk assessments and messages are delivered even in rural "dead zones." If the 4G network fails, the system automatically maintains the link via available alternative bearers.
Digital Forms Drag-and-drop creation of mandatory forms with validation logic for standard reporting formats.	Accurate Information Sharing: Standardises reporting (e.g., M/ETHANE major incident messages) across the service and other partners if applicable. Validation ensures no critical field is missed before data is transmitted to HQ/Control.
Safer Response Tracking Real-time visibility of all crew members, appliances, and resources on the incident ground.	Crew Accountability: Incident Commanders can instantly see the location of all resources relative to the hazard. For example, if conditions deteriorate, they can visualise resources redeploying to safer locations.

Feature / Capability	Operational Benefit for Fire & Rescue
Risk Management Tools Proactive identification and documentation of risks with automated timestamping.	Audit-Ready Operations: Ensures that every safety decision is captured as it happens. This shifts risk management from a "paper exercise" to a live operational tool that actively safeguards crews.
Comprehensive Audit & Replay "Black box" style logging of every location ping, button press, and decision made during an incident.	Organisational Learning: Enables trainers to "replay" incidents exactly as they unfolded. This is vital for debriefs (Hot/Cold) to identify training gaps and validate successful tactics for future incidents.
Seamless CAD Integration Two-way data exchange with existing Computer Aided Dispatch (CAD) systems.	Operational Continuity: Acts as a force multiplier for existing systems, pulling call data directly from CAD to the MDT without manual re-entry, ensuring data accuracy and speed.

5. GUARDIAN MOBILE MODULES

5.1 The Guardian Mobile solution is built upon a modular, service-oriented architecture. To ensure clarity of supply, we have categorised the software modules into five distinct functional layers.

5.2 CORE APPLICATIONS & CLIENTS

- 5.2.1 **Guardian Mobile Professional:** A comprehensive Windows-based client engineered for ruggedised Mobile Data Terminals (MDTs) and tactical hardware. Designed for the frontline, it delivers critical situational intelligence to drive informed decision-making and streamline communications across the full incident lifecycle.
- 5.2.2 **Guardian Mobile Response:** An agile, cross-platform application for iOS and Android that extends critical core system functionality to smartphones and tablets. This solution ensures seamless connectivity, providing users with real-time access to dispatch information, status updates, location reporting, and text messaging.
- 5.2.3 **Guardian Mobile Web:** A browser-based command console that delivers instant access to mission-critical intelligence and a unified Common Operating Picture to support decisive action from any web-enabled device.

5.3 OPERATIONAL COMMAND MODULES

- 5.3.1 **Guardian Incident Command:** An advanced coordination tool that enables Incident Commanders to establish a live Common Operating Picture, ensuring the seamless real-time synchronisation of risk-critical information, tactical decisions, and resource management between operational crews and control rooms.
- 5.3.2 **Guardian Fire Survival:** A specialised Fire Survival Guidance command module that assists Control Room Operators and Incident Commanders in coordinating complex high-rise, flood or wildfire operations. It utilises live evacuation boards to track resource deployments, record hazards, and manage safety guidance issued to occupants in real-time.
- 5.3.3 **Guardian Station Notifier:** A dynamic station display system that visualises real-time mobilisation data. It presents key incident intelligence immediately upon alert, improving situational awareness and firefighter safety before the crew leaves the station.
- 5.3.4 **Guardian Mobile OpsSim:** An interactive training and simulation environment designed for Station personnel and Trainers to orchestrate realistic incident scenarios. This self-contained suite facilitates end-to-end operational exercises, mirroring live workflows to ensure a seamless transition from training to active duty.

5.4 DATA MANAGEMENT INFRASTRUCTURE

- 5.4.1 **Guardian Mobile Gateway:** The central communications hub that manages secure connectivity and real-time data communications between mobile clients and the dispatch system.
- 5.4.2 **Guardian Mobile Connect:** The dedicated communication service that powers Guardian Mobile Response, ensuring rapid data transmission between handheld devices, the dispatch system, and Guardian Mobile Professional MDTs.
- 5.4.3 **Guardian Mobile DataNexus:** A centralised data processing engine that maintains fleet-wide operational readiness. It utilises automated dataset monitoring to ingest changes, package diverse operational documents, GIS data etc., and seamlessly deploy critical updates to MDTs.
- 5.4.4 **Guardian Mobile FormsStudio:** A visual design tool that enables the rapid creation of professional digital forms. Using intuitive drag-and-drop tools, it allows crews to capture critical incident data, signatures, and multimedia directly on the incident ground.
- 5.4.5 **Guardian Mobile Cartographer:** A dedicated map generation engine that automates the retrieval and processing of Ordnance Survey data to produce optimised tile sets for Guardian Mobile Professional, ensuring crews have access to precise, customised mapping.
- 5.4.6 **Guardian Mobile GeoLocator:** A high-performance geocoding engine embedded within Guardian Mobile Professional and Guardian Mobile Web. It delivers rapid, accurate address and location search results to expedite dispatch, navigation, search and rescue activities.
- 5.4.7 **Guardian Mobile DataPump:** An automated service that synchronises critical operational data across multiple databases. It features flexible pump modes to support real-time updates, historical tracking, and full data integrity.

5.5 INTEGRATION SERVICES

- 5.5.1 **Guardian Mobile Sentinel:** A dedicated proxy service that connects internet-restricted MDTs with external web resources, managing API queries for environmental alerts, geospatial intelligence, and license verification on behalf of the device.
- 5.5.2 **Guardian Mobile SMPP Agent:** A dedicated messaging interface that facilitates high-volume SMS delivery, bridging the core Guardian Mobile ecosystem with mobile networks via standard SMPP protocols.
- 5.5.3 **Guardian PageOne Service:** The specialised integration interface that maintains connectivity with the PageOne network, unifying the delivery of critical alerts across one-way paging, two-way response devices, and SMS channels.

- 5.5.4 **Guardian Mobile GartanLink:** A dedicated service that connects to the Gartan crewing systems to retrieve crew data and publish those within the Guardian Mobile ecosystem.

5.6 ADMINISTRATION

- 5.6.1 **Guardian Mobile Tools:** A comprehensive administrative suite that empowers system administrators to streamline configuration, conduct advanced diagnostics, and maintain granular control over the entire mobile solution lifecycle.
- 5.6.2 **Guardian Mobile CAD Simulator:** The core emulation engine powering the Guardian Mobile OpsSim. It provides a controlled environment for system administrators to test new scenarios, digital forms and software releases without impacting live operations.

6. SOLUTION SCOPE

- 6.1 Motorola Solutions will deliver the core Guardian Mobile software solution, supported by professional services to ensure a seamless, fully integrated deployment for your agency.
- 6.2 This approach provides a complete foundation from which your agency can operate effectively from day one. In addition, your agency has the flexibility to expand functionality by incorporating optional modules, enabling them to further enhance the solution they deliver to their operational crews.
- 6.3 The Guardian Mobile solution is built upon a modular, service-oriented architecture. To ensure clarity of supply, we have categorised the core software modules into four distinct functional layers: Operational End-User Software, Connectivity, Data Management and System Administration.
- 6.4 The following tables define the specific software components included in this proposal.

6.5 OPERATIONAL END-USER SOFTWARE

- 6.6 The user-facing applications deployed on MDTs and web browsers.

Product Module	Function / Description
Guardian Mobile Professional	The primary MDT application provides full operational capabilities, mapping, and incident management for frontline crews.
Guardian Mobile Web (Lite Edition)	A browser-based version of the software, allowing remote access for officers or support staff without requiring full MDT hardware.
Guardian Mobile Sync	A background service ensuring the local MDT data remains synchronised with the central DataNexus server.
Guardian Mobile SatNav Engine - Optional Extra Subscription	An integrated turn-by-turn navigation module for front/rear MDTs.

6.7 CONNECTIVITY & SECURITY LAYER

- 6.7.1 The backbone of the solution, ensuring secure, encrypted message delivery between the Control Room, various agency systems and the MDT fleet.

Product Module	Function / Description
Guardian Mobile Gateway	The core communications engine responsible for routing

Product Module	Function / Description
	real-time operational messages such as mobilisation, status, AVL etc.
Guardian Mobile Citadel	A security service that locks the MDT to a single app or a limited set of apps, preventing users from accessing the desktop, Start menu, or system settings.

6.8 DATA MANAGEMENT & BACK-OFFICE LAYER

6.8.1 The intelligence engine that collates, processes, and distributes risk-critical data (Site Specific Risk Information (SSRI), Point of Interests (POI), Standard Operating Procedures etc.) to frontline crews.

Product Module	Function / Description
Guardian Mobile DataNexus	The central data collation and distribution engine. It automates the ingestion of agency datasets (SSRI, Intelligence, hydrants etc.) and schedules updates to the fleet.
Guardian Mobile DataPump	An automated service that synchronises critical operational data across multiple databases.
Guardian Mobile Gazetteer Importer	A dedicated tool for importing and formatting address data. (Note: Deployed only if the agency is not utilising the standard Guardian CAD gazetteer).
Data Transfer Service	File transfer server (SFTP/FTP) to facilitate data and application updates is supplied by the Agency. The preferred option is SolarWinds Serv-U Managed File Transfer Server.

6.9 CONFIGURATION AND DIAGNOSTIC TOOLS

6.9.1 A suite of utility software enabling the agency to build, test, and maintain their own system configuration.

Product Module	Function / Description
Guardian Mobile Cartographer	A map importer used to process and style Ordnance Survey data for optimised display on MDTs.
Guardian Mobile Configurator	The administrative interface for customising system

	parameters, buttons, user permissions etc.
Guardian Mobile Traffic View	A diagnostic tool for analysing message flows and network traffic in real-time.
Guardian Mobile Test Suite	Includes but not limited to the CAD Simulator, Test Monitor, and Automated Test Service to troubleshoot or validate system operations.

7. PROFESSIONAL SERVICES

7.1 To ensure operational readiness, our proposal includes a comprehensive, end-to-end Professional Services engagement. We go beyond simple installation to deliver a fully managed project lifecycle, ensuring the solution is technically robust, data integrity is maintained, and your team is empowered to manage the system post-launch.

7.2 Our delivery scope includes:

7.2.1 Core Infrastructure & Server Deployment

7.2.1.1 Guardian Mobile Gateway: Deployment, configuration, and commissioning of the Gateway architecture to establish secure, resilient connectivity from the dispatch system to the agency's Guardian Mobile fleet.

7.2.1.2 Guardian Mobile DataNexus: Implementation of the DataNexus engine, including technical consultancy to validate Agency data schemas. We automate the ingestion logic to ensure seamless integration of the Agency's risk and operational datasets.

7.2.1.3 Guardian Mobile Web: Configuration of the secure browser-based interface, enabling real-time asset management and situational awareness for Control Room and Admin users.

7.2.1.4 Guardian Mobile Services: Configuration of other Guardian Mobile Services to provide a holistic and integrated solution

7.2.2 Mobile Client Configuration & Mapping

7.2.2.1 Guardian Mobile Cartographer: Installation and optimisation of the mapping engine, specifically tuned to process and render Ordnance Survey data efficiently on mobile hardware.

7.2.2.2 Guardian Mobile Professional (The "Gold Build"): We configure, test, and validate the software on a single master "Gold" MDT image.

7.2.2.3 Deployment Flexibility: Once validated, this Master Release is handed over to the agency for mass fleet cloning. Alternatively, our software installers are fully compatible with Microsoft Intune or SCCM, enabling the agency to integrate the software into an automated, touchless build workflow.

7.2.3 Quality Assurance & Testing

7.2.3.1 Factory Acceptance Testing (FAT): An internal verification event conducted in a controlled environment. This validates core system functionality against the specification prior to deployment.

7.2.3.2 Site Acceptance Testing (SAT): Comprehensive validation is conducted within the agency's live environment. This confirms successful integration with local

systems (CAD, agency data sources, connectivity etc.) and ensures performance meets operational benchmarks.

7.2.4 Transition & Enablement

- 7.2.4.1 Go-Live: We will provide dedicated engineering support during the critical cutover window. This includes transition planning, execution oversight, and immediate rapid-response support to stabilise operations post-launch.
- 7.2.4.2 Knowledge Transfer (Train-the-Trainer): Deliver a specialised "Train-the-Trainer" course for up to six (6) agency instructors. This session is designed to transfer "Super User" capability, empowering your team to cascade training to operational crews autonomously.
- 7.2.4.3 Project Management & Governance: Continuous oversight to manage the critical path. Our PM provides risk mitigation, schedule management, and strict scope control to ensure the project delivers on time and on budget.

8. SCALABILITY & OPTIONAL ENHANCEMENTS

8.1 The Guardian Mobile architecture is designed to be modular. While the Core Solution provides comprehensive dispatch and data capabilities, the following "Bolt-On" modules are available to extend system functionality. These can be activated during the initial rollout or procured later as the agency's operational requirements evolve.

8.2 ADVANCED INCIDENT COMMAND & CONTROL

8.2.1 Designed for Officer led command support and complex incident management.

8.2.2 Guardian Incident Command Module: This comprehensive suite transforms core MDT functionality into the level required for high-order Command Support operations, such as those within a Command Support Unit or Command Room. It facilitates a complete common operating picture, including sectorisation, resource tracking, and tactical planning necessary for major incidents and multi-agency collaboration.

8.2.2.1 *Includes:* Guardian Mobile FormsStudio to create and manage digital forms such as Analytical Risk Assessment forms, JESIP forms etc.

8.2.2.2 *Benefit:* Enables a full digital audit trail for post-incident debriefs (live and historic).

8.2.2.3 *Integration:* Includes Identity & Access Management to ensure only authorised Commanders/users access sensitive incident command features.

8.3 GUARDIAN FIRE SURVIVAL GUIDANCE (FSG): *[PREREQUISITE: INCIDENT COMMAND MODULE]*

8.3.1 *Critical Functionality:* Seamlessly integrates Control Room FSG records into the Incident Commander's dashboard.

8.3.2 *Common Operating Picture:* Real-time synchronisation allows the Commander and control staff to see exactly where trapped callers are reported to be located within the building footprint or other wide area incidents, e.g. flooding or wildfire.

8.4 MOBILISATION & ALERTING EXTENSIONS

8.4.1 Extending the reach of the Control Room beyond the appliance.

8.4.2 Guardian Station Notifier:

8.4.2.1 *Pre-Alert Displays:* Large-format display integration for Station appliance bays and turnout rooms.

8.4.2.2 *Critical Information:* Displays route overview, assigned crew roster, and risk info to crews before they board the appliance, reducing turnout times.

8.4.3 Guardian PageOne Service:

- 8.4.3.1 *Remote Alerting*: Integration with PageOne devices and apps to mobilise On-Call/Officers and crews who are off-station.

8.4.4 Guardian Mobile SMPP Agent:

- 8.4.4.1 *Mass Communication*: A robust Messaging Engine using Short Message Peer-to-Peer (SMPP) protocol to transmit SMS messages.
- 8.4.4.2 *Use Case*: Enables rapid bulk SMS transmission for recall-to-duty or major incident broadcasting to staff devices.

8.5 AGILE WORKFORCE

8.5.1 Guardian Mobile Response delivers tactical awareness for the modern first responder.

- 8.5.1.1 *App-Based Access*: Extends core Guardian Mobile functionality to standard iOS and Android smartphones/tablets.
- 8.5.1.2 *Functionality*: Provides Mobilisation alerts, Status updates, AVL tracking, and Mapping/Navigation for flexi-duty response officers in non-MDT vehicles.
- 8.5.1.3 *Guardian Mobile Connect*: Secure middleware ensuring app traffic is encrypted and authenticated against the core system.

8.6 SATELLITE NAVIGATION ENGINE

8.6.1 Minimise driver distraction and improve response times providing automated routing.

- 8.6.1.1 *Integrated Routing*: Fully embedded within the Guardian Mobile Professional client (removing the need for separate hardware).
- 8.6.1.2 *Auto-Start*: Routing initiates automatically upon receipt of a mobilization instruction.
- 8.6.1.3 *Dynamic ETA*: Calculates accurate Estimated Time of Arrival (ETA) based on live conditions and shares this instantly with the Control Room and Web Users.

8.7 GUARDIAN TRAINING SIMULATORS:

- 8.7.1 *Provide a risk-free, virtualised sandbox environment that mirrors live operations for safe and effective scenario training.*
- 8.7.2 *Safe Sandbox Environment*: A self-contained, virtualised training suite that replicates the live environment without operational risk.

- 8.7.3 Training Package: Includes two (2) virtual Guardian Mobile Professional MDTs and one (1) virtual Guardian Mobile Gateway/Web, allowing trainers to simulate complex scenarios and fault-finding workflows.

9. IMPLEMENTATION MODEL

9.1 We provide a fully managed, low-risk implementation of the Guardian Mobile solution. Our plan combines a proven PRINCE2-aligned delivery methodology with the deployment of experienced technical leads to oversee supply, integration, and testing. By strictly managing the critical path and risk register, we ensure a streamlined rollout that meets all milestones on time and within budget, ensuring Operational Continuity throughout the transition.

9.2 Our methodology is structured around eight key pillars:

9.3 COMPREHENSIVE DELIVERY PLAN

9.3.1 We utilise a stage-gated project approach to ensure quality control at every step.

9.3.2 Project Phasing: A granular breakdown of the project lifecycle, covering Mobilisation, Planning, Installation, Integration, Testing, Training, and Final Cutover.

9.3.3 Transparency: All phases include defined entry/exit criteria to ensure no stage is closed until quality standards are met.

9.4 EXPERT DELIVERY TEAM

9.4.1 Sector Expertise: Our implementation team consists of highly qualified professionals with specific experience in deploying mission-critical mobility products for the Fire and Rescue and blue-light community. They understand the operational nuances of frontline appliances.

9.4.2 Defined Roles: We provide a clear RACI matrix delineating responsibilities for our Project Managers, Technical Leads, Integration Specialists, and Trainers to ensure accountability.

9.5 MANAGEMENT OF IMPLEMENTATION & TESTING

9.5.1 Our rollout strategy creates a "Gold Build" standard before mass deployment.

9.5.2 Installation & Hosting: A step-by-step provisioning plan for hosting platforms and Guardian Mobile software components.

9.5.3 System Integration: We will fully integrate various Guardian Mobile products with the agency's existing ecosystem. This includes connecting to the Computer Aided Dispatch (CAD) system and importing all critical agency data sets.

9.5.4 Testing Strategy: A rigorous validation phase including Factory Acceptance Testing (FAT), System Testing, and Site Acceptance Testing (SAT).

9.5.5 Note: Formal test events are timeboxed at two (2) days per stage to maintain project momentum.

- 9.5.6 Bench Testing (Golden Image): We will build, test, and deploy an initial Guardian Mobile Pro MDT. This unit serves as the "Gold Build" to validate full communications, data set integrity (including policy applications), and patch management.
- 9.5.7 Pilot Phase (Agency Led): Utilising the validated Gold Build, the Agency will build and deploy two (2) units to selected vehicles for operational field trials.
- 9.5.8 Full Rollout (Agency Led): Following a successful Pilot, the Agency will proceed to build and deploy the software to the remaining frontline fleet.

9.6 PROGRAMME MILESTONES & SCHEDULE

- 9.6.1 Key Milestones: Our schedule tracks critical events including Project Kick-off, Server Provisioning, Software Configuration/Packaging, Integration Sign-off, Training (Pilot & Rollout), and Go-Live.
- 9.6.2 Adaptive Scheduling: Our plan includes calculated buffer periods to accommodate collaborative changes. We prioritise flexibility to adapt to unforeseen operational requirements.
- 9.6.3 Risk Management: We maintain a live Risk Register to proactively identify challenges, implement mitigation strategies, and execute pre-agreed contingency plans for high-risk scenarios.

9.7 Go-LIVE

- 9.7.1 Cutover Plan: A detailed sequence of events to ensure valid user access immediately upon Go-Live.
- 9.7.2 Enhanced Support: Provision of 24/7 support during the initial Go-Live period to immediately triage and resolve any teething issues.
- 9.7.3 User Proficiency: Deployment assumes that Agency Trainers (supported by our Train-the-Trainer program) will have completed end-user training prior to the Go-Live date.

9.8 AGENCY DEPENDENCIES

- 9.8.1 To ensure a successful partnership, the following resources are required from the Agency:
 - 9.8.1.1 Resource Allocation: Dedicated personnel for project management, coordination and UAT. Crucially, the appointment of "Product Champions" at each station is required during the trial period to drive user adoption.
 - 9.8.1.2 Infrastructure: Provision of network access, firewall configuration, and server availability as defined in our System Planning Guide prerequisites.

- 9.8.1.3 Data Provisioning: The agency must provide a full data extract of all risk-critical data sets. This enables our engineers to build the business logic required to import data into Guardian Mobile DataNexus.
- 9.8.1.4 System Planning Guide: We will issue a comprehensive guide detailing server specs, MS AD/EntraID integration, service account requirements etc. The agency must configure their environment in accordance with this guide.

9.9 STAKEHOLDER MANAGEMENT & GOVERNANCE

- 9.9.1 Communication Cadence: Regular status reporting via weekly highlight reports and steering meetings.
- 9.9.2 Feedback Loops: A formal mechanism for stakeholders to review progress and validate that requirements are being met throughout the implementation lifecycle.

9.10 TRAIN-THE-TRAINER

- 9.10.1 Train-the-trainer training is designed to ensure that all personnel can effectively use the Guardian Mobile Software. Our training program includes:
 - 9.10.1.1 Train-the-trainer Workshops: Interactive sessions where users can learn by doing, with guidance from our trainers.
 - 9.10.1.2 User Manuals and Guides: Comprehensive documentation to assist users post-training.

9.11 ADMINISTRATIVE TRAINING

- 9.11.1 Administrative training ensures that system administrators can manage and maintain the software efficiently. This includes:
 - 9.11.1.1 System Configuration: Training on how to manage, configure and customise the system according to the needs of the agency.
 - 9.11.1.2 Troubleshooting: Guidance on how to identify and resolve common issues.

10. ASSUMPTIONS

10.1 The following assumptions underpin the Motorola Solutions proposal:

10.2 HOSTING & INFRASTRUCTURE

10.2.1 Motorola Solutions Hosting: It is assumed that the Guardian Mobile Gateway (for MDT support) and Guardian Mobile Web services will be hosted within the Motorola Solutions Datacentre.

10.2.2 Agency Hosting Obligations: The Agency is responsible for providing the necessary hosting environment either via Virtual Machines (VMs) or an Azure Tenant to support the Guardian Mobile DataNexus application and the optional Guardian Mobile Connect.

10.2.3 Note: The Agency retains responsibility for supplying, licensing, and maintaining all third-party hardware, operating systems, and software required to host components residing outside the Motorola Solutions hosting environment (e.g., within the Agency DMZ).

10.2.4 Remote Access: To facilitate installation, configuration, and ongoing support, the Agency will provide Motorola Solutions with secure remote access to all relevant host machines and environments.

10.3 DATA, MAPPING & INTEGRATION

10.3.1 Data Structure & Structuring: Motorola Solutions assumes that all Agency risk-critical data sets are structured in a format compatible with Guardian Mobile DataNexus import standards

10.3.2 *Limitation:* As the current data structure has not been reviewed, this proposal allocates a fixed cap of five (5) consultancy days for business analysis, import rule creation, and data importation. Any effort required beyond this allocation to cleanse, restructure, or modify data import processes will be treated as Out of Scope and subject to Change Control.

10.3.3 Mapping Services: Guardian Mobile Web is configured by default to use OpenStreetMap via an internet feed. The Agency can add their Ordnance Survey Maps API key to enable OS mapping. Alternatively, the solution can be configured to support other Agency-specified map tile servers, provided technical specifications are compatible and supplied during the design phase.

10.3.4 Identity Management: The Agency is responsible for providing a compatible Identity Provider, such as Microsoft Entra ID (OpenID), to enable secure Single Sign-On (SSO) authentication for Guardian Mobile Web users.

10.4 TECHNICAL PREREQUISITES & INFRASTRUCTURE

- 10.4.1 Internet Connectivity: The solution requires unrestricted outbound internet access to ensure the correct functioning of:
- 10.4.2 Guardian Mobile Gateway and Sentinel communications.
- 10.4.3 Web applications hosted on MDTs or external devices.
- 10.4.4 Third-party API integrations, e.g. Gartner.
- 10.4.5 Private APN Routing: The Agency must ensure that all 4G/5G APN connections are correctly routed to the Motorola Solutions Datacentre. This routing is critical for seamless communication between the Guardian Mobile Gateway, MDTs, and Web components.
- 10.4.6 Firewall Configuration: The Agency retains responsibility for implementing and maintaining all firewall rules necessary to permit traffic between the Guardian Mobile Gateway, Professional, DataNexus, Web, and CAD components. Detailed port requirements are defined in the Guardian Mobile System Planning Guide.
- 10.4.7 Operating Systems: Motorola Solutions supports the current and previous major releases of Android and iOS. This ensures the App maintains optimal stability and security, avoiding risks associated with deprecated OS versions or manufacturer patching inconsistencies.

10.5 AGENCY RESPONSIBILITIES & DEPENDENCIES

- 10.5.1 Project Point of Contact: The Agency will appoint a dedicated Project Manager or Single Point of Contact (SPOC) with decision-making authority to coordinate with Motorola Solutions.
- 10.5.2 Timely Provision of Information: The Agency agrees to provide all necessary agency data sets, technical information, API documentation, and system access required for integration work in accordance with the agreed project schedule. Delays in providing this information may impact the delivery timeline and costs.
- 10.5.3 Third-Party API Procurement & Costs: The Agency retains sole responsibility for procuring and maintaining valid commercial API keys for all external integrations. This includes mapping/data services (e.g., Google Maps, what3words, Met Office, NCEC Chemdata) and messaging providers (e.g. Sinch, GOV.UK Notify). The Agency must supply these keys to Motorola Solutions for configuration and is responsible for all associated costs, including ongoing subscription and message usage fees.
- 10.5.4 Airwave Certification: Whilst Guardian Mobile software is Airwave certified, the agency is solely responsible for securing Airwave certification for their specific MDT build. The agency must determine if such certification is required and is responsible for arranging and funding any associated charges

10.5.5 Integration: The Agency must provide information or access to the system(s) for any integration work in a timely manner.

10.6 COMMERCIAL & LICENSING

10.6.1 Pricing Validity & Inflation:

10.6.1.1 Subscription Indexation: The proposal assumes a minimum 3-year subscription term. Annual fees are subject to increase in line with RPI (Retail Price Index) or CPI (Consumer Price Index).

10.6.1.2 Satellite Navigation: Pricing for the optional Satellite Navigation licenses is based on 2026 rates. Motorola Solutions reserves the right to pass through any OEM price increases incurred at the time of purchase or renewal.

10.6.2 Scope of Deliverables: The quoted price covers the standard Guardian Mobile solution as explicitly defined in this proposal. Any deviations, including custom features, additional scope, or non-standard configurations, will be subject to Change Control.

10.6.3 Licensing Boundaries: Licenses are valid only for use within the designated Agency boundary. The following core licenses will be activated:

10.6.3.1 Guardian Mobile Gateway (Mobility License)

10.6.3.2 Guardian Mobile Sentinel & Sentinel Web

10.6.3.3 Guardian Mobile DataPump & DataNexus

10.6.3.4 Guardian Mobile Professional & Sync

10.6.3.5 Guardian Mobile Citadel

10.6.3.6 Guardian Mobile Cartographer

10.6.3.7 Guardian Mobile Tools

10.6.4 Intellectual Property: All Intellectual Property Rights associated with the software and deliverables remain the exclusive property of Motorola Solutions.

10.6.5 Contractual Pre-requisites: This proposal is subject to the execution of a mutually agreed End User Licence Agreement (EULA).

10.7 DELIVERY APPROACH

10.7.1 Remote Delivery: The majority of implementation and configuration work will be delivered remotely. Onsite attendance is included only where strictly necessary for specific testing, go-live support, or training activities.

10.7.2 Standard Working Hours: All professional services estimates are based on work being performed during standard business hours (09:00 – 17:00, Monday to Friday, excluding Public Holidays). Work required outside these hours will be subject to additional charges.

10.7.3 Environment Availability: The Agency is responsible for ensuring all test and production environments are available and stable prior to the commencement of scheduled installation work. Aborted deployment attempts due to environment unavailability may incur additional charges.