PRIMARY CONTRACTING DOCUMENT

This Primary Contracting Document together with the Master Terms referenced and incorporated below constitutes a Master Agreement by and between **WILLIAMSON COUNTY, TEXAS** ("Customer" or the "County") and **INTERGRAPH CORPORATION by and through its HEXAGON SAFETY, INFRASTRUCTURE & GEOSPATIAL division** ("Hexagon") and is binding upon the Parties on the Effective Date.

1. Those certain Master Terms and Conditions ("Master Terms") attached hereto as Attachment A are incorporated into this Primary Contracting Document as if fully set forth herein.

2. Additionally, the Customer's Solicitation Documents 23RFP55, which shall be incorporated into this Primary Contracting Document, including but not limited to the following provisions are incorporated herein:

   A. Payment. The County's payment for goods and services shall be governed by the Texas Government Code, Chapter 2251.
   Interest charges for any overdue payments shall be paid by the County in accordance with Texas Government Code, Section 2251.025.

   In the event that an error appears in an invoice submitted by Hexagon, the County shall notify Hexagon of the error not later than the twenty-first (21st) day after the date the County receives the invoice. If the error is resolved in favor of Hexagon, Hexagon shall be entitled to receive interest on the unpaid balance of the invoice submitted by Hexagon beginning on the date that the payment for the invoice became overdue. If the error is resolved in favor of the County, Hexagon shall submit a corrected invoice that must be paid in accordance with the time set forth above. The unpaid balance accrues interest as provided by the Texas Government Code, Chapter 2251, if the corrected invoice is not paid by the appropriate date.

   As a minimum, invoices shall include:
   1. Name, address, and telephone number of Hexagon and similar information in the event the payment is to be made to a different address.
   2. The County Contract, Purchase Order.
   3. Identification of items or service as outlined in the Order.
   4. Quantity or quantities, applicable unit prices, total prices, and total amount.
   5. Any additional payment information which may be called for by the Order.

   Payment inquiries should be directed to the following address:
   Williamson County Auditor's Office, Accounts Payable Department
   Email: accountspayable@wilco.org Phone: 512-943-1500

   B. Safety. Hexagon is responsible for initiating, maintaining, and supervising all safety precautions and programs in connection with its Services to be provided hereunder. The safety program shall comply with all applicable requirements of the current federal Occupational Safety and Health Act and all other applicable federal, state, and local laws and regulations.

   C. No Waiver of Immunities. Nothing herein shall be deemed to waive, modify, or amend any legal defense available at law or in equity to the County, its past or present officers, employees, or agents, nor to create any legal rights or claim on behalf of any third party. The

County does not waive, modify, or alter to any extent whatsoever the availability of the defense of governmental immunity under the laws of the State of Texas and of the United States.

D. **Sales and Use Tax Exemption.** The County is a body, corporate and politic, under the laws of the State of Texas and claims exemption from sales and use taxes under Texas Tax Code, Section 151.309, as amended, and the Services and/or Products subject hereof are being secured for use by the County.

E. **Compliance with Laws.** Hexagon shall comply with all federal, state, and local laws, statutes, ordinances, rules and regulations, and the orders and decrees of any courts or administrative bodies or tribunals in any matter affecting the performance of the Contract and any ensuing agreement(s), including, without limitation, Workers' Compensation laws, salary and wage statutes and regulations, licensing laws and regulations. When required, Hexagon shall furnish the County with certification of compliance with said laws, statues, ordinances, rules, regulations, orders, and decrees above specified.

F. **Equal Opportunity.** Neither Party shall discriminate against any employee or applicant for employment because of race, color, sex, religion, or national origin.

G. **Right to Audit.** Hexagon agrees that the County or its duly authorized representatives shall, until the expiration of three (3) years after termination or expiration of the services to be performed, have access to and the right to examine and photocopy any and all books, documents, papers and records of Hexagon, which are directly pertinent to the services to be performed or goods to be delivered for the purposes of making audits, examinations, excerpts and transcriptions. Hexagon agrees that the County shall have access during normal working hours to all necessary facilities and shall be provided adequate and appropriate workspace in order to conduct audits in compliance with the provisions of this section. The County shall give Hexagon reasonable advance notice of intended audits.

3. All capitalized terms in this Primary Contracting Document shall have the same meaning as provided in the Master Terms except as may be otherwise defined herein.

4. Any notice to be given pursuant to Section 13 of the Master Terms shall be directed to each Party at the following address, which reflects the Customer's location, in accordance with the Master Terms.

CUSTOMER:	HEXAGON:
Williamson County, Texas	Attn: Safety, Infrastructure & Geospatial Legal Department
Williamson County	305 Intergraph Way
Attn: County Judge	Madison, Alabama 35758
710 S. Main Street	victor.vasile@hexagon.com
Suite 101	(256) 730-2000
Georgetown, Texas 78626	

5. In executing this Primary Contracting Document, the Parties simultaneously accept, without need to execute any other Order Documents, Orders 1, 2, and 3: the SOW for the HxGN OnCall Dispatch and Records Implementation ("Order 1), HxGN Connect Cloud Program ("Order 2"), and SOW for the Implementation of HxGN Connect ("Order 3" and collectively with Order 1 and Order 2, the "Initial Orders"). The summary pricing for the Initial Orders being accepted through this Primary Contracting Document is reflected below and described in more particularity in the respective Order Documents. Any Change Order to those Order Documents affecting price shall also simultaneously change the information in the table below without the need to separately execute an Amendment.

Initial Orders Pricing Summary		
Order Name	**Description**	**Fee**
Order 1		

	OnCall Dispatch and Records Implementation Services	$6,248,307
Order 2		
	HxGN Connect Cloud Program for Year 1	$30,492
Order 3		
	HxGN Connect Implementation Services	$83,751
TOTAL		**$6,362,550**

6. In consideration of the mutual obligations assumed under this Primary Contracting Document, Customer and Hexagon agree to the terms and conditions set forth herein and represent that this Primary Contracting Document has been executed by each Party's duly authorized representative. The signatories represent that they have the authority to bind their respective organizations to this Primary Contracting Document. This Primary Contracting Document may be executed in counterparts or in duplicate originals. Each counterpart or each duplicate shall be deemed an original copy of this Primary Contracting Document signed by each Party for all purposes.

AGREED TO BY:

WILLIAMSON COUNTY, TEXAS

By: _____

Name: _____

Title: _____

Date: _____

INTERGRAPH CORPORATION

By: Signed by: Rachel Bryan E8867318855348D...

Name: Rachel Bryan

Title: Analyst - Finance

Date: December 6, 2024

ATTACHMENT A

MASTER TERMS AND CONDITIONS

These Master Terms and Conditions (the "Master Terms") govern transactions and relations between Customer and Hexagon (each a "Party" and collectively the "Parties").

Hexagon will make available to Customer certain proprietary software, including related proprietary Documentation; software maintenance services; Equipment/Content; DevTools; Cloud Programs; and professional services; and other items, which will be provided to Customer pursuant to these Master Terms and an Order. Before Hexagon will provide any items or services (including the Services), Customer must agree to these Master Terms and the corresponding Order. The Parties agree these Master Terms will govern each Order. To the extent the Master Agreement purports to impose obligations, restrictions, or limitations upon Customer's Affiliates or Users, Customer shall be responsible to Hexagon for Customer's Affiliates' and Users' compliance with such terms and shall procure Customer's Affiliates and Users compliance.

These Master Terms consist of the following:

- The General Terms and Conditions set forth below;
- Exhibit A – End User License Agreement;
- Exhibit B – Maintenance Terms and Conditions for Software;
- Exhibit C – Sample Project Deliverable Sign-Off Form;
- Exhibit D – Cloud Program Conditions;
- Exhibit E – Subscription License Terms;
- Exhibit F – COTS Training Program Terms; and
- Exhibit G – Common Terms Glossary.

GENERAL TERMS AND CONDITIONS

1 Definitions. All capitalized terms not otherwise defined herein shall have the meaning set forth in Exhibit G (Common Terms Glossary). Words used herein in the singular, where the context so permits, shall be deemed to include the plural, and vice versa.

2 Elements of an Order.

2.1 Order Composition. Each Order will be comprised of Order Documents, including any applicable Schedule(s). An Order is formed only once both Parties accept the Order Documents, which the Customer shall do by executing the Order Documents and/or issuing a PO in connection with the Order Documents. Orders shall be effective as of the date both Parties accept the Order Documents except where the Order is for a term-based offering (e.g., Subscription License), in which case the Order shall commence as of the date specified in the Order Documents, if provided.

2.2 Schedules. Any Schedules applicable to Products or items purchased in an Order are incorporated and are either included in the Order Documents or, in the absence thereof, accessible via hyperlinks contained within Exhibit G. If a Product or item is not listed in the document(s) accessed via hyperlinks

provided in Exhibit G, and related Schedule(s) are not otherwise included in the Order Documents, then that Product or item does not have a corresponding Schedule.

2.3 Pricing. Order Documents shall describe basic pricing and include other details relevant to the offerings included in the Order.

2.4 Change Control. During the course of Hexagon's performance under an Order, either Party may request a change in the scope of the Order in writing, delivered to the other Party. Any changes in price, schedule, or other terms must be documented either by an amendment or Change Order. No change, as contemplated in this paragraph, shall become effective until set forth in a mutually executed writing.

2.5 Acceptance. Acceptance will occur based upon the following:

2.5.1 For Fixed Price Project Assignments, not governed by Exhibit F, acceptance shall occur when the applicable Task Acceptance Criteria has been satisfied in accordance with the Task Acceptance Process.

2.5.2 For Time and Materials Project Assignments and Maintenance Services, the Services are accepted as performed.

2.5.3 For a Cloud Program, acceptance occurs when the License Keys are provided to Customer.

2.5.4 For all Orders not described more specifically above, acceptance occurs once the ordered item has been delivered or access to the ordered item has been provided and completion of a Project Deliverable Sign-Off Form provided that Hexagon may issue the invoice upon delivery of the Products notwithstanding the return of the executed Project Deliverable Sign-Off Form. If, however, the Customer reasonably disputes the delivery of the Products specified in the Quote it may return the Project Deliverable Sign-Off Form with such notation to Hexagon and toll the timing of the payment of the invoice associated with that Order until the issue is resolved.

3 Composition of the Master Agreement.

3.1 Components. The agreement between the Parties (herein referred to as the "Master Agreement") consists of: (1) the Primary Contracting Document, (2) County's Solicitation Documents (23RFP55), (3) these Master Terms (including the General Terms and Conditions and all Exhibits), (4) any amendments to the Master Agreement, (4) Orders, together with any Change Orders, that may be delivered, prepared, or issued after the Effective Date, and (5) all documents, including applicable Schedules and documents referenced via hyperlink, incorporated by reference in the documents identified in this Section. For certain Third Party Software, Third Party Terms will also be applicable and be considered as part of the Master Agreement.

3.2 Order of Precedence. In the event of any conflict or inconsistency among documents forming the Master Agreement, the following order of precedence shall be used to determine the resolution of the discrepancy, unless the Parties mutually agree in writing to an alternative decision:

(1) Any amendments to the Master Agreement;

(2) The Primary Contracting Document;

(3) Applicable Schedules;

(4) These Master Terms (excluding Exhibits);

(5) Exhibits to these Master Terms; and

(6) Order Documents, if any, in addition to items specifically identified in this Section 3.2 above.

(7) Hexagon Response to (RFP 23RFP55)

(8) County's Solicitation Documents (23RFP55)

For only Third Party Software subject to Third Party Terms, the Third Party Terms shall have precedence in the event of a conflict between the Third Party Terms and any other terms of the Master Agreement.

4 Invoicing and Payment.

4.1 Invoices. Invoices shall be issued based upon the contents of the Order. Williamson County will provide invoice submission instructions.

4.1.1 For Fixed Price Project Assignments Hexagon may invoice Customer upon completion of a milestone identified in the Order Documents, or when applicable, in accordance with Exhibit F; provided however, if this type of Order also includes Subscription Licenses or Cloud Program(s), the fees for such shall be due in accordance with Exhibits E and D, respectively.

4.1.2 For Product(s) or items not included within an Order for a Fixed Price Project Assignment or otherwise more specifically addressed in this Section 4, Hexagon may invoice Customer for the full amount set forth in the Quote in addition to any applicable freight/shipping charges upon delivery of or access having been provided to any of the Product(s) or items identified in the Order Documents.

4.1.3 Time and Materials Project Assignments shall be billed and invoiced monthly as the hours are expended and Onsite Fees are incurred, or after all hours set forth in the Order Documents have been expended, whichever occurs first.

4.1.4 Maintenance Services not included within an Order for a Fixed Price Project Assignment or Product Order shall be billed and invoiced in accordance with Exhibit B.

4.1.5 Cloud Program(s) (even if included within a Fixed Price Project Assignment) shall be billed and invoiced in accordance with Exhibit D.

4.2 Payment. OMITTED.

4.3 Late Payment. OMITTED.

4.4 Taxes. OMITTED.

5 Term and Termination.

5.1 Term. The Term of the Master Agreement shall begin on the Effective Date and remain in effect for a period of sixty (60) consecutive Months (“Initial Term”) or until the Master Agreement is earlier terminated pursuant to the terms set forth herein or by mutual agreement of the Parties. At the end of the Initial Term, the parties may renew the Master Agreement for up to five (5) additional twelve (12) month terms, with the terms and conditions remaining the same. An Order that is executed prior to the expiration of the term of the Master Agreement shall be governed by the Master Agreement even if the Master Agreement Term expires during the performance of the Order. To the extent Customer executes an Order pursuant to later issued master terms, then this Master Agreement shall terminate upon completion of all Orders executed hereunder regardless of the amount of time remaining in the Term.

5.2 Termination for Convenience. Either Party may terminate the Master Agreement or an Order in its sole discretion at any time upon providing the other Party with thirty (30) days written notice. In the event of a termination pursuant to this paragraph, Customer agrees to pay Hexagon for the Work performed and Product(s) or items delivered and provided, plus the cost of any labor and/or Product(s) or items ordered in good faith prior to notice of termination that could not be canceled, less amounts previously paid by Customer for such Work and/or Product(s) or items. Hexagon is entitled to retain all amounts paid under any Order prior to termination for Products and Services actually received or ordered and could not reasonably be cancelled at the time notice of termination is received. To the extent a Party exercises its right to terminate a specific Order, that termination shall have no effect upon the remaining Master Agreement, which, along with any other active Orders, shall remain in full force and effect. If a Party desires to terminate the Master Agreement, then the Parties shall proceed to wind down all ongoing work under the respective Orders in effect under the Master Agreement by the termination date. Each Party shall take commercially reasonable steps to bring the work to a close and to reduce its costs and expenditures.

5.3 Termination for Cause. Either Party may terminate the Master Agreement or a specific Order, as the case may be, in the event the other Party materially breaches a material term of the Master Agreement or any Order.

5.3.1 In the event a Party materially breaches an Order, the non-breaching Party may terminate the Order only after providing a sixty (60) calendar day cure period to cure such breach and the breach has not been cured, except for material breaches arising from non-payment. During the sixty (60) day cure period, the Parties shall try to determine a mutually agreeable plan to cure such breach. If such breach cannot be cured or an acceptable plan is not provided within the sixty (60) day cure period, the non-breaching Party may, but does not have the obligation to, terminate the Order.

5.3.2 In the event a Party materially breaches the Master Agreement or multiple Orders, the non-breaching Party may terminate the Master Agreement only after providing a sixty (60) calendar day cure period to cure such breach and the breach has not been cured except for material breaches arising from non-payment. During the sixty (60) day cure period, the Parties shall try to determine a mutually agreeable plan to cure such breach. If such breach cannot be cured or an acceptable plan is not provided within the sixty (60) day cure period, the non-breaching Party may, but does not have the obligation to, terminate the Master Agreement. If the Master Agreement is terminated pursuant to this paragraph, by the termination date, Hexagon will stop all Work pursuant to any Orders arising under the Master Agreement.

5.3.3 If the Master Agreement or any one or more Orders is terminated pursuant to paragraphs 5.3.1 or 5.3.2, Hexagon will stop all Work with respect to impacted Orders as soon as practicable and shall be entitled to payment for all Work performed as well as Product(s) provided on all impacted Orders up to the termination date, less amounts previously paid by Customer under the affected Orders.

5.3.4 Notwithstanding the foregoing, Hexagon may suspend its performance of or terminate any Order or the Master Agreement for cause if payment is not received within thirty (30) days following the date when payment was due. In the event an Order is suspended or terminated for cause, Hexagon shall be entitled to, and Customer agrees to pay Hexagon, payment for Work performed and/or Product(s) delivered on said Order up to the suspension or termination date, less amounts previously paid by Customer under the affected Orders. Hexagon is entitled to retain all amounts paid under any Order prior to its termination. If Hexagon suspends an Order under this paragraph, then it may thereafter terminate the Order upon giving written notice to Customer.

5.3.5 Notwithstanding the foregoing, Customer may not exercise a termination pursuant to the terms of Section 5.3 if Hexagon's material breach of the terms and conditions of the Master Agreement or any Order thereunder is caused or partially caused by Customer's negligence or failure to perform its obligations.

6 Ownership.

6.1 Customer acknowledges Hexagon will retain ownership and title of Hexagon IP made or provided pursuant to any Order. All Software (including Software embedded within Equipment) provided under the Master Agreement is licensed to Customer in accordance with Exhibit A (End User License Agreement), except as it is inconsistent with the terms set forth herein. Third Party Software, including any Software developed by a third party embedded within Equipment, is licensed to Customer pursuant to Third Party Terms or as otherwise specified in the applicable E/C Schedule.

6.2 As it pertains to any Equipment, and only Equipment, provided to Customer under an Order, the Customer shall receive title to and ownership of the Equipment identified in the Order Documents, excluding any IPR pertaining to the Equipment and Software provided with the Equipment, FOB place of destination and subject to Customer's payment of all amounts owed for the Equipment.

6.3 Customer shall own Customer Data. Customer grants Customer Data Rights to Hexagon, to, among other things, facilitate Hexagon's performance of its obligations.

7 Warranties.

7.1 Software. The Software Products licensed under Exhibit A are warranted to meet Minimal Operations Levels for a period of thirty (30) days from the initial installation; additional warranties are covered by a Maintenance Contract between Customer and Hexagon shall instead be warranted and supported as stated in the Maintenance Contract.

7.2 Subsystem Warranty Coverage. For, and only for, new Subsystems procured/implemented pursuant to an Order under these Master Terms, the warranty coverage shall be set forth in the applicable Order Documents, which shall be in lieu of the warranty coverage set forth in Section 7.1.

7.3 Equipment Warranty Coverage. If Equipment supplied by Hexagon is provided with a warranty or other Equipment support, then the extent of the Equipment support is provided within the corresponding E/C Schedule or other Order Documents.

7.4 Third-party Warranty Coverage. To the extent no warranty or Equipment support is described in the applicable E/C Schedule or other Order Documents, third-party products supplied by Hexagon, are provided with a pass-through-warranty from the original manufacturer, if any.

7.5 Disclaimer. Any product information Hexagon has shared with Customer during the proposal and/or contract activities to date was to provide an understanding of Hexagon’s current expected direction, roadmap, or vision and is subject to change at any time at Hexagon’s sole discretion. Hexagon specifically disclaims all representations and warranties regarding future features or functionality to be provided in any Software or Deliverable(s). Hexagon does not commit to developing the future features, functions, and/or products discussed in this material beyond that which is specifically committed to being provided by Hexagon pursuant to a valid Order. Customer should not factor any future features, functions, or products into its current decisions since there is no assurance that such future features, functions, or products will be developed. When and if future features, functions, or products are developed, they may be made generally available for licensing by Hexagon.

7.6 Warranty Disclaimer. EXCEPT AS SPECIFICALLY SET FORTH IN THIS ARTICLE, HEXAGON DISCLAIMS (TO THE FULLEST EXTENT PERMITTED BY LAW) ALL WARRANTIES ON PRODUCTS FURNISHED PURSUANT TO THE MASTER AGREEMENT, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, DURABILITY, FITNESS FOR A PARTICULAR PURPOSE, HIGH RISK USE, AND NON-INFRINGEMENT. ALL WARRANTIES PROVIDED PURSUANT TO THIS MASTER AGREEMENT ARE VOID IF FAILURE OF A WARRANTED ITEM RESULTS DIRECTLY OR INDIRECTLY FROM AN UNAUTHORIZED USE OR MISUSE OF A WARRANTED ITEM, INCLUDING, WITHOUT LIMITATION, USE OF A WARRANTED ITEM UNDER ABNORMAL OPERATING CONDITIONS OR UNAUTHORIZED MODIFICATION OR REPAIR OF A WARRANTED ITEM OR FAILURE TO ROUTINELY MAINTAIN A WARRANTED ITEM. THE WARRANTIES SET FORTH IN THIS ARTICLE 7 ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, AND, EXCEPT AS SET FORTH IN ARTICLE TITLED “INDEMNIFICATION PROVISIONS” BELOW, REPRESENT THE FULL AND TOTAL WARRANTY OBLIGATION AND/OR LIABILITY OF HEXAGON.

8 LIMITATION OF LIABILITY

IN NO EVENT WILL HEXAGON BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR SPECIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS, LOSS OF USE OR PRODUCTION, LOSS OF REVENUE, LOSS OF DATA, OR CLAIMS OF THIRD PARTIES, EVEN IF HEXAGON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. UNDER NO CIRCUMSTANCE WILL HEXAGON'S LIABILITY UNDER THIS MASTER AGREEMENT EXCEED THEORDER VALUE UNDER WHICH THE EVENT GIVING RISE TO THE CAUSE OF ACTION HAS OCCURRED.

9 Indemnification Provisions.

9.1 Subject to the limitation of liability provisions in the Master Agreement, Hexagon will defend, at its expense, a third party action, suit, or proceeding against Customer ("Claim"), and indemnify Customer from any judgments, settlements, and reasonable attorney's fees resulting therefrom, to the extent such Claim is (i) attributable to bodily injury, death, or physical damage to tangible property caused by Hexagon's negligent acts or omissions arising under the Master Agreement; or (ii) based upon an allegation that a Software Product, Customized Software, Cloud Application, or Services Deliverable as of its delivery date

under the Master Agreement, infringes a valid United States: patent, copyright, or trademark, or misappropriates a third party's trade secret ("Infringement Claim").

9.2 Hexagon's defense and indemnification obligations are conditioned upon:

9.2.1 Customer providing prompt written notice to Hexagon of any Claim;

9.2.2 Hexagon having primary control of the defense of any actions and negotiations related to the defense or settlement of any Claim, understanding Hexagon may not settle a claim without Customer's consent if such settlement assigns fault or culpability to Customer; and

9.2.3 Customer cooperating fully in the defense or settlement of any Claim.

9.3 Hexagon will have no obligation to defend Customer or to pay any resulting costs, damages, or attorneys' fees for any Infringement Claims alleging direct or contributory infringement of the Software Product, Cloud Program, or Service Deliverable (i) by the combination of or integration with a product, process, or system not supplied by Hexagon; (ii) by material alteration by anyone other than Hexagon or its subcontractors; (iii) by use after Customer has been notified of possible infringement; (iv) by use after modifications are provided to Customer; (v) by use after a return for refund as described below is ordered by Hexagon; (vi) if the creation of which was pursuant to specifications provided by Customer; or (vii) by use other than as specified in the Documentation associated with the Software Product.

9.4 In connection with any Infringement Claims, Hexagon, at its own expense and option, may either (i) obtain rights for Customer to continue using the allegedly infringing Hexagon supplied item; (ii) replace the item with a non-infringing alternative, or modify the allegedly infringing elements of the item, while maintaining substantially similar software functionality or data/informational content; or (iii) refund to Customer a prorated portion of the license fees paid by Customer for the infringing item(s); provided that proration for perpetually licensed software shall be based on a five (5)-year, straight-line depreciation basis beginning from the initial date of delivery. In the event of a prorated return, Customer will uninstall, cease all use of and return to Hexagon the infringing item(s).

9.5 In no event will the indemnification for Infringement Claims apply to any Beta Software, or sample, hot fix, royalty free, or evaluation software delivered pursuant to the Master Agreement.

9.6 This section provides the sole and exclusive remedies of Customer and Hexagon's entire liability in the event of a Claim. Customer has no right to recover, and Hexagon has no obligation to provide any other or further remedies, whether under another provision of the Master Agreement or any other legal theory or principle in connection with a Claim.

10 Insurance.

10.1 Policies and Coverage Amounts. Hexagon agrees to procure and maintain in force during the term of the Master Agreement, at its own cost, the policies and amounts of coverage as indicated below.

Workers' Compensation:

Coverage A: Statutory

Coverage B: $100,000

2. General Liability:

Per Occurrence: $1,000,000

Personal/Advertising Injury: $2,000,000

General Aggregate: $2,000,000

Products/Completed Operations: $2,000,000

Fire Damage Legal Liability: $100,000

3. Automobile Liability:

Combined Single Limit: $2,000,000

4. Professional Liability:

Per Occurrence: $2,000,000

General Aggregate: $2,000,000

D. The following provisions shall be agreed to by Hexagon:

1. No change, cancellation, or nonrenewal shall be made in any insurance coverage without a thirty (30) day written notice to the County from Hexagon. Hexagon shall furnish a new certificate prior to any change or cancellation date. The failure of Hexagon to deliver a new and valid certificate will result in the suspension of all payments until the new certificate is furnished.

Liability Insurance “Claims Made” basis:

If the liability insurance purchased by Hexagon has been issued on a “claims made” basis, Hexagon must comply with the following additional conditions. The limits of liability and the extensions to be included as described previously in these provisions remain the same. Hexagon must either:

a. Agree to provide, prior to commencing work under the contract, certificates of insurance evidencing the above coverage for a period of two (2) years after final payment for the Contract for general liability policies and five (5) years for professional liability policies. This certificate shall evidence a “retroactive date” no later than the beginning of Hexagon’s work under this contract or

b. Purchase the extended reporting period endorsement for the policy or policies in force during the term of this Contract and evidence the purchase of this extended reporting period endorsement by means of a certificate of insurance or a copy of the endorsement itself.

3. Hexagon must disclose the amount of deductible/self-insured retention applicable to the general liability, automobile liability and professional liability policies, if any. Williamson County reserves the right to request additional information to determine if Hexagon has the financial capability to meet its obligations under a deductible/self-insured plan, which Hexagon may comply with by only providing the Annual Report for its parent company or itself. If this provision is utilized, Hexagon will be permitted to provide evidence of its ability to fund the deductible/self-insured retention.

4. Hexagon agrees to provide insurance issued by companies admitted within the State of Texas, with the Best’s Key Rating of at least A: VII.

a. European markets, including those based in London, and the domestic surplus lines market that operates on a non-admitted basis are exempt from this requirement provided that Hexagon’s broker can provide financial data to establish that a market’s policyholder surpluses are equal to or exceed the surpluses that correspond to Best’s A: VII Rating.

5. Hexagon will provide an original signed Certificate of Insurance and such endorsements as prescribed herein.

6. Williamson County, its officers, employees, and member agency evaluation team personnel shall be named as an “additional insured” on the automobile and general liability policies, and it shall be stated on the Insurance Certificate with the provision that this coverage “is primary to all other coverage Williamson County may possess.” (Use “loss payee” where there is an insurable interest.)

7. Compliance by Hexagon with the foregoing requirements as to carrying insurance shall not relieve Hexagon of the liability provisions of the contract.

Contractual and other liability insurance provided under this Contract shall not contain a supervision, inspection or engineering services exclusion that would preclude Williamson County from supervising and/or inspecting the project as to the end result. Hexagon shall assume all on-the-job responsibilities as to the control of persons directly employed by it.

Precautions shall always be exercised for the protection of persons (including employees) and property.

Hexagon is to comply with the Occupational Safety and Health Act of 1970, Public Law 91956, as it may apply to this contract.

Any loss insured under subparagraph 9.6.B.4 is to be adjusted with the project PM and made payable to Williamson County as trustee for the requirements of any applicable mortgagee clause.

If an “ACORD” Insurance Certificate form is used by Hexagon’s insurance agent, the words “endeavor to” and “. . . but failure to mail such notice shall impose no obligation or liability of any kind upon the company” in the “cancellation” paragraph of the form shall be deleted.

Hexagon agrees to waive all rights of subrogation against Williamson County, its officers, employees, and agents.

10.2 Certificate of Insurance. A Certificate of Insurance shall be completed by Hexagon’s insurance agent(s) as evidence that policies providing the required coverage amounts, conditions, and minimum limits are in full force; and, the completed Certificate of Insurance shall be sent to the Customer’s Risk Management Department 301 South East Inner Loop Suite 105 Georgetown, TX 78626.

10.3 Insurance Deductible. Hexagon shall be solely responsible for any deductible losses under the policies required above.

11 Security and Breach Notification.

11.1 Hexagon shall take reasonable industry action to prevent, detect, identify, report, track and respond to Security Incidents. In the event of a Security Incident, Hexagon will provide a Security Incident report to the Customer or its Affiliates via the Designated Portal. The report shall be provided within twenty-four (24) Business Hours following Hexagon’s discovery, confirmation, and investigation of a Security Incident.

12 Dispute Resolution.

12.1 Resolution Protocol. The Parties shall exercise their best efforts to negotiate and settle promptly any dispute that may arise with respect to the Master Agreement or Order made pursuant to the Master Agreement ("Dispute") in accordance with the provisions set forth herein. If either Party disputes any provision of the Master Agreement (the "Disputing Party"), or the interpretation thereof, or any conduct by the other Party under the Master Agreement, the Disputing Party shall bring the matter to the attention of the other Party at the earliest possible time in order to resolve the Dispute, except for Disputes for non-payment. If such Dispute is not promptly resolved by the employees responsible for the subject matter of the Dispute, the Disputing Party shall be permitted to deliver to the non-disputing Party's contact person identified in the Primary Contracting Document a written notice of the Dispute, whereupon the Parties shall endeavor in good faith to escalate the Dispute to appropriate executives for each Party for resolution within fifteen (15) Business Days, or such longer period as to which the Parties may mutually agree.

12.2 Mediation. To the extent a Dispute is not resolved through the process outlined in the previous section and remains unresolved, the Parties agree to enter into non-binding mediation to resolve the Dispute. Within sixty (60) calendar days, of the issuance of the Dispute notice, or such longer period that is mutually agreeable to the Parties, the Parties agree to identify a mutually acceptable mediator who shall mediate the Dispute. If, after making reasonable efforts to identify a mutually acceptable mediator and no later than fifty (50) calendar days after the issuance of the Dispute Notice, the Parties are unable to identify such a mediator, the Disputing Party shall provide the non-disputing Party with a list of five (5) proposed mediators. The non-disputing Party shall have five (5) Business Days from receipt of such list from the Disputing Party to identify one proposed mediator on the list to use as a mediator. If the non-disputing Party fails to identify and communicate its choice to the Disputing Party in the time allotted, then the Disputing Party shall be permitted to unilaterally identify the mediator from the list of five (5) mediators previously given who shall mediate the Dispute. The mediator shall be an attorney licensed to practice law in the state courts identified in section below titled "Governing Law." Subject to the mediator's availability, the Parties agree to mediate the Dispute within thirty (30) days after the Parties have identified a mediator who has agreed to mediate the Dispute. To the extent the mutually identified mediator is unavailable, unwilling, or unable to mediate the Dispute, the Parties shall utilize the same steps listed above to identify a new mutually agreeable mediator. To the extent the Disputing Party had to prepare a list of proposed mediators previously, it shall prepare and transmit a revised list within five (5) Business Days of receiving notice of the proposed mediator's unavailability. Subject to the mediator's requirements, the Parties agree they shall be permitted to attend the mediation via telephone or video conferencing. The Parties agree to pay in equal shares the mediator's fee and expenses unless otherwise agreed to pursuant to a settlement agreement.

12.3 Prerequisites to Litigation. Except for Disputes for non-payment, only after the Parties have endeavored to resolve the Dispute through the processes outlined in the immediately preceding two sections may a Party commence litigation to resolve the dispute.

12.4 Injunctive Relief. Notwithstanding the foregoing, either Party may, before or during the exercise of the informal dispute resolution procedures set forth above, apply to a court identified in the section titled "Governing Law" for a temporary restraining order or preliminary injunction where such relief is necessary to protect its interests pending completion of such informal dispute resolution procedures.

13 Notices.

All notices given between the Parties shall be in writing and shall be considered properly sent by postage prepaid United States Mail or overnight carrier to the Customer and/or Hexagon representative, as applicable and identified in the Primary Contracting Document, or such substitutes as may hereafter be disclosed by proper notification.

14 Force Majeure.

Neither Party shall be deemed to be in default of any provision of the Master Agreement or an Order or be liable for any delay, failure in performance, or interruption of service resulting from acts of war, acts of terrorism, criminal acts, acts of God, natural disaster, fire, lightning, acts of or restriction imposed by civil or military authority, pandemics, epidemics, cyber-attack, labor disruption, civil disturbance, expropriation,

embargo, lawful export restriction, or any other cause beyond its reasonable control. This section does not relieve or suspend a Party's obligation to pay money to the other Party under the terms of the Master Agreement.

15 Place of Performance.

To the extent necessary, Customer agrees to provide appropriate workspace and workplace accommodations; computer equipment; software; access to relevant data, documents, plans, reports, and analyses; and necessary access for Hexagon personnel to perform work on an Order. To the extent work is performed remotely, Customer must provide VPN or secured remote connectivity (including a login and password) to all servers and workstations requiring installation/configuration by Hexagon.

16 Amendments.

Any and all amendments to the Master Agreement shall be in writing specifically reference the fact the amendment is intended to alter these Master Terms and executed by authorized representatives of both Parties. No Order or Change Order shall affect these Master Terms, unless expressly stated in such document.

17 Confidential Information.

The Parties agree not to disclose Confidential Information provided to it by the Disclosing Party to the maximum extent allowable under applicable law unless it first obtains the Disclosing Party's written consent to such disclosure. It is further understood and agreed that money damages may not be a sufficient remedy for any breach of this provision of the Master Agreement by the Receiving Party and the Disclosing Party may seek equitable relief, including injunction and specific performance, as a remedy for any such breach. Such remedies shall not be deemed to be the exclusive remedies for a breach of this provision of the Master Agreement but will be in addition to all other remedies available at law or equity. The covenants set forth herein and the rights and obligations related thereto shall continue for a period of five (5) years from the date of disclosure.

18 Personal Data.

18.1 Where Personal Data is provided by the Customer to Hexagon, the Customer shall act as the data controller and shall be responsible for complying with all applicable data protection laws. Hexagon shall act as the data processor in respect of such Personal Data and shall process the Personal Data in accordance with applicable data protection laws. The Customer acknowledges and agrees that Hexagon is not capable of being a data controller due to Hexagon's inability to determine the purpose and means of the processing of Personal Data provided by Customer to Hexagon. To the extent that: (a) Personal Data of Users or Authorized Cloud Users provided by the Customer to Hexagon pursuant to the Master Agreement is subject to the European Union General Data Protection Regulation 2016/679, as may be amended from time to time ("GDPR"); and (b) the Customer and Hexagon do not have a separate, written data processing agreement, then the Customer and Hexagon agree that the terms of Hexagon's Data Processing Addendum, as updated from time to time, found at: https://www.hexagonsafetyinfrastructure.com/-/media/Legal/Hexagon/SI/Policies/DPA/DPALP/DPA_LP_08-2019.pdf, shall apply.

18.2 Where Customer is responsible for providing Personal Data on behalf of Users or Authorized Cloud Users directly to Hexagon, Customer will secure and maintain all necessary consents and make all necessary disclosures before including Personal Data in Customer Data input to, or otherwise supplied to Hexagon. In the event Customer, including all its Users, does not consent to Personal Data being processed as a result of the Master Agreement, Customer acknowledges Hexagon may be unable to provide Services, Product(s), Maintenance Services, and/or Cloud Program (or part thereof).

18.3 Hexagon will only process Customer supplied Personal Data in accordance with the Customer's lawful instructions and to the extent and as necessarily required to provide the applicable goods and services under the Master Agreement and for no other purpose. Except as may be otherwise required by law, contract, or judicial order, after expiration or earlier termination of the Master Agreement, Hexagon will destroy all Customer-supplied Personal Data in accordance with applicable data protection laws.

18.4 If Hexagon supplies maintenance, support, or subscription services to Customer with respect to third-party products, and if the third-party supplier or proprietor of such requires Customer be party to any data processing agreement in connection therewith, and if Customer has not separately executed an instrument to satisfy such requirement, then Customer and Hexagon agree that the terms of the applicable third-party data processing agreement, as updated from time to time, found at https://www.hexagonsafetyinfrastructure.com/-/media/Legal/Hexagon/SI/Policies/DPA/DPALP/DPA_LP_08-2019.pdf, shall apply.

19 Assignment.

Neither Party shall assign, sublet, or transfer all or any portion of the Master Agreement, nor any interest in the Master Agreement, without the express written consent of the non-assigning Party, which consent may be granted or withheld in the sole discretion of the non-assigning Party. Notwithstanding the foregoing, Hexagon may assign its rights and obligations under the Master Agreement, without the approval of Customer to: (1) an Affiliate or (2) another business entity in connection with a merger, consolidation, or reorganization of Hexagon or any of its subsidiaries.

20 Cooperative Purchasing.

If Customer is a government entity, another government entity (referred to in this paragraph as a cooperative purchaser) may, with prior written consent of Hexagon, use the Master Agreement, excluding Orders to which it is not a party, as a contract vehicle for its purchases from Hexagon; provided that in such event the term "Customer" shall refer solely to the relevant cooperative purchaser with respect to its transaction and shall not refer to the cooperative purchaser with respect to transactions not for its direct benefit. Product(s) and services will be priced and scoped upon request of the cooperative purchaser and dependent upon the scope of the intended project. To the extent this clause is exercised by any cooperative purchaser with Hexagon's consent, Hexagon shall deal directly with the cooperative purchaser regarding the scope and pricing of the project. Cooperative purchasers shall make their own legal determination as to whether the collective purchasing permitted by this clause is consistent with laws, regulations, and other policies applicable to the cooperative purchaser; and, Customer shall have no liability with respect to obligations of any cooperative purchaser utilizing the terms of this section 20 to place Orders under the Master Agreement.

21 Export.

Equipment/Content, and Hexagon IP, including any technical data related to Software, Services, Maintenance Services, or Cloud Programs, are subject to the export control laws and regulations of the United States. Diversion contrary to United States law is prohibited. Equipment/Content and/or Hexagon IP, including any technical data related to Software, Services, Maintenance Services, or Cloud Programs, shall not be exported or re-exported, directly or indirectly (including via remote access), under the following circumstances:

- To Cuba, Iran, North Korea, Syria, the Crimean region of Ukraine or any national of these countries or territories;
- To any person or entity listed on any United States government denial list, including, but not limited to, the United States Department of Commerce Denied Persons, Entities, and Unverified Lists, the United States Department of Treasury Specially Designated Nationals List, and the United States Department of State Debarred List (http://export.gov/ecr/eg_main_023148.asp);
- To any entity if Customer knows, or has reason to know, the end use is related to the design, development, production, or use of missiles, chemical, biological, or nuclear weapons, or other unsafeguarded or sensitive nuclear uses; and/or
- To any entity if Customer knows, or has reason to know, that a reshipment contrary to United States law or regulation will take place.

Customer agrees to comply with all applicable export control laws and regulations. User shall not request information or documentation where the purpose of such request is to support, give effect to or comply with a boycott of any country that is not sanctioned by the United States, including but not limited to the Arab League boycott of Israel. Any questions regarding export or re-export of the Software should be addressed to Hexagon's Export Compliance Department at 305 Intergraph Way, Madison, Alabama, 35758, USA or

at exportcompliance@intergraph.com. If the Software Customer received is identified on the media as being ITAR-controlled, the Software has been determined to be a defense article subject to the U.S. International Traffic in Arms Regulations ("ITAR"). Export of the Software from the United States must be covered by a license issued by the Directorate of Defense Trade Controls ("DDTC") of the U.S. Department of State or by an ITAR license exemption. The Software may not be resold, diverted, or transferred to any country or any end user, or used in any country or by any end user other than as authorized by the existing license or ITAR exemption. Subject to the terms of the EULA included herein, such Software may be used in other countries or by other end users if prior written approval of DDTC is obtained.

If Customer is located outside the United States, Customer is responsible for complying with any local laws in Customer's jurisdiction which might impact Customer's right to import, export or use the Software, and Customer represents that Customer has complied with any and all regulations or registration procedures required by applicable law related to the use and importation of the Software.

22 Non-Solicitation of Employees.

Customer agrees it will not, without the prior written consent of Hexagon, directly solicit any Hexagon employee, or induce such employee to leave Hexagon's employment, directly or indirectly, during the Term and for a period of twelve (12) Months after the Master Agreement expires or is terminated.

23 Miscellaneous.

23.1 Authority. Each Party represents and certifies to the other Party it has the requisite legal authority to enter into and be bound by the Master Agreement and all Orders arising from the Master Agreement. Any individual purporting to execute or accept a Quote, Primary Contracting Document, or any Order Documents governed by the Master Terms on behalf of a Party represents and warrants to the other Party that such individual has the authority to bind, and does bind, the Party on whose behalf such individual purports to execute or accept such instrument(s). By issuance of a Quote to Customer without the word "DRAFT" or similar markings thereon, Hexagon represents it has the requisite legal authority to enter into and be bound by the Master Agreement and the Order intended to result from the Quote. By executing the Quote and returning it to Hexagon or otherwise entering into an Order, Customer represents and certifies to Hexagon it has the requisite legal authority to enter into and be bound by the Master Agreement and the Order associated therewith.

23.2 Survival. In addition to other provisions that are specifically identified as surviving termination of this Master Agreement, the rights and obligations in sections titled "IP Ownership," "Limitation of Liability," "Dispute Resolution," "Confidential Information," "Export," and the terms of any license or access granted pursuant to the Master Agreement (including, but not limited to, Exhibit A, Exhibit D, Exhibit E, and/or Exhibit F), shall survive and continue after expiration or termination of the Master Agreement, shall remain in effect until fulfilled, and shall apply to any permitted successors and assigns. Upon termination of the Master Agreement, the provisions of the Master Agreement, including those in the preceding sentence, which by their express terms survive termination, shall remain in full force and effect.

23.3 Waiver. The waiver by either Party of any of its rights or remedies in enforcing any action or breach under the Master Agreement in a particular instance shall not be considered as a waiver of the same or different rights, remedies, or actions for breach in subsequent instances.

23.4 Severability. If any provision of the Master Agreement or an Order is void, voidable, unenforceable, or illegal in its terms, but would not be so if it were rewritten to eliminate such terms that were found to be voidable, unenforceable, or illegal and such rewrite would not affect the intent of the provision, then the provision must be rewritten to be enforceable and legal.

23.5 Headings. Numbered topical headings, articles, paragraphs, subparagraphs or titles in the Master Agreement are inserted for the convenience of organization and reference and are not intended to affect the interpretation or construction of the terms thereof.

23.6 Governing Law. The Master Agreement shall for all purposes be construed and enforced under and in accordance with the laws of the State of Texas. The Parties agree any legal action or proceeding relating to the Master Agreement shall be instituted in either State courts located in Williamson County, Texas or the U.S. District Court for the Western District of Texas. The Parties agree to submit to the

jurisdiction of and agree that venue is proper in these courts in any such legal action or proceeding. The Parties waive the application of the United Nations Commission on International Trade Law and United Nations Convention on Contracts for the International Sale of Goods as to the interpretation or enforcement of the Master Agreement.

23.7 Governing Language. The controlling language of the Master Agreement is English. If Customer received a translation of the Master Agreement into another language, it has been provided for convenience only.

23.8 Independent Contractor. The Parties agree that Hexagon is an independent contractor, that nothing in the Master Agreement shall be construed as establishing or implying a relationship of master and servant between the Parties, or any joint venture or partnership between the Parties, and that nothing in the Master Agreement shall be deemed to constitute either of the Parties as the agent of the other Party or authorize either Party to incur any expenses on behalf of the other Party or to commit the other Party in any way whatsoever. Hexagon and its agents, employees, or subcontractors shall at no time be deemed to be agents, employees, or subcontractors of Customer, or be deemed to be under the control or supervision of Customer when carrying out the performance of its obligations in the Master Agreement. Without the prior written consent of Customer, Hexagon shall not carry on any activity that could be construed as being on behalf of Customer.

23.9 Limitation on Claims. Except as otherwise prohibited from applicable law, no claim, regardless of form, arising out of or in connection with the Master Agreement may be brought by Customer more than two (2) years after the event giving rise to the cause of action has occurred or would be reasonably discoverable.

23.10 Anti-Bribery. Each Party hereby certifies it shall comply with all applicable laws in carrying out its duties under the Master Agreement, including, but not limited to, the United States Foreign Corrupt Practices Act ("FCPA"). In particular, Customer, on behalf of itself and its Affiliates, and Hexagon, each severally represent and agree that: such party is familiar with the FCPA and its purposes and agrees to comply with the acts; specifically, such party is aware of and will comply with the FCPA's prohibition of the payment or the gift of any item of value, either directly or indirectly, to an official of a government, political party or party official, candidate for political office, or official of a public international organization, for the purpose of influencing an act or decision in his/her official capacity, or inducing him/her to use his/her influence with the government to assist a company in obtaining or retaining business for, with, or in that country or directing business to any person; such party has not made, and will not make, payments to third parties which such party knows or has reason to know are illegal under the FCPA, or the laws of any applicable jurisdiction; and the method of making payment to Hexagon as provided hereunder is not in violation of the law of any applicable jurisdiction. Either Party has the right to terminate the Master Agreement upon any violation of the FCPA or similar laws by the other Party.

24 Entire Agreement.

The Master Agreement constitutes the entire agreement between the Parties with regard to the subject matter hereof. Except as otherwise provided in the Primary Contracting Document, the Master Agreement supersedes any and all prior discussions and/or representations, whether written or oral, and no reference to prior dealings may be used to in any way modify the expressed understandings of the Master Agreement. The Master Agreement may not be amended or modified unless so done in a writing signed by authorized representatives of both Parties. The pre-printed terms and conditions of Customer's PO or any other terms and conditions of a Customer PO shall be void, even if issued subsequent to the effective date of the Master Agreement, and shall not be deemed to constitute a change to the Master Agreement.

EXHIBIT A

END-USER LICENSE AGREEMENT

IMPORTANT—READ CAREFULLY: This EULA is a legal agreement by and between User and Hexagon. Software is also subject to Use Terms. Any software, including, without limitation, any third party components and/or Updates, associated with a separate end-user license agreement is licensed to User under the terms of that license agreement. Use Terms applicable to an Update shall apply to the Update. All use of the Software is subject to applicable Order Documents.

1.0 LICENSE GRANT. Provided User is not in breach of any term or condition of this EULA, Hexagon hereby grants User a limited, non-exclusive license up to the quantity of Software licenses purchased by User to: (i) install and use the Software, in object code form only; (ii) use, read, and modify Documentation prepared by Hexagon and delivered to User pursuant to the Order Documents; and/or (iii) view and/or use Hexagon audio-visual training materials provided to User pursuant to the Order Documents; provided all of the foregoing shall be strictly for User's internal use and strictly in accordance with this EULA and the applicable Order Documents. The license is non-transferable, except as specifically set forth in this EULA. User assumes full responsibility for the selection of the Software to achieve User's intended results, and for the installation, use and results obtained from the Software.

2.0 UPDATES. If the Software is an Update to a previous version of the Software, User must possess a valid license to such previous version to use the Update. Neither the Software nor any previous version may be used by or transferred to a third party. All Updates are provided to User on a license exchange basis and are subject to all of the terms and conditions of the EULA provided with the Update. By using an Update, User (i) agrees to voluntarily terminate User's right to use any previous version of the Software, except to the extent that the previous version is required to transition to the Update; and (ii) acknowledges and agrees that any obligation that Hexagon may have to support the previous version(s) of the Software will end upon availability of the Update. If an Update is provided, User will take prompt action to install such Update as directed by Hexagon. If User fails to do so, User acknowledges that the Software may not work correctly or that User will not be able to take advantage of all the Software's available features. In such event, Hexagon will not be liable for additional costs User incurs because of User's failure to install such Update. For Third Party Software, please read carefully the applicable Third Party Terms regarding concurrent use of an Update and the prior version of Software during transition to the Update as the Third Party Terms may differ from terms applicable to Hexagon Software Products.

3.0 RIGHTS AND LIMITATIONS.

3.1 **The Following are Permitted for User's License:**

User may make one copy of Software media in machine readable or printed form and solely for backup purposes. Hexagon retains ownership of all User created copies. User may not transfer the rights to a backup copy unless User transfers all rights in the Software and license as provided for in Section 3.2.1 below. Any other copying of the Software, any use of copies exceeding the number of copies User has been authorized to use and has paid for, and any distribution of the Software not expressly permitted by this EULA, is a violation of this EULA and of federal and/or applicable governing law.

3.2 **The Following are Prohibited for User's License:**

3.2.1 User shall not sell, rent, license, lease, lend or otherwise transfer the Software, or any copy, modification, or merged portion thereof without Hexagon's express written consent for such transfer, which consent may not be unreasonably withheld. Any such unauthorized transfer will result in automatic and immediate termination of the license.

3.2.2 The Software is licensed as a single product. User shall not, and User shall not authorize anyone else to: (i) decompile, disassemble, or otherwise reverse engineer the Software; (ii) work around any technical limitations in the Software; (iii) publish the Software for others to copy or use; (iv) use, copy, modify, distribute, disclose, license or transfer the Software, or any copy, modification, or merged portion, in whole or in part, except as expressly provided for in this EULA; (v) re-use the component parts of the Software with a different software product from the one User is licensed to use or on different computers; (vi) circumvent any license mechanism in the Software or the licensing policy; (vii) publish to a third party any results of benchmark tests run on the Software; (viii) use or view the Software for any purposes competitive with those of Hexagon; (ix) use the Software except as expressly set forth in this EULA; and (x) unless otherwise specifically permitted in writing by Hexagon, use the Software outside the country in which it is licensed.

3.3 **Fault Tolerance.**

The Software is not one hundred percent (100%) fault tolerant. Unless the Software's Documentation expressly provides the contrary, the Software is not designed or intended for use in any situation where failure or fault of any kind of the Software could lead to death or serious bodily injury of any person, or to severe physical, property or environmental damage ("High-Risk Use"); and, User is not licensed to use the Software in, or in conjunction with, any High-Risk Use. High-Risk Use is STRICTLY PROHIBITED. High Risk Use includes, for example, the following: operation of aircraft or other modes of human mass transportation, nuclear or chemical facilities, and Class III medical devices. User hereby agrees not to use the Software in, or in connection with, any High-Risk Use. High Risk Use shall not mean use of the Software for purposes for which it is regularly marketed and sold (e.g., public safety and utility dispatch software may be used to dispatch police, fire, emergency medical services, and emergency utility services).

3.4 **Licensing Mechanism Disclaimer.**

Without waiver of any of its rights herein, Hexagon may at its sole discretion provide User who is operating public safety Software a licensing mechanism to allow such Software to be available for use even when User has accessed all of its purchased licenses. Regardless of whether it receives the licensing mechanism, User acknowledges it is permitted to use the Software only up to the number of licenses it has purchased. Any usage of Software beyond the amount purchased by User will be subject to the payment of additional fees by User to Hexagon at then current prices for the Software in like manner as provided in Section 6.2 below (Audit).

4 USER OBLIGATIONS.

4.1 The Software may require User's System to comply with specific minimum software, hardware, and/or Internet connection requirements. The specific minimum software, hardware, and/or Internet connection requirements vary by Software and type of license and are available from Hexagon upon request.

4.2 User is responsible, and bears the sole risk, for backing up all systems, software, applications, and data, as well as properly using the Software.

4.3 At all times, User must keep, reproduce and include all copyright, patent, trademark and attribution notices on any copy, modification or portion of the Software, including, without limitation, when installed, used, checked out, checked in, and/or merged into another program.

4.4 User shall comply with the Use Terms, including limitations that apply to specific types of licenses identified therein.

5 TERM.

5.1 For a Perpetual License, this EULA is effective until terminated (i) by User, by returning to Hexagon the original Software or by permanently destroying the Software, together with all

copies, modifications, and merged portions in any form; (ii) by Hexagon, upon User's breach of any of the terms hereof or User's failure to pay the appropriate license fee(s); or (iii) upon User's installation of an Update that is accompanied by a new license agreement covering the Software Update. User agrees upon the termination of this EULA to cease using and to permanently destroy the Software (and any copies, modifications and merged portions of the Software in any form, and all of the component parts of the Software), and to certify such destruction in writing to Hexagon.

For a Subscription License, this EULA is effective until the User's Subscription Term expires without being renewed; by Hexagon upon User's breach of any of the terms hereof; User's failure to pay the appropriate Subscription License fee(s); or, the Subscription is otherwise terminated. User agrees upon the termination of this EULA or expiration of User's Subscription to cease using and to permanently destroy the Software (and any copies, modifications, and merged portions of the Software in any form, and all of the component parts of the Software), and to certify such destruction in writing to Hexagon.

6 AUDIT.

6.1 Hexagon shall have the right to:

6.1.1 Audit User's use of the Software and User's compliance with the provisions of this EULA during User's normal Business Hours. Hexagon will provide User with thirty (30) days prior written notice of an audit under this Section. Hexagon's right to conduct this type audit shall be limited to twice per calendar year. Prior to the start of an audit, Hexagon's personnel will sign a reasonable non-disclosure agreement provided by User. During the audit, User shall allow Hexagon's personnel to be provided reasonable access to both User's records and personnel.

6.1.2 Obtain certain documentation from User, as follows. If the Software includes logging mechanisms intended to track usage volume or quantity, User shall transmit log files associated therewith to Hexagon upon Hexagon's demand and in accordance with Hexagon's reasonable transmission instructions. Hexagon will not demand the transmission of usage tracking log files more frequently than four (4) times in any calendar year.

6.2 In the event the results of the audit in Section 6.1.1 or the documentation provided by User in Section 6.1.2 indicate User has used unlicensed Software or quantities thereof, User agrees to promptly pay Hexagon: (i) the current list price for each unlicensed Software used by User; and (ii) the costs for the audit in Section 6.1.1.

END OF EXHIBIT A

EXHIBIT B

MAINTENANCE TERMS AND CONDITIONS FOR SOFTWARE

These terms and conditions ("Maintenance Terms") govern the provision of maintenance and support services by Hexagon with respect to Covered Products.

1. DEFINITIONS.

All capitalized terms not otherwise defined herein shall have the meaning set forth in the associated Exhibit titled "Common Terms Glossary."

2. TERM.

2.1. Term. The Maintenance Contract shall begin, retroactively (if applicable), on the first calendar day of the first Month of the Coverage Period and shall expire on the last calendar day of the last Month of the Coverage Period. The Coverage Period shall be for whole Months only.

2.2. Renewal. Prior to expiration of the Coverage Period, Hexagon may submit to Customer a renewal quote with pricing for extension of the Coverage Period. The Parties may extend the Coverage Period pursuant to Order Documents.

2.3. Lapse. In the event of a Lapse: (i) Hexagon shall, at any time, be entitled to discontinue Maintenance Services, in whole or in part, for the affected Covered Products; (ii) Hexagon shall be relieved of any previously provided pricing commitments or options for Maintenance Services, if any, related to time periods following the Lapse; and, (iii) Hexagon may permit Customer to reinstate support for Covered Products pursuant to Hexagon's then current policies and practices, including any policies or practices related to payment of reinstatement fees.

3. SCOPE OF COVERAGE FOR COVERED SOFTWARE PRODUCTS.

Maintenance Services described in this Section apply to Covered Software Products only. Maintenance Services for Covered Third Party Products are separately stated.

Hexagon offers three levels of Maintenance Services for Covered Software Products, dependent upon the Software Product and other factors. Under all levels of Maintenance Service, Hexagon shall provide reasonable commercial efforts to aid in the diagnosis of Defects. Under all levels of Maintenance Services, but only until the subject Software Product version reaches Version Limitation I or Version Limitation II, Hexagon shall provide reasonable commercial efforts to aid in correction of Defects. After a Software Product version reaches Version Limitation I, but only until the subject Software Product reaches Version Limitation II, Hexagon shall provide reasonable commercial efforts to aid in correction of Level One Defects only. The level of Maintenance Services for each Software Product is identified in the Order Documents, subject however to Version Limitations. Defect corrections provided by Hexagon shall, unless otherwise agreed by Hexagon, be delivered within Hexagon's product releases, and in accordance with Hexagon's standardized release cycles. Levels of Maintenance Services are as follows:

3.1. Advantage Support. Advantage Support will include and be limited to the diagnostic and Defect correction support as described above, and the following: Out-of-the-box functionality support via the support help desk (telephone or eService via the Designated Portal; and, access to any available Hexagon problem knowledge base online self-help tool. Phone support is available Monday through Friday from 8AM – 5PM at Customer's local time, excluding Hexagon-observed holidays. Local variances in support hours will be posted online or can be determined by contacting Customer's local Hexagon office.

3.2. Standard Support. Standard Support will include and be limited to the following:
  3.2.1. All features of Advantage Support.
  3.2.2. Access to available Updates of Covered Software Products. Hexagon will notify Customer when Updates are made available for any Covered Software Products for which Maintenance Services have been purchased, by way of posting notices of such to the "Support Notices and Announcements" section on the Designated Portal site , where available, or via direct notification by Hexagon. Updates are shipped to Customer upon Customer's request logged in the Designated Portal site. Hexagon is not obligated to produce any Updates. For avoidance of doubt, a Customer's entitlement to Updates shall not include entitlement to any therein embedded or otherwise related module or function which is licensed and priced separately from Covered Products for which Customer has purchased an entitlement to Updates.

3.3. Premium Support. Premium Support will include all features available under Standard Support (subject to Version Limitations). Additionally, for a Level One Defect, phone support is also available after-hours and on Hexagon-observed holidays.

3.4. Product Change Requests will be reported in like manner as set forth in Section 3.1. Hexagon will review Product Change Requests and at its sole discretion decide whether to make the requested change to the Covered Product(s) through an Update. Product Change Requests not accepted may be the subject of a separate Order between the Parties. For the avoidance of doubt, to the extent Hexagon agrees to make a requested change to a Covered Product pursuant to a Product Change Request, any and all IPR resulting from the Update, including the change or modification is and shall remain the property of Hexagon.

4. MINIMUM SYSTEM REQUIREMENTS; CUSTOMER'S OBLIGATIONS.

Performance of Maintenance Services by Hexagon is specifically conditioned upon the following minimum system requirements and fulfillment by Customer of the following obligations (collectively, minimum system requirements and customer obligations hereinafter referred to as "Customer Obligations"):

4.1. System Requirements. Customer is responsible for ensuring: the System Equipment and network infrastructure meet minimum system requirements specified by Hexagon and made available to Customer upon request; its System Equipment and network infrastructure are adjusted as required to accommodate Updates of Covered Products; compatibility of non-Hexagon provided products with products provided by Hexagon; and, its systems, software, and data are adequately backed up. Hexagon is not liable for lost data.

4.2. Hexagon Access and Customer Cooperation. Customer's system and/or System Equipment must have input and output devices that enable the use of Hexagon's diagnostic programs and supplemental tests. Customer will permit Hexagon to electronically access Customer's system via Secure Access Tool . Customer will ensure availability of its own system technical support personnel so that Hexagon can fulfill its Maintenance Services obligations. When reporting problems to Hexagon's support help desk, Customer will provide a complete problem description, along with all necessary documents and information that is available to Customer and required by Hexagon to diagnose and resolve the problem. Customer will grant all necessary access to all required systems as well as to the Covered Products, and any other reasonable assistance needed. Customer will carry out any reasonable instructions and will install any necessary patches, Defect corrections, or Updates. Customer will appoint a minimum of two and a maximum of five contact people who are each authorized to make use of the Maintenance Services ("Authorized Contacts"). Customer is obligated to select only those personnel for this task who are suitable for it by means of training and function, and who have knowledge of Customer's operating system, network, and hardware and software. Customer agrees to promptly notify Hexagon of any replacement of an Authorized Contact. Customer must ensure Authorized Contacts have adequate expertise, training, and experience to provide professionally accurate descriptions of malfunctions and facilitate Hexagon's efficient response. Authorized Contacts must have successfully completed Hexagon product training, or complete it at the next available scheduled opportunity, for those products for which formal training is available.

Customer will bear the cost of this training. Customer will enter and/or log requests for assistance in such systems, and utilizing such forms, as Hexagon may designate from time to time.

5. EXCLUDED SOFTWARE SERVICES.

Services for the following are outside the scope of the Maintenance Contract and may be available under separate Order at an additional charge (collectively "Excluded Services"):

5.1. Installation of any Covered Product, Update, or interface software;
5.2. Network configuration;
5.3. Configuration or customization of Covered Products to Customer or other third party requirements (except as necessary to remedy a Defect);
5.4. System-level tuning and optimization and system administration support;
5.5. Training;
5.6. Services required because the Authorized Contact is not available or is not trained;
5.7. On-site services (unless waived by Hexagon, in its sole discretion);
5.8. Services required due to modifications of Covered Products by Customer;
5.9. Services required due to use other than in the ordinary manner intended for the Covered Products, or use in a manner that contravenes terms hereunder, or Customer's disregard of the installation and operating instructions according to the Documentation provided with the Covered Products;
5.10. Services required due to failure of software or hardware that is not a Covered Product;
5.11. Services required due to Customer's use of hardware or software that does not meet Hexagon specifications or failure of Customer to maintain or perform industry standard maintenance on Customer's hardware or software;
5.12. Services required due to software or portions thereof that were (i) incorrectly installed or configured (other than by Hexagon), (ii) used in an environment inconsistent with the support environment specified by Hexagon, and/or (iii) used with peripherals, operational equipment or accessories not conforming to Hexagon's specifications;
5.13. Services required due to cases of force majeure, especially lightning strikes, fire or flood, third-party criminal acts, or other events not caused through Hexagon's fault;
5.14. Services required due to Customer's failure to fulfill the Customer Obligations; and/or
5.15. Services required due to faulty or incomplete Customer data.

6. COVERED THIRD PARTY PRODUCTS.

Support and Updates of Covered Third Party Products shall be provided in the fashion and to the extent or duration that Hexagon is authorized to provide such by the third party manufacturer of the Covered Third Party Products, and such Covered Third Party Products and related services may be subject to additional terms and conditions of the third party manufacturer of the Third Party Software.

Services and updates for any Third Party Software not listed in the Order Documents as Covered Products must be obtained from the third party owner of the products or their designated representative.

7. REQUIRED COVERAGE.

7.1. Multiple or Interdependent Licenses. If Customer holds multiple licenses for any Covered Product, all held licenses must be included as Covered Products in the Maintenance Contract.
7.2. Prerequisite Licenses. All prerequisite licenses for Software Products necessary to operate the Covered Products, together with all licenses of Software Products interoperating with Covered Products in a single solution, must be included as Covered Products in the Maintenance Contract.

8. ADDITIONS AND REMOVALS OF COVERED PRODUCTS.

8.1. Additions of Covered Products. Software Products licensed from Hexagon during the term of the Maintenance Contract may be added as Covered Products, if such addition is addressed through additional related Order Documents. If Software Products are not added as Covered Products by commencement of Production use thereof, Hexagon may permit Customer to add them as Covered Products, but subject to additional fees payable pursuant to Hexagon's then current policies or practices.

8.2. Removal of Covered Products from Maintenance. Either Party may provide written notice to the other Party at least sixty (60) calendar days prior to the end of any Coverage Period Anniversary of its intent to remove any individual Covered Products from the Maintenance Contract at the end of the then current and contracted Coverage Period or any Coverage Period Anniversary. Neither Party may remove Covered Products except upon Coverage Period renewal or extension or Coverage Period Anniversary; provided that Hexagon may additionally remove Covered Products as part of a general discontinuance program at any time upon one hundred eighty (180) days' written notice. Customer may not remove from the Maintenance Contract individual software licenses of a Covered Product for which Customer has multiple copies under Maintenance Services or for Covered Products that are being used interdependently, unless Customer has first certified to Hexagon on a "Software Relinquishment Agreement" that it surrenders and relinquishes all rights in and to the applicable Software licenses and the copies of the Covered Product for which Customer desires to cease Maintenance Services (the "Relinquished Licenses") for the renewal Coverage Period have been uninstalled and removed from its System(s). Should Customer desire to resume usage of the Relinquished Licenses at a later date, Customer must re-purchase the licenses at the then current list price.

9. PAYMENT.

9.1. Terms of Payment. Charges for Maintenance Services are due and payable in accordance with Chapter 2251 of the Texas Government Code. Charges for Covered Software Products added during a Coverage Period shall be prorated to the remaining Months of the Coverage Period, in whole Month increments only. Covered Third Party Products added during a Coverage Period are subject to Section 6 of these Maintenance Terms.

9.2. Past Due Accounts. HEXAGON RESERVES THE RIGHT TO REFUSE SERVICE TO ANY CUSTOMER WHOSE ACCOUNT IS PAST DUE. At the discretion of Hexagon, Customers who have not paid any charges when due (i) under the Maintenance Contract, (ii) under any other agreement between the Parties, or (iii) under any agreement between Hexagon and Customer's parent and/or subsidiary, may not be rendered Maintenance Services until all past due charges are paid in full. The start of the Coverage Period shall not be postponed due to delayed payment of any charges.

9.3. Customer's Responsibilities Concerning Invoice Questions. Subject to applicable law, if Customer intends to dispute a charge or request a credit, Customer must contact Hexagon within thirty (30) calendar days of the date on the invoice. Customer waives any right to dispute a charge or receive a credit for a charge for Maintenance Services that Customer does not report within such period.

10. CUSTOMER ACKNOWLEDGEMENTS.

During the Coverage Period, Customer commits to the following:

10.1. Customer shall have reviewed the Order Documents and by executing the Order Documents confirms the Order Documents accurately reflects all Hexagon software in its possession or control.

10.2. Customer acknowledges and confirms that for all Covered Products supported under the Maintenance Contract, all licenses of a Covered Product for which Customer has multiple copies

in its possession and all prerequisite licenses necessary to operate Covered Products, are accounted for in the Order Documents. If all like Covered Products or prerequisite software licenses are not accounted for in the Order Documents, Customer agrees to notify Hexagon so that Hexagon may issue a revised Quote to Customer.

10.3. Customer acknowledges and confirms Maintenance Services provided herein shall be utilized only for the quantity of Covered Products licenses listed in the Order Documents.

11. ADDITIONAL TERMS.

11.1. Pass-Through Third Party Warranties. Covered Third Party Products are only warranted pursuant to a pass-through warranty to Customer from the applicable Third Party Software manufacturer and only to the extent warranted by the applicable Third Party Software manufacturer.

11.2. Remedies. In the event a warranted Maintenance Service, Covered Product, or Update provided pursuant to the Maintenance Contract does not substantially comply with the limited warranties set forth in the Maintenance Contract, Hexagon's entire liability and Customer's remedy shall be, in addition to those remedies legally available, in Hexagon's sole and absolute discretion, either (i) providing of a Service, Covered Product, or Update which conforms substantially with the warranty; or (ii) a refund of the purchase price of the particular warranted Service, Covered Product, or Update for the period of time that the warranted Service, Covered Product, or Update did not substantially conform to the limited warranties set forth in the Maintenance Contract. Hexagon is acting on behalf of its suppliers for the sole purpose of disclaiming, excluding and/or limiting obligations and liability as provided in the Maintenance Contract, but in no other respects and for no other purpose.

11.3. WARRANTY DISCLAIMERS. In addition to the Warranty Disclaimer provided in the Master Terms, Hexagon does not warrant that any Services, Covered Products, and Updates provided pursuant to the Maintenance Contract will meet Customer's requirements, and under no circumstances does Hexagon warrant that any Services, Covered Products, and Updates will operate uninterrupted or error or Defect free.

11.4. Third Party Providers. Hexagon reserves the right to provide Maintenance Services through a third party provider.

END OF EXHIBIT B

EXHIBIT C

PROJECT DELIVERABLE SIGN-OFF FORM

CUSTOMER NAME, CUSTOMER CITY – PROJECT NAME

Submission Date:	Month/Day/Year	Sign-Off Target Date:	Month/Day/year
Submitted By:	Hexagon Contact Name	Submitted To:	Customer Contact Name
Customer Contract #:	Customer Contract Number	Customer/Project #:	Hexagon Project Number

TYPE OF DELIVERABLE

☐ SOW Tasks ☐ Payments ☐ Plans/Designs ☐ Training ☐ Other

DELIVERABLE INFORMATION

DELIVERABLE DESCRIPTION THIS SECTION DESCRIBES THE DELIVERABLE	$AMOUNT OF PYMT (If applicable)

With the deliverable described above complete, the Customer shall have ten (10) Business Days after receipt of a written request from Hexagon, to either sign-off that the Task Acceptance Criteria has been satisfied or state in writing to Hexagon the reason the Task Acceptance Criteria has not been satisfied.

Sign-off of the Task shall be based solely upon satisfaction of the Task Acceptance Criteria stated in the Contract between Hexagon and CUSTOMER NAME dated Month/Day/Year and shall be indicated by the Customer signing the Project Deliverable Sign-off Form. If the Customer does not provide such sign-off or rejection within the ten (10) Business Days after delivery then the Task will be deemed to have been accepted.

The signature below acknowledges that Task Acceptance Criteria described in the Statement of Work and listed above has been satisfied and the Task is accepted.

Authorized Customer Representative
Customer Contact Name

_____ _____

SIGNATURE **DATE**

END OF EXHIBIT C

EXHIBIT D

CLOUD PROGRAM CONDITIONS

These terms and conditions ("Cloud Conditions") govern the provision of the Cloud Program by Hexagon to Customer under a Cloud Program Order. Any additional terms in any Cloud Services Schedule(s) also apply.

1. DEFINITIONS.

Capitalized terms used and not otherwise defined herein have the meanings assigned in the Common Terms Glossary.

2. SCOPE OF CLOUD PROGRAM.

2.1 From the Cloud Program Start Date and for the duration of the Cloud Term, Hexagon will provide the License Key(s) to Customer in the amount specified in the Quote with respect to the Cloud Program purchased by Customer to use the Cloud Program subject to the provisions of these Cloud Conditions. Except for the Cloud Services, no other service, including Cloud Consulting Services, are provided by Hexagon pursuant to a Cloud Program Sales Order.

2.2 Hexagon may from time to time provide or otherwise make available Local Software. Local Software may include mobile applications obtainable from an online applications store, applications owned by a third-party, or other facilitating applications. In the event Hexagon provides or makes available such applications, the same shall be made available to Customer and owned by Hexagon (or the relevant third party) and used subject to these Cloud Conditions. If not sooner terminated, the license to use such Local Software shall terminate upon expiration of the Cloud Term.

3. CLOUD SERVICES AUTHORIZATION.

During the Cloud Term, Hexagon grants Customer and its Affiliates the right to access and use components of the Cloud Program listed in the quantities reflected on the Quote solely for Customer's and Affiliates' own internal business purposes and subject to these Cloud Conditions.

4. TERM, TERMINATION AND SUSPENSION.

4.1 The Cloud Program Order commences on the Effective Date of the Order and shall continue for the Cloud Term, unless earlier terminated in accordance with the Master Terms and these Cloud Conditions. To the extent any optional renewals are identified in the Quote, the Customer must issue a PO or a notice to proceed to extend the Cloud Term and at the prices set forth in the Quote not less than sixty (60) days prior to the end of the Cloud Term. Prior to the end of the Cloud Term, the Customer may renew the Cloud Program Order and/or have Customer Data Offboarded.

4.2 In addition to the rights and remedies set forth in the Master Terms, once notified in writing of an overdue payment, Customer acknowledges Hexagon may, without further notice, reduce the Cloud Services to the lowest tier of Cloud Services offered by Hexagon. During such time, Hexagon or the Third Party Service Provider is not obligated to facilitate or provide any services related to Onboarding or Offboarding. Without waiver of its right to terminate the Master Agreement and/or Cloud Program Order or seek additional remedies, if full payment has not been received by Hexagon within thirty (30) days following written notice, Hexagon may suspend providing the Cloud Program to Customer until all outstanding Cloud Program Fees together with any applicable interest has been paid to and received by Hexagon. Suspension of the Cloud

Program for non-payment shall not prejudice Hexagon's rights hereunder or relieve Customer from the obligation to pay Cloud Program Fees associated with the period of suspension.

4.3 Termination shall not relieve the Customer of the obligation to pay any Cloud Program Fees accrued or payable to Hexagon prior to the date of termination. Unless otherwise agreed to in writing by Hexagon, in the event Hexagon terminates a Cloud Program Order due to any of the conditions set forth in Section 4.2 above, then under no circumstances whatsoever shall Customer be entitled to any refund of Cloud Program Fees paid in advance to Hexagon pursuant to the terms of the Master Agreement.

5. AVAILABILITY. Hexagon shall reasonably endeavor to deliver Availability in accordance with the Service Level specified in the applicable Cloud Services Schedule. "**Availability**" or "**Available**" means the ability to connect to the Cloud Portal, connect to the Customer Cloud Environment for Production, launch Cloud Application(s), and access Customer Data contained in the Customer Cloud Environment for Production. Availability does not include the availability of third-party portals or Cloud Optional Services. Availability of Cloud Application(s) shall be determined by launching the main application for the applicable Cloud Application. For purposes of calculating Availability time, the following is excluded: time expended for Planned Maintenance; downtime required to perform Cloud Consulting Services; time expended due to the inability for Customer to connect to the Cloud Portal due to problems with the Customer's infrastructure or the internet; unavailability arising from Customer exceeding Customer purchased Cloud Application capacity; and, time expended due to any other circumstances beyond Hexagon's reasonable control, including Customer's or any User's use of third-party materials or use of the Cloud Program other than in compliance with the express terms of the Master Agreement and Hexagon's reasonable instructions (collectively "**Exception(s)**").

6. CRITICAL SERVICE LEVELS. The purchased Service Level classifications are set forth in the Cloud Service Schedule. "**Service Operational Time**" means the time, expressed in a percentage as set forth below, that the Cloud Application is Available for a given Month during the service. The method of calculating the Service Operational Time is:

$$\frac{\textit{Hours of Cloud Program Availability for a given Month}}{\textit{Hours of Cloud Program Availability + downtime hours for such Month which are not related to an Exception}} \times 100$$

7. SERVICE CREDITS.

7.1 If in any Month the Service Operational Time in a Cloud Environment for Production falls below the purchased Service Level (a "**Service Incident**"), a "Return to Green Plan" shall be initiated for the Customer's Production Environment. Hexagon shall have: (i) the remainder of the Month in which the Customer notified Hexagon of the Service Incident by way of a Cloud Service Request, which notified Hexagon of the problem which resulted in the Service Operational Time falling below the applicable Service Level, *plus* (ii) one (1) additional Month (collectively, the "**Go Green Period**"), to return the Service Operational Time to such Service Level.

7.2 Subject to Section 7.3 below, if the Service Operational Time does not rise to the applicable Service Level within the Go Green Period, then the Service Credit provided in the Cloud Service Schedule will be applied against each Month in which the Service Operational Time remains below such Service Level.

7.3 Service Credits apply:

7.3.1 Only as specified within the applicable Cloud Services Schedule;

7.3.2 Only to the extent that the affected Customer Environment is used in Production;

7.3.3 In strict accordance with Section 5;

7.3.4 Only if a Customer has logged a Cloud Service Request which notified Hexagon of the problem that causes the Critical Service Level to fall below the identified Availability percentage in the applicable Cloud Services Schedule ("Green"); and

7.3.5 Only where Customer is compliant with the AUP.

7.4 To the extent applicable and properly noticed by Customer in accordance with Section 7.1 above, Service Credits shall be credited against the next invoice until such applicable Service Credits have been used. If the Master Agreement is terminated or Customer elects not to renew the Master Agreement before an ensuing invoice is issued, then such Service Credits are forfeited. Customer shall have no right to receive any monetary remuneration in exchange for unused Service Credits. Notwithstanding anything herein to the contrary, in no event shall Service Credits for any given year during the Cloud Term exceed twenty percent (20%) of the amount of Cloud Program Fees payable by Customer to Hexagon pursuant to the Quote for the annual period in which the Service Credit accrued.

7.5 The Customer's exclusive remedy for not meeting the Critical Service Level specified in the applicable Cloud Services Schedule shall be the Service Credits as set forth in this Section.

8. CLOUD SERVICES SUPPORT.

8.1 As part of Cloud Services, Hexagon will provide the Cloud Services Support described within this Section 8.

8.2 Cloud Services Support is available at the times specified in the applicable Cloud Services Schedule. Cloud Service Requests and Product Change Requests can be directed by an Authorized Cloud User to Hexagon by: (i) the Designated PortalWe, or (ii) telephoning Hexagon support at the times permitted within the Cloud Services Schedule.

8.3 When reporting a Cloud Service Request, if an Error, an Authorized Cloud User shall assign the Cloud Service Request a priority level based upon the criteria set forth in the Designated Portal . The Authorized Cloud User shall provide a brief justification as to the criticality of the Cloud Service Request and a description of the Error giving rise to the Cloud Service Request, to include a statement of steps necessary to produce the Error. Hexagon shall respond to the Cloud Service Request and provide commercially reasonable efforts to aid and address the Cloud Service Request. If Hexagon disagrees with the priority of the Cloud Service Request, it shall discuss the matter with Customer, but Hexagon, in its sole discretion, reserves the right to revise the initially reported priority level of the Cloud Service Request.

8.4 Product Change Requests will be reported in like manner as set forth in Section 8.3. Hexagon will review Product Change Requests and at its sole discretion decide whether to make the requested change to the Cloud Program. Product Change Requests not accepted may be the subject of a separate contract between the Parties. For the avoidance of doubt, to the extent Hexagon agrees to make a requested change to the Cloud Program pursuant to a Product Change Request, any and all IPR resulting from such change or modification is and shall remain the property of Hexagon.

8.5 Customer acknowledges and agrees that, as part of providing Cloud Services Support, Hexagon is permitted to make necessary changes to the Cloud Program, without notice if necessary, to perform Emergency Maintenance. Hexagon shall be permitted to access the Customer Cloud Environment in the event Hexagon deems Emergency Maintenance is necessary.

8.6 As it relates to, and only to, Local Software which is listed on the Quote, Hexagon shall provide support in like manner as is provided for Cloud Applications except Customer will permit Hexagon to electronically access the Local Software in the Local Environment via Secure Access Tool. Support for Local Software listed on the Quote is included within Cloud Services Support except as is otherwise rendered commercially unreasonable due to the Local Software being hosted by Customer.

8.7 Except as otherwise necessary, as determined by Hexagon in its sole discretion, to satisfy the requirements of Sections 8.3 and 8.4, Cloud Services Support does not include: (i) training; (ii) configuration of Cloud Application(s), Cloud Optional Services, Cloud Portal, Third Party Software Products, Software Products, or other components of the Cloud Program; (iii) Customer Cloud Administration; (iv) programming or software development; (v) modifications to the Cloud Applications or Cloud Optional Services not accepted as a Product Change Request; (vi) onsite services; or (vii) services required because Customer has not performed its obligations under the Master Agreement.

8.8 Updates.

8.8.1 As part of Cloud Services Support, Customer is entitled to receive all Updates to the purchased Cloud Application(s) and Local Software that Hexagon makes available. Cloud Consulting Services may be necessary to Update Cloud Optional Services, which is not part of Cloud Services Support.

8.8.2 From time to time, Hexagon may notify Customer through the Designated Portal that Hexagon has developed an Update for the purchased Cloud Application(s) and intends to deploy said update, including any applicable Third Party Software Products. On the date specified in the notification, Hexagon will deploy the Update to the Cloud Development Environment for Customer testing and review, which Customer shall complete within the time prescribed in the notification of the availability of the Update, but not less than thirty (30) days thereafter (the "Testing Period"). In the event no Material Adverse Effect is reported by Customer within the Testing Period, then on a subsequently specified date by Hexagon, Hexagon will, at its discretion, deploy the update to Customer Cloud Environment for Production.

8.8.3 In the event Customer provides written notice to Hexagon, within the Testing Period, of a Material Adverse Effect as a result of Customer's testing of the Update in accordance with Section 8.8.2 above, Hexagon shall discuss the matter with Customer and use commercially reasonable efforts to address any reasonable workarounds to such Material Adverse Effect, such agreed upon workaround to be subject to the same protocols set forth in Section 8.8.2 and this Section 8.8.3; provided, however, if Hexagon reasonably finds that no Material Adverse Effect exists, Hexagon may deploy the Update to the Customer Cloud Environment for Production.

8.8.4 As it relates to implementing Updates for Local Software that is included within the Cloud Program, Customer shall permit Hexagon to electronically access the Local Software on Customer's System Equipment via Secure Access Tool to implement the Update in conjunction with the updating of the Cloud Applications and provide any other reasonable support and cooperation required by Hexagon to update the Cloud Program.

9. CUSTOMER RESPONSIBILITIES.

9.1 Customer shall be responsible for all activities that occur in Authorized Cloud Users' and Users' accounts, including, but not limited to, its Affiliates' accounts, and for Authorized Cloud Users' and Users' compliance with the Master Agreement. Customer shall:

9.1.1 Have sole responsibility for the accuracy, quality, integrity, reliability and appropriateness of all Customer Data that is placed into the Customer Cloud Environment;

9.1.2 Use commercially reasonable efforts to prevent unauthorized access to or use of Cloud Program, including preventing utilization of more Credentials than otherwise reflected by the License Key(s) set forth in the Quote, and notify Hexagon of any such unauthorized access or use;

9.1.3 Provide and maintain its own System Equipment, third party software, networks, internet access, and communication lines, including any public lines required to properly access the Cloud Portal and use the Local Software, including content or data and ensure such meet the minimum standards required to interoperate with the Cloud Program as communicated by Hexagon to Customer via the Cloud Portal or as otherwise determined by Hexagon; and

9.1.4 Abide by and comply with the Acceptable Use Policy, Documentation, and other requirements of these Cloud Conditions.

9.2 Customer shall reasonably cooperate with Hexagon as it pertains to Planned Maintenance.

10. CLOUD SERVICE PROGRAM FEES.

10.1 Generally. Subject to Section 10.2 below, in consideration of the Cloud Program provided by Hexagon, Customer shall pay to Hexagon the Cloud Program Fees.

10.2 Adjustment. It is the Customer's responsibility to monitor its usage of License Key(s) and/or Cloud Application capacity it has purchased. Hexagon may periodically review the Customer's usage of the Cloud Program to determine whether Customer's usage is consistent with the quantity of License Key(s) and/or Cloud Application capacity purchased. If the usage shows the Customer has used more License Key(s) than are specified in the Quote, then Customer shall pay Cloud Program Fees corresponding to the number of License Key(s) used in excess of the purchased quantity. If a Cloud Application is subject to capacity limitations (e.g. a limited number of transactions in a period), as expressly set forth in the applicable Cloud Services Schedule, the Cloud Application may be configured to cease or degrade some or all functions upon Customer reaching those capacity limitations and/or may be configured to permit additional usage for additional fees, all as and if described in the applicable Cloud Services Schedule(s).

11. TERMS OF PAYMENT.

The invoice corresponding to the first year of Cloud Program Fees shall be provided to Customer upon Hexagon's issuance of License Key(s) to Customer. For purposes of clarity, once the first License Key(s) is issued for any Cloud Environment, the annual Cloud Program Fee will be due and payable according to Chapter 2251 of the Texas Government Code. Invoices for subsequent years included within the Cloud Term as specified in the Quote (as may be adjusted pursuant to Section 10.2 above) will be issued prior to the Cloud Anniversary.

12. ACCEPTABLE USE POLICY (AUP).

12.1 The AUP forms part of these Cloud Conditions and is incorporated by reference. It may be found at the following site: https://www.hexagonsafetyinfrastructure.com/-/media/Legal/Hexagon/SI/Policies/AUP/Cloud_AUP-L.pdf. The Customer and any Authorized Cloud User or User shall comply with the AUP. A User or Authorized Cloud User will be prompted with review and acceptance of the AUP to gain access to the Cloud Application(s). Any update to the AUP will require each User or Authorized Cloud User to re-accept the modified AUP. Failure to comply with the AUP may result in the suspension of the Cloud Program or termination of the Cloud Program Order as provided in Section 5 of the Master Terms. During any period of suspension, the Customer will still be liable for payment of the applicable Cloud Program Fees.

12.2 Hexagon reserves the right to change the AUP at any time, but to the extent within the control of Hexagon, it will give Customer thirty (30) days' notice in accordance with the Master Terms and the Primary Contracting Document of any such changes by posting notice of the upcoming change in the AUP on the Cloud Portal or as otherwise determined by Hexagon, unless otherwise required by law or where a Third Party Service Provider requires a change to be made to the AUP and is unable to provide such period of notice. If a Third Party Service Provider requires a change to be made to the AUP, Hexagon shall provide the equivalent period of notice as is provided by the Third Party Service Provider to Hexagon.

12.3 Without waiver of any other requirement or limitation set forth herein, Customer's use of any third party software in conjunction with the Cloud Application, Cloud Optional Services, and Hexagon Software Products that is not certified by Hexagon to operate in conjunction with the same is

solely at Customer's risk. Addressing service requests arising from the use of uncertified third party software is not included within Cloud Services Support or the Cloud Program.

13. OWNERSHIP AND INTELLECTUAL PROPERTY.

13.1 In accordance with Section 6 of the Master Terms, Hexagon owns all right, title and interest in and to Cloud Application(s), Cloud Optional Services, the Software Products, Local Software, Documentation written by Hexagon, and any other data and information provided as part of the Cloud Program (except for data and information being owned by a third party), and all copies of all or any part thereof, are and shall remain vested in Hexagon. Third parties shall retain any and all IPR in and to their intellectual property that may be provided as part of the Cloud Program. Customer and its Affiliates do not have, and shall not attempt to decompile, disassemble, or otherwise attempt to gain access to any source code for the Cloud Application, Cloud Optional Services, any other Hexagon Software Product, or Third Party Software . Customer, for itself and its Affiliates acknowledges and agrees the Cloud Program is comprised of trade secrets, proprietary information, and Confidential Information, and that Customer, and its Affiliates shall not use, distribute, copy, perform, amend, alter, modify, create derivative works, reverse engineer, exploit, sublicense, or assign the Cloud Program or any component thereof except as expressly permitted by Hexagon (which permission may in some instances, subject to stated limitations, be contained in a Cloud Services Schedule with respect to a particular Cloud Application). Without Hexagon's express, written permission, Customer shall ensure that no User transfers or assigns any Credentials to any other person or entity that is not an employee of Customer.

13.2 Customer and its Affiliates, respectively, shall retain their respective full ownership and all rights associated therewith solely to Customer Data to the extent they own IPR to said information, as well as work product input or output generated by the Cloud Program. This ownership shall not extend to any formats or other Intellectual Property provided by Hexagon under the Master Agreement that makes a particular data file intelligent or that structures output, said formats and Intellectual Property which shall remain the property of Hexagon or the respective third party that owns said format or Intellectual Property.

14 PERSONAL DATA.

14.1 Hexagon reserves the right, but does not assume the obligation, to investigate any violation of this Exhibit D (Cloud Program Conditions) and/or AUP or misuse of the Cloud Services or Cloud Program. Hexagon may: (a) investigate violations of this Exhibit D (Cloud Program Conditions) and/or AUP or misuse of the Cloud Services or Cloud Program; and (b) remove, disable access to, or modify any content or resource that violates this Exhibit D (Cloud Program Conditions) and/or AUP. Hexagon may report any activity that Hexagon suspects violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Hexagon's reporting may include disclosing appropriate information related to Customer or any User. Hexagon also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this Exhibit D (Cloud Program Conditions) and/or AUP.

14.2 Unless Customer Specified Data Center(s) are included in the Cloud Services as identified in the Quote, Hexagon and its Third Party Service Provider shall have sole discretion of the location of the Data Center(s).

15 SECURITY & BREACH NOTIFICATION.

15.1 Hexagon shall take reasonable industry action to prevent, detect, identify, report, track and respond to Security Incidents.

15.2 Hexagon Response to Security Incident. In the event of a Security Incident, Hexagon will provide a Security Incident report to the Customer or its Affiliates (as applicable) via the Designated Portal, or otherwise. The report shall be provided within twenty-four (24) Business Hours following Hexagon's discovery, confirmation, and investigation of a Security Incident.

15.3 Additional Requirements for Personal Data. With respect to any Personal Data in the possession or under the control of Hexagon, which does not include Customer Data within the Customer Cloud Environment, and in order to protect Personal Data from unauthorized access, destruction, use, modification or disclosure, Hexagon shall:

15.3.1 Develop, implement, and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Personal Data from unauthorized access, destruction, use, modification, or disclosure; and

15.3.2 Develop, implement, and maintain data privacy and security programs with administrative, technical, and physical safeguards appropriate to the size and complexity of Hexagon's business and the nature and scope of Hexagon's activities to protect Personal Data from unauthorized access, destruction, use, modification, or disclosure.

16 WARRANTIES, DISCLAIMER AND INDEMNITIES.

16.1 During the Cloud Term, Hexagon does not warrant the Cloud Application(s) purchased by Customer will meet the Service Level specified in the applicable Cloud Services Schedule. The Cloud Program may be subject to limitations, delays and other problems inherent in the use of the internet, electronic communications, and Customers' IT infrastructures. Hexagon will not be responsible for any delays, delivery failures, or other damage.

16.2 Hexagon does not warrant the Cloud Application(s) and Third Party Software accessed via Cloud Services will perform substantially in accordance with the Documentation provided. To the extent an Error should be discovered, Customer shall report such Error to Hexagon as provided in Section 8 of the Cloud Program Conditions and Hexagon will respond as provided therein.

16.3 Cloud Services will use industry standard Virus detection software to avoid transmission to the Customer and its Affiliates any Viruses (except for any Viruses contained in Customer Data uploaded or Onboarded by Customer).

16.4 The warranties set forth herein are in lieu of all other warranties, expressed or implied, and represents the full and total warranty obligation and/or liability of Hexagon

17 ACCESS TO THE MASTER AGREEMENT BY CUSTOMER'S AFFILIATES.

If Customer's Affiliate accesses or utilizes any or all components of the Cloud Program, the Affiliate shall be deemed to have agreed to be bound by the terms and conditions of these Cloud Program Conditions. The Affiliate, in accessing the Cloud Program (or any part thereof), and Customer, in permitting the Affiliate's access, each represent to Hexagon they have entered into an agreement by which Affiliate is permitted to use the Cloud Program and is bound to the terms herein. Except for Affiliates and employees of Affiliates, no other person, including any third parties not authorized by Hexagon, may access the Cloud Program or be provided with Credentials.

END OF EXHIBIT D

EXHIBIT E

SUBSCRIPTION TERMS AND CONDITIONS

These Subscription Terms and Conditions ("Subscription Terms") govern the licensing and support for the Subscription.

1. DEFINITIONS. All capitalized terms not otherwise defined herein shall have the meaning set forth in Exhibit G (Common Terms Glossary).

2. SERVICES PROVIDED.

2.1 Access. Subject to an Order and these Master Terms, including Exhibit A (End User License Agreement), Hexagon will make the Subscription Licenses available to Customer for Customer's use during the Subscription Term. Any renewal or extension of the Subscription Term shall be subject to such terms and product components as reflected in the applicable renewal or extension Quote issued by Hexagon (the "***Renewal Quote***"). Customer acknowledges and agrees that Customer shall compensate Hexagon for Customer's continued use of a Subscription after expiration or termination of a Subscription Term, at a rate equitably and proportionately calculated based upon the Renewal Quote and based upon the period of such extended use; *provided that* if no Renewal Quote is issued prior to expiration or termination of the Subscription Term, the initial Quote shall be substituted in the calculations set forth in this Section 2.1.

2.1.1 As it pertains to Metered Licenses, the Customer's right to use the Metered Licenses shall end upon the earlier of: (i) expiration of the Subscription Term, or (ii) Customer's use of its allotment of units of service as set forth in the Quote.

2.2 Maintenance and Support. During the applicable Subscription Term, Hexagon will provide maintenance services and support to the Customer for the Subscription Licenses in accordance with Exhibit B (Maintenance Terms and Conditions) of these Master Terms.

2.3 Services. These Subscription Terms only provide for the licensing and support of the Subscription. If the Customer desires for Hexagon to provide Services for implementation, configuration, training, or other work in relation to the Subscription, then Customer may contract with Hexagon pursuant to these Master Terms for Services.

3. INVOICES. Hexagon shall invoice Customer for the full amount set forth in the Quote upon delivery of or access having been provided for any of the Subscription Licenses identified in the Quote. To the extent the Quote includes multiple types of Subscription Licenses, Hexagon shall invoice the Customer when the first type of Subscription License is allowed to be invoiced as provided in this section.

4. CUSTOMER OBLIGATIONS.

4.1 Customer Control. Customer and its authorized Users of the Subscription shall at all times comply with Exhibit A (End User License Agreement). Customer will be solely responsible for administering and monitoring the use of login IDs and passwords provided by Customer to authorized Users pursuant to the Subscription, or by Hexagon on behalf of Customer. Upon the termination of employment of any authorized User, Customer will terminate that individual's login ID and password. Hexagon is not responsible for any damages resulting from Customer's failure to manage the confidentiality of its login ID and passwords and Customer is responsible for any actions arising out of use or misuse of Customer's login IDs.

4.2 Security. Customer shall take commercially reasonable security precautions to prevent unauthorized or fraudulent use of Hexagon IP by Customer, Customer's employees, consultants, agents, or any other third parties authorized by Customer to access the Subscription on Customer's behalf.

END OF EXHIBIT E

EXHIBIT F

COTS Training Program Terms

These terms and conditions ("COTS Training Program Terms") govern the provision of the Training Curricula by Hexagon to Customer under a Fixed Price Project Assignment. Any additional terms in a Training Program Statement also apply; and, notwithstanding the order of precedence stated in the Master Terms, but without otherwise modifying such order of precedence, any conflict between these COTS Training Program Terms and any applicable Training Program Statement shall be resolved in favor of the Training Program Statement.

1. DEFINITIONS.

Capitalized terms used and not otherwise defined herein have the meanings assigned in the Common Terms Glossary.

2. SCOPE OF TRAINING PROGRAM.

Hexagon will provide the Training Curricula specified in the Quote and purchased by Customer, in accordance with and subject to the provisions of these COTS Training Program Terms and the applicable Training Program Statement(s). The Training Program Statements(s) and Quote shall describe the duration and delivery method for the Training Curricula; provided that if no duration is otherwise stated for a Training Curricula delivered by online means, Customer shall cease use thereof twelve (12) months following the date the Order was placed for the Training Curricula.

3. FEES AND PAYMENT.

Unless otherwise expressly provided in applicable Training Program Statement(s) corresponding to the Order, fees for Training Curricula delivered by a live instruction method shall be invoiced as and when the Training Curricula is delivered; and fees for Training Curricula delivered by an online on-demand method shall be invoiced upon first delivery to Customer of the initial ability to access any portion of the Training Curricula.

4. SPECIFIC ONLINE TERMS.

4.1 Assignment of Credentials. For Training Curricula delivered by an online on-demand method, Customer acknowledges and agrees that: each specific student/user must be assigned individual credentials, thereby consuming one of the overall quantity of credentials available to Customer under the terms of the Order, and student/user credentials may not be shared or used by more than one student/user. Upon request, and subject to processing and any requirements of the Third Party Service Provider, credentials may be subject to reassignment to a new student/user and from a student/user no longer requiring access to the Training Curricula. The period of availability of an online on-demand Training Curricula shall not be extended due to delays in Customer's assignment of available credentials or in any reassignment of credentials.

4.2 Use Restrictions. Customer shall comply, and assure all students/users comply, with terms of use of the Training Curricula and the platform through which it is provided, including without limitation, each of the following: the platform and assets associated therewith shall never be used to perform unlawful activity or activity which interferes with networks, systems, or facilities associated with operation of the platform; the platform shall not be used to store, process, or publish threatening, disparaging, or offensive material, or material that constitutes Spam/E-Mail/Usenet abuse or to create a security risk or an infringement of privacy or IPR; the platform shall not be used for any activity intended to directly or indirectly circumvent security measures of the Third Party Service Provider or Hexagon; and, the platform shall be used solely within the use requirements of the Third Party Service Provider and solely for the purpose of consuming the Training Curricula.

5. OWNERSHIP AND INTELLECTUAL PROPERTY.

In accordance with Section 6 of the Master Terms, Hexagon owns all right, title and interest in and to Training Curricula, and any other data and information provided as part of Training Curricula (except for data and information being owned by a third party), and all copies of all or any part thereof, are and shall remain vested in Hexagon. Third parties shall retain any and all IPR in and to their intellectual property that may be provided as part of the Training Curricula, to include without limitation the Third Party Service Provider's retention of intellectual property associated with the platform through which any online on-demand Training Curricula is provided. Customer and its Affiliates shall not attempt to decompile, disassemble, obtain any source code for, or record Training Curricula, in whole or in part. Customer, for itself and its Affiliates and their respective personnel accessing the Training Curricula, acknowledges and agrees the Training Curricula is comprised of trade secrets, proprietary information, and Confidential Information, and that Customer, and its Affiliates shall not use, distribute, copy, record, perform, amend, alter, modify, create derivative works, reverse engineer, exploit, sublicense, or assign the Training Curricula or any component thereof except as expressly permitted by Hexagon. The Customer acknowledges Hexagon shall retain sole custody and control of the underlying online Training Curricula and any documents and information displayed therein. Unless otherwise set forth in the Training Program Statement, Hexagon shall only provide electronic copies of any specified Documentation. Without Hexagon's express, written permission, Customer shall ensure student/user credentials issued to Customer are only assigned and/or used only by Customer's employees.

6. CUSTOMER OBLIGATIONS.

Customer shall at all times be responsible for administering and monitoring the use of Training Curricula by its students/users. Training Curricula shall be used solely for Customer's internal training purposes. Upon the termination of employment of any student/user, Customer will terminate that individual's access to Training Curricula. Customer shall be responsible for supplying all components necessary to supply of the Training Curricula not expressly specified in the Training Program Statement as a deliverable by Hexagon. Depending upon the nature and delivery method of the particular Training Curricula, components to be supplied by Customer may include, by way of example only, computers or software for use by students/users, internet connectivity, or training space at the Customer's site.

END OF EXHIBIT F

EXHIBIT G

COMMON TERMS GLOSSARY

"Acceptable Use Policy (AUP)" means the Acceptable Use Policy identified as such within Exhibit D (Cloud Program Conditions).

"Activity" or **"Activities"** means a single work activity/event or collection of work activities/events by a Party or by both Parties under a specified Task.

"Affiliate" means, for business entities, the parent business entity of a Party and any business entities in which a Party or its parent company directly or indirectly hold a controlling ownership interest. "Affiliates" means, for government entities which are Customers, an entity which has entered into an intergovernmental agreement with Customer which: (i) relates to or addresses the subject matter of the Primary Contracting Document; and (ii) was disclosed to, and acknowledged by, Hexagon (A) prior to the Effective Date for any existing intergovernmental agreements, and (B) prior to any renewal date of such Primary Contracting Document for any intergovernmental agreements entered into after the Effective Date. "Control" for the purposes of this definition means that Customer owns in excess of fifty percent (50%) of the ownership interest of the Affiliate or owns a majority of the voting shares of the Affiliate. For purposes of Section 9 in the General Terms and Conditions, an Affiliate is not a third party.

"Authorized Cloud User" means an individual user authorized by the Customer to use an entire Cloud Program on behalf of the Customer and for whom an account is set up by which the Authorized Cloud User can utilize Cloud Services Support and log Cloud Service Requests and Product Change Requests.

"Auxiliary System License" means the license(s) of Software Product made available by Hexagon for select Software Products to augment Production System Licenses. Each Auxiliary System License requires a corresponding Production System License and the term of the Auxiliary System License shall not exceed the term of the applicable Production System License.

"Beta Software" means any version of Software Product prior to a generally available commercial release of such Software Product.

"Business Day" means any day other than a weekend or public holiday in the country listed on the Quote.

"Business Hour" means an hour occurring during a Business Day and during the generally recognized eight (8) working hours comprising the Business Day at the Customer's location.

"Catastrophic Event" means a rare circumstance in which mass casualties and/or significant property damage has occurred or is imminent (e.g., September 11th, hurricanes greater than Category 2 on the Saffir-Simpson scale, earthquakes greater than 6.1 on the Richter scale).

"Change Order" means a document executed or accepted in writing by both Parties that modifies the scope, price, milestones, and/or project schedule of an Order.

"Client" means a computing device connected to a Server.

"Cloud Anniversary" means the anniversary of the date on which Hexagon provided the License Key(s) to Customer.

"Cloud Application(s)" means the Hexagon software applications, including without limitation application programming interfaces made available by Hexagon through the Cloud Portal as part of the Cloud Program. Cloud Application(s) are subject to Cloud Services Schedules.

"Cloud Consulting Services" means Services that relate to the Cloud Program including, but not limited to, implementation, configuration, customization, data conversion, Onboarding, design, training, and or enhancement of the Cloud Program.

"Cloud Cutover" means the point in time when Customer first uses the Cloud Program for its generally marketed purpose.

"Cloud Development Environment" means a logical group of virtual or physical computers comprised within the Cloud Environment to which the Customer will be provided with access and use for the limited purpose of making modifications, as specifically permitted herein, to the Cloud Application. For purposes of clarity, the Cloud Development Environment cannot be used in Production or for training purposes.

"Cloud Environment" means the collection of remote environments provided to Customer on which the Cloud Application(s) operates and that is supported by Hexagon.

"Cloud Optional Services" means those certain Hexagon Software Products that provide ancillary functionality or capability to the Cloud Applications, including, but not limited to, interfaces and custom forms and functionality. Unless specific Cloud Optional Services are identified in the Quote with a corresponding purchase commitment from Customer, Cloud Program does not include Cloud Optional Services.

"Cloud Portal" means the website through which Customer accesses and uses the Cloud Program. The Cloud Portal provides access to the Cloud Program according to Customer's rights, and further provides access to additional Cloud Services, as made available by Hexagon.

"Cloud Program" means the combination of Cloud Services, Cloud Application(s), Local Software, Third Party Software , and Cloud Optional Services provided pursuant to the Order Documents. The components of the Cloud Program are specifically identified in the Quote and for purposes of this definition shall mean only those components and not any other components not specifically listed in the Quote.

"Cloud Program Fees" means, collectively, any of the fees payable by Customer to Hexagon for the Cloud Program (or any part thereof). Cloud Program Fees shall be in the amount described in the Quote and/or Cloud Services Schedule, and shall be invoiced on an annual basis, except to the extent otherwise expressly provided in the Primary Contracting Document or the Cloud Services Schedule.

"Cloud Program Start Date" means the date on which the first License Key(s) are provided to the Customer. For Cloud Program Fees purposes, Cloud Program use by Customer will be assumed to be for the entire Month in which the Cloud Program Start Date falls regardless of the actual date in such Month that access to the applicable Cloud Application began.

"Cloud Service Request" means a request made to the first level support service to diagnose and address an Error in a Cloud Application or to report the purchased Cloud Application(s) is not Available.

"Cloud Services" means the services, service levels, Cloud Services Support, Customer Cloud Environment, and Third Party Service Provider's hosting services (which are more particularly described in the Cloud Services Schedule(s)), for Cloud Application(s), Cloud Optional Services, and Third Party Software and ordered by the Customer.

"Cloud Services Schedule" means a document(s) titled "Cloud Services Schedule" related to one or more Cloud Application(s) that contains additional details regarding the Cloud Services being provided to Customer with respect to the applicable Cloud Program components purchased by Customer. In the absence of Cloud Service Schedule(s) being included within the Order Documents, Cloud Services Schedules may be found at https://www.hexagonsafetyinfrastructure.com/-/media/Legal/Hexagon/SI/TPS/CSS-LLP.pdf, which Schedules are incorporated into the Order as if fully set forth therein.

"Cloud Services Support" means the service specified as such in the Cloud Conditions through which Customer can report Cloud Service Requests and Product Change Requests.

"Cloud Staging Environment" or **"Cloud Testing Environment"** means a logical group of virtual or physical computers comprised within the Cloud Environment to which the Customer will be provided with access and use for the limited purposes of testing modifications and training, as specifically permitted herein, to the purchased Cloud Application(s). For purposes of clarity, the Cloud Staging Environment cannot be used in Production.

“Cloud Term” means the duration of a Cloud Program Order.

“Confidential Information” means any data or information, tangible or intangible, disclosed or made available by either Party (the "Disclosing Party") to the other Party (the "Receiving Party") that the Disclosing Party considers confidential or proprietary and is not generally known in the industry or to competitors of the Disclosing Party and which shall include: (i) tangible information marked by the Disclosing Party with the word "Confidential" or otherwise identified by an appropriate stamp or legend indicating its confidential nature; (ii) information disclosed orally or visually and identified by the Disclosing Party as confidential when disclosed, and confirmed by the Disclosing Party in a written notice within thirty (30) days following disclosure, which notice shall include markings similar to those outlined above; and (iii) all other information that, notwithstanding the absence of markings or designations, would be understood by the Parties, exercising reasonable business judgment, to be confidential. The term Confidential Information does not include information that: (i) is or becomes available in the public domain through no act of the Receiving Party; (ii) has been received on a non-confidential basis from a third party without breach of the Primary Contracting Document, where the Receiving Party has no reason to believe that such third party is bound by any confidentiality obligation to the Disclosing Party; (iii) was developed independently by the Receiving Party without reliance on the disclosed Confidential Information, provided that such independent development can be substantiated; (iv) was within the Receiving Party’s possession prior to its being furnished by the Disclosing Party, where the Receiving Party has no reason to believe that such third party was bound by any confidentiality obligation to the Disclosing Party, or (v) is confirmed in writing by the Disclosing Party as not being confidential.

“Core” means a physical processor on a computer Server that can respond to and execute the basic instructions that drive the computer. A Central Processing Unit (“CPU”) may have one or more Cores, and a given Server may have multiple CPU sockets that may each contain multiple Cores.

“COTS” means commercial off the shelf Intellectual Property in the form generally released and distributed to Hexagon’s customers and not including any functionality or features requiring source code changes.

“COTS Documentation” means commercial off the shelf Documentation in the form generally released and distributed to Hexagon’s customers and not including or requiring changes thereto.

“Coverage Period” means the period of performance of Maintenance Services with respect to a Covered Product, as stated in the Order Documents. Coverage Periods may differ for discrete Covered Products.

“Coverage Period Anniversary” means the anniversary of the date on which the Coverage Period commenced.

“Covered Products” means collectively, Covered Software Product(s) and Covered Third Party Products.

“Covered Software Product(s)” means Software Product(s) and Developer Tools identified in the Order Documents as software for which Maintenance Services are to be provided by Hexagon. Covered Software Products shall not include Third Party Software or any Cloud Program.

“Covered Third Party Products” means Software Product(s) identified in the Order Documents as Third Party Software for which Maintenance Services are to be provided by Hexagon. Covered Third Party Products shall not include Software Products or any Cloud Program.

“Credentials” means the unique log-in identifier by which a person could access a service or benefit, such as, without limitation, a Cloud Program or Training Curricula.

“Customer” means the non-Hexagon party to the Primary Contracting Document.

“Customer Cloud Administration” means providing User’s access to the Cloud Application(s) purchased by Customer, managing User accounts, providing Credentials to Users, and any system administration beyond User interface.

“Customer Cloud Environment” means a logical group of virtual or physical computers comprised within the Cloud Environment and Local Environment to which the Customer will be provided with access and use

of as part of the Cloud Program. A Customer Cloud Environment consists of a Cloud Development Environment and Production Environment.

"Customer Data" means all electronic data or information: (i) provided by Customer to Hexagon in connection with the Deliverables provided pursuant to an Order; and/or (ii) created by Customer and/or submitted to the Cloud Environment by Customers, Users, and/or Authorized Cloud Users. "Customer Data" shall not mean data which (i) is not particular to Customer, and/or (ii) is of value to the general implementation, development, operation, or use of Hexagon products or services for the benefit of other customers. For the avoidance of doubt, Customer Data shall not include the Cloud Application(s), Software Products, Cloud Optional Services, Documentation written by Hexagon, DevTools, Content, Equipment and Software intentionally designed and embedded with Equipment or Special Purpose Items, and any other data and information provided as part of the Cloud Program or constituting a Hexagon Deliverable.

"Customer Data Rights" means: (i) the right to use Customer Data that contains Customer's Confidential Information to perform Hexagon's obligations within the Order; (ii) the right to use, alter, modify, and disclose Customer Data that does not include Customer's Confidential Information to perform Hexagon's obligations and other business purposes for which the information may be disclosed to third parties; and (iii) except as otherwise provided in the EULA or Developer Tools Schedule, a worldwide, royalty-free, irrevocable license to use, replicate, sell, modify, enhance, and distribute any works created by the Customer through its use of Developer Tools.

"Customer Specified Data Center" means a data center used in the provision of a Cloud Environment, whose location has been specified by the Customer and agreed to by Hexagon and identified in the Quote. Additional Cloud Program Fees may be payable for a Customer Specified Data Center.

"Customized Software" means those Services Deliverables that are software or computer code, whether in source code or object code.

"Cutover" means the point in time in which a Software Product(s) is first used by User for its generally marketed purpose.

"Data Center(s)" means the data center(s) from which the Cloud Program (or part thereof) will be stored as determined by Hexagon or its Third Party Service Provider.

"Defect" means a reproducible instance of an adverse and incorrect functioning of a Software Product or Cloud Application that impacts the ability to use functionality intentionally integrated in the design of the Software Product or Cloud Application, assuming proper usage of the Software Product or Cloud Application in its required operating environment. Defects are further classified into four levels as follows:

Level	Impact of Defect
▸ Level One	*No workaround available and either:* ▸ *Productive use prohibited, or* ▸ *Aborts.*
▸ Level Two	*No workaround available and either:* ▸ Primary purpose compromised, or ▸ Productive use significantly impacted
▸ Level Three	▸ Productive, but incomplete operation Level Three Defects generally have a workaround or do not otherwise substantially impair productive use.
▸ Level Four	▸ Defects not qualifying as Level One, Two, or Three, including defects of a cosmetic nature and defects not materially limiting complete productive use

Customer shall classify a Defect in accordance with the foregoing; provided that, Hexagon shall reclassify the Defect as appropriate following its review thereof.

"Deliverable(s)" means all Services Deliverables, software, hardware, Cloud Programs, and other items delivered or to be delivered by Hexagon to Customer and identified in the Order.

"Designated Portal" means the portal(s), website(s), platform(s), or other similar channels designated by Hexagon from time to time to be used for specific collaboration(s), information dissemination(s), or communications(s).

"Developer Tools" or "DevTools" means any software intended for use by developers to create (i) software for (a) redistribution, or (b) interfacing two or more of the following: Software, Cloud Applications, E/C; or (ii) specific customizations for which the Developer Tool is intended and designed. Developer Tools are subject to Developer Tools Schedules.

"Developer Tools Schedule" or "DevTools Schedule" means a document relating to certain DevTools provided by Hexagon listed in the Order Documents that identifies particular details, limitations, licensing, and other parameters relating to the DevTools. In the absence of DevTools Schedule(s) being included within the Order Documents, DevTools Schedules may be found at https://www.hexagonsafetyinfrastructure.com/-/media/Legal/Hexagon/SI/TPS/DT-LLP.pdf, which Schedules are incorporated into the Order as if fully set forth therein.

"Documentation" means, whether in electronic or printed form, any user's guides, reference guides, administrator's guides, configuration guides, release guides, installation guides, and help guides made available through the Designated Portal. Not all of the types of Software Products or Cloud Applications are provided with Documentation or with similar Documentation.

"Effective Date" means the date and time the last Party is on notice that all Parties have accepted the Primary Contracting Document.

"Emergency Maintenance" means all maintenance performed when a Cloud Service Request demands immediate, unplanned attention, as reasonably determined by Hexagon.

"Equipment" means tangible, personal property to be provided by Hexagon identified in Order Documents, including, but not limited to computing hardware, computer-related equipment, computer devices, furniture, sensors, equipment, unmanned aerial vehicles, and instruments.

"**E/C" or "Equipment/Content"** means digital content identified in an E/C Schedule and/or any Equipment supplied by or through Hexagon. For purposes of clarity, the term "E/C" excludes Maintenance Services, Cloud Program, Software (except Software intentionally designed and embedded with Equipment), and Services. E/C is subject to E/C Schedules.

"E/C Schedule" means a document relating to certain E/C provided by Hexagon listed in the Order Documents that address some or all of the following depending upon the offering being addressed: licensing requirements for any embedded Software, maintenance parameters and limitations, warranty, and support provisions. In the absence of E/C Schedule(s) being included within the Order Documents, E/C Schedules may be found at https://www.hexagonsafetyinfrastructure.com/-/media/Legal/Hexagon/SI/TPS/EC-LLP.pdf, which Schedules are incorporated into the Order as if fully set forth therein.

"Error" means a Defect with a purchased Cloud Application, Cloud Optional Service, or Third Party Software causing a purchased Cloud Application to fail to materially conform to its designed functionality or Documentation. Errors are further classified into the same four levels as corresponding to the definition for "Defect."

"EULA" means the certain Hexagon End-User License Agreement set forth in these Master Terms as Exhibit A and/or that is delivered with Software and which must be accepted prior to Software installation.

"Exchanged Product" means a later released Software Product which the Customer will receive pursuant to its Maintenance Contract and supplants the Replaced Product.

"Fixed Price Project Assignment" means a type of Order where Hexagon will provide Services with or without accompanying Product(s) for a fixed price.

"Hexagon" means the entity that is a member of the Hexagon Group of companies that is identified in the Order Documents; provided however, as used in the EULA, "Hexagon" means Intergraph Corporation.

"Hexagon IP" means Hexagon or Hexagon Affiliate developed, created, or prepared Intellectual Property. Additional information regarding Hexagon patents, including a list of registered patents associated with the Software Products, is available at www.intergraph.com/patents and/or www.uspto.gov.

"Intellectual Property" or **"IPR"** means all forms of intellectual property including, but not limited to, patents, trademarks, copyrights, trade secrets, methodologies, logos, techniques, processes, know-how, formulae, algorithms, logic designs, screen displays, schematics, source and object code computer programs or software, declaring code, implementing code, Documentation, mask work rights, digital data content, design, ideas, product information, inventions and improvements thereto, and all works of authorship fixed in any medium of expression (including any form of online, digital, or electronic medium), whether or not copyrightable and whether registered or not.

"Lapse" means an occurrence of any period of time, regardless of duration, during which (i) a Covered Product is not the subject of an active Order for Maintenance Services or other Maintenance Contract and an active Coverage Period, and/or (ii) payment is past due to Hexagon under a Maintenance Contract. Extension of a Coverage Period and/or payment to Hexagon after the occurrence of a Lapse shall not negate a Lapse, absent Hexagon's express written waiver.

"License Key(s)" means certain unique data string(s) verifying authorized access to the Cloud Application(s), which are purchased by the Customer and provided by Hexagon, as set forth on the Quote.

"Local Environment" means the collection of environments provided and supported by Customer (e.g. providing System Equipment, etc.) in which the Local Software operates.

"Local Software" means software applications incidental to the Cloud Program which are designed to operate natively on devices outside the Cloud Portal and in the Local Environment.

"Maintenance Contract" means a contract under which Hexagon provides Maintenance Services to Customer in relation to Covered Products and under which Customer is to compensate Hexagon therefor.

"Maintenance Services" means only those services described in the document titled "Maintenance Terms and Conditions for Software" provided by Hexagon with respect to Software and other Deliverables licensed to Customer and identified in the Order Documents as the subject of Maintenance Services.

"Material Adverse Effect" means a change that individually or collectively in aggregate with other changes has the impact of (i) negatively and materially reducing the Customer's and/or its Affiliates and/or its/their Authorized Cloud Users' or Users' access and/or usage rights in respect of the Cloud Program and which render the Cloud Program unusable for its primary intended purpose; or (ii) making the Cloud Program materially less secure which results in increased risk to Customer Data or to data belonging to other Hexagon customers. For clarity, a Material Adverse Effect is a condition which would render the Cloud Program un-usable or materially less secure for intended users generally, and not merely as a result of individual characteristics associated with Customer or its specific implementation or operation.

"Metered License" means a specific type of Subscription License that allows the Customer to use the Subscription License up to the number of hours set forth in the Quote during the Subscription Term. For reference, a Subscription License that is a Metered License shall have the word "Metered" in the Software Product name and/or have the letters "MTR" at the end of the product number for the Software Product instead of the other identifiers corresponding to an unmetered Subscription License referenced in its definition.

"Minimal Operations Levels" means operation of a Software Product without a Level One Defect.

“Modern Release” means a version of a Software Product published by Hexagon no more than eighteen (18) months prior to Customer’s first use thereof in Production.

“Month” means, unless otherwise stated in the applicable provision, a calendar month.

“Network Requirements” means (i) the minimum requirements, including but not limited to software and/or hardware, internet connection, latency or other requirements, which must be met by Customer in order to access the Cloud Portal and use the Cloud Program; and (ii) network recommendations to the Customer which describe general and specific recommendations for the network connection requirements of the Cloud Program in order to enable the Cloud Program to function as designed. The Network Requirements may be updated from time to time and Customer will be notified of such update via posting in the Cloud Portal or as otherwise determined by Hexagon.

“Offboarding” or **“Offboarded”** means the process for offboarding the Customer Data (or part thereof) from the Customer Cloud Environment and relocating or facilitating relocation of Customer Data to another Customer-designated location.

“Onboarding” or **“Onboarded”** means the process of loading Customer Data into the Customer Cloud Environment.

“Onsite Fee” means a fixed fee encompassing Hexagon’s travel expenses for an individual trip (an individual trip means to travel from the Hexagon resource’s primary duty station in furtherance with an Order and lasting no more than five (5) consecutive days).

“Order” means each individual purchase transaction in which the Parties engage, as evidenced by Order Documents.

“Order Documents” shall mean written documents, the terms of which include Hexagon’s commitment to provide specific products, licenses, and/or services at a specified price, subject to the terms and conditions of the Primary Contracting Document. Order Documents may consist of a single document executed by the parties or a combination of documents that together form an Order. Any Schedule applicable to the Order is incorporated into the Order Documents as if fully set forth therein.

“Perpetual License” means a type of license for Software Product which allows the User to use the Software Product in perpetuity so long as the User does not otherwise violate the terms of the EULA. For reference, a Perpetual License on a Quote is denoted by its absence of either the terms “Subscription,” “SaaS,” or “Metered” and/or the absence of the letters ”SU,” ”UB,” “CLD,” or “MTR” at the end of the Software Product number or the letters “HCL” at the beginning of the Software Product number.

“Personal Data” means data, including but not limited to criminal justice information, and other information which corresponds to a living individual person defined to be Personal Data under the applicable Personal Data protection laws of the Customer’s jurisdiction.

“Planned Maintenance” means maintenance planned and communicated in advance by Hexagon to Customer for the maintenance of the Cloud Program.

“Primary Contracting Document” means the contract document accepted by the Parties which references and incorporates this Common Terms Glossary and/or references and incorporates a document to which this Common Terms Glossary is an exhibit or attachment.

“Product Change Request” means a request for additional functionality or modification to the purchased Cloud Application(s) or Covered Products.

“Product Order” means a type of an Order that involves only the sale of Products from Hexagon. A Product Order may include the sale of Maintenance Services or maintenance for Equipment so long as the subject of the services is also included in the Product Order. This type of Order does not include Services or Cloud Programs.

“Product(s)” means either or the combination of Software (including Subscription Licenses), E/C, or other goods, and excluding Services, Maintenance Services, or a Cloud Program.

“Production” means, as applicable, where a Subsystem or Cloud Program is used in production/operation with an aim to accomplish one or more of its ultimate intended purposes. Operation solely for testing or training is not Production.

“Production Environment” means a logical group of virtual or physical computers comprised within the Cloud Environment to which the Customer will be provided with access and use the purchased Cloud Application(s) in production and for its generally marketed purpose.

“Production System License” means the license(s) of Software Product provided to User for general production use.

“Product-Specific Terms” modify the EULA, and (ii) in the event of a conflict between the EULA and Product-Specific Terms, Product-Specific Terms shall govern for the applicable Software. In the event of a conflict of terms between the EULA, any prior Product-Specific Terms (including any product-specific terms delivered in the form of an addendum to the EULA), and later Product-Specific Terms, the later Product-Specific Terms shall take precedence over the EULA and any prior Product-Specific Terms regarding the subject Software.

“Purchase Order” or **“PO”** means a document issued by Customer to Hexagon to authorize the delivery of certain Product(s), Services, Deliverables, or Cloud Programs.

“Quote” means a document issued by Hexagon reflecting Product(s), Services, Maintenance Services, Deliverables, and/or Cloud Programs, which Hexagon offers to provide Customer, as well as the prices and fees therefor, the Customer’s name and location, and any applicable Schedule(s). To the extent any document or information is identified in the Quote with the intention of it being incorporated into the Quote, it will form part of the Quote.

“Replaced Product” means an earlier Software Product which will be replaced pursuant to a Maintenance Contract for an Exchanged Product.

“**Schedule”** means one or more of: E/C Schedule(s), Cloud Services Schedule(s), DevTools Schedule(s), Training Program Statement(s), and/or Special Purpose Schedule(s).

“**Secure Access Tool**" is a tool designated by Hexagon for providing secure, auditable remote access to Customer utilized environments in order for Hexagon support personnel to effectively perform services.

“Security Incident” means an event or set of circumstances resulting in a compromise of the security, confidentiality, or integrity of Customer Data under Hexagon’s control. Examples of Security Incidents include: (i) security breaches to Hexagon’s network perimeter or to internal applications resulting in compromise of Customer Data; (ii) severe degradation of, Hexagon’s security controls, methods, processes or procedures that result in compromise of the security, confidentiality or integrity of Customer Data; and (iii) the unauthorized disclosure of Customer Data.

“Server” means a computer or computer program which manages access by Clients to a centralized resource or service in a network.

“Server-based Software Product” means Server-based software that is accessed by one or more Clients.

“Services” means the work, services, projects, assignments, or tasks Hexagon shall perform pursuant to an Order. Services do not include Maintenance Services, Cloud Programs, or XaaS (anything as a service).

“Services Deliverable” means any data, document, information, Customized Software, Third Party Software, or material provided to Customer as a product of Hexagon’s performance of Services pursuant to an Order. Cloud Programs are not Services Deliverables.

“Software” means the software and DevTools owned by Hexagon or an Affiliate and Third Party Software that is licensed to Customer. For the avoidance of doubt, Cloud Programs and their contents are not “Software” as that term is used herein.

“Software Product” means the Hexagon or Hexagon Affiliate software product(s) identified in the Order Documents, which includes (i) any associated Hexagon files, sample data, demo data, or media with which

the software is provided, (ii) any associated templates, data, printed materials, and "online" or electronic Documentation, and (iii) any Updates of such Software Products not made the subject of a separate license agreement. The term Software Products shall not include, and no rights of use are granted to User for, third party components, Hexagon products, or dependencies unnecessary to operate products made the subject of the Order Documents, but incidentally delivered within the same files or media. Software Product shall not mean any Third Party Software. For the avoidance of doubt, Cloud Programs and their contents are not "Software Products" as that term is used herein. For avoidance if doubt, Software Product does not include Developer Tools. Software Products are subject to all of the terms and conditions of the EULA which the Parties agree will apply to the same; and in the absence of such agreement, then the terms of the EULA provided with the Software Product.

"SOW" means a statement of work setting forth the scope of Services being provided pursuant to an Order.

"Special Purpose Item" means an item identified in Order Documents as due to be delivered by Hexagon, which item is subject to certain unique terms, conditions, restrictions, or requirements identified in a Special Purpose Schedule.

"Special Purpose Schedule" means a document identifying terms, conditions, and restrictions applicable to a Special Purpose Item. In the absence of Special Purpose Schedule(s) being included within the Order Documents, Special Purpose Schedules may be found at https://www.hexagonsafetyinfrastructure.com/-/media/Legal/Hexagon/SI/TPS/SPS-LLP.pdf.

"Subscription" means the collection of Subscription License(s) identified on the Quote and or purchased by the Customer.

"Subscription License" means a particular type of license to a Software Product that allows a Customer to use the Software Product for a specified period of time identified in the Quote. For reference, a Software Product that is a Subscription License shall have the word "Subscription" in the Software Product name and/or have the letters "SU" at the end of the product number for the Software Product.

"Subscription Term" means the period of time during which Users are authorized to use the Subscription License as set forth on the applicable Quote beginning on the date the Subscription Licenses are provided to the User or the User is provided license keys or access to the Subscription License, unless otherwise noted in the Order Documents.

"Subsystem" means a Hexagon solution that is designed to provide a specific capability independent of the procurement of any other Subsystem. Hexagon's computer aided dispatch system ("I/CAD" or "OnCall Dispatch"), records management system ("RMS" or "OnCall Records"), and G/Technology (G/Tech) are each an example of a Subsystem.

"System" means a physical or operational location where the Software resides and operates on an individual Server or where a single operational identification number ("Site ID") has been assigned by Hexagon.

"System Equipment" means all computer-related hardware, including but not limited to, servers, workstations, cables, mice, keyboards, cameras, and SAN's; operating system software; database software; and other third party software.

"Task" means an Activity or combination of Activities of any nature whether tangible or intangible, whether onsite or remote, or an event, as further identified in an SOW.

"Task Acceptance" means the event when the Task Acceptance Criteria has been satisfied in accordance with the Task Acceptance Process.

"Task Acceptance Criteria" means the criteria by which a Task will be evaluated for completion as described in an SOW.

"Task Acceptance Process" means the process by the Customer and Hexagon verify completion of the Task Acceptance Criteria as further described below. Once Hexagon believes the Task Acceptance Criteria

has been successfully completed, Hexagon shall submit for execution by Customer's project manager a sign-off form in substantial conformity with Exhibit C, "Project Deliverable Sign-off Form." Within ten (10) Business Days of receipt of the applicable Project Deliverable Sign-off Form for the completed milestone or Task, Customer's project manager will either: (i) execute the Project Deliverable Sign-off Form provided by Hexagon, or (ii) provide a written description of all deficiencies to Hexagon. If Customer fails to perform either action identified in the preceding sentence within ten (10) Business Days, or if the Deliverable, including the Software contained in the Fixed Price Project Assignment Order, is placed into Production or utilized in a live environment, then the Task or milestone shall be deemed accepted.

"Term" means the duration of performance under the contract into which this Common Terms Glossary is incorporated by reference.

"Third Party Service Provider" means the third party service provider with whom Hexagon enters into a subcontract with respect to the hosting of a cloud platform, Training Curricula, and/or other services to provide an element of the Cloud Program, Training Curricula, or other service to Customer (if applicable) on behalf of Hexagon.

"Third Party Software" means computer software or other technology in which any person or entity, other than Hexagon or Hexagon's Affiliate, has any right, title or interest, including any restrictions or obligations (such as obligations to obtain consents or approvals and restrictions that may be eliminated only by obtaining such consents or approvals) applicable to the computer software or technology, but does not include software embedded in the Software Products by license from third parties. The use of Third Party Software is subject to all of the terms and conditions of the Third Party Terms. "Third Party Software Products" also means, where applicable, pre-requisite third party software products used by Hexagon in order for Customer to receive other components of the Cloud Program or licensed by Hexagon and used by the Customer to use Cloud Application or Cloud Optional Services.

"Third Party Terms" means for certain Third Party Software additional terms and conditions provided with the Order Documents and/or cited in the Use Terms, or otherwise made available to the Customer or any User.

"Time and Materials Project Assignment" means Hexagon will perform the Services set forth in an Order on an hourly basis until the project is either completed or the authorized hours are exhausted, whichever comes first. Unless otherwise specified in the Order Documents, a Time and Materials Project Assignment shall end six (6) months after formation of the Order.

"Training Curricula" means one or more training classes or resources provided by Hexagon to Customer as a service over a limited time period. Training Curricula are subject to Training Program Statements.

"Training Program Statement" means document(s) titled "Training Program Statement" containing additional details regarding the Training Curricula parts being provided to Customer, including, but not limited to: whether the training is provided live on-site, live but remotely, or by way of recorded or static online content; and, certain other pertinent details; provided that "Training Program Statement" may alternatively refer to only those specific terms of an SOW containing additional details regarding Training Curricula being provided to Customer. In the absence of Training Program Statement(s) being included within the Order Documents, Training Program Statements may be found at https://www.hexagonsafetyinfrastructure.com/-/media/Legal/Hexagon/SI/TPS/TPS-LLP.pdf, which Training Program Statements are incorporated into the Order as if fully set forth therein.

"Update" means any upgrade, modified version, new release, fix, patch and/or update of the Software. Updates can require full installation and a new License Key. Updates are subject to all of the terms and conditions of the EULA provided with User's then current version of the Software; provided that if a new EULA is delivered with an Update, acceptance thereof is a requirement for its use.

"User" means Customer and/or an individual employed by Customer and authorized by Hexagon to use a particular Software, Cloud Application, Third Party Software, or Cloud Optional Services on behalf of the Customer. A User may also include Customer's contractor who requires temporary use in order to provide services on Customer's behalf. A person can only be authorized and a User if the person is an employee

or designee of Customer and Customer has purchased the requisite number of licenses, or in the case of Cloud Programs, the requisite number of License Key(s) to provide Credentials for that User.

"Use Terms" means the Hexagon Product Usage Policy and Product Specific Terms accessible from https://www.hexagonsafetyinfrastructure.com/-/media/Legal/Hexagon/SI/Licenses/LLP/LLP_08-2019.pdf which are incorporated herein. For purposes of clarity, the Use Terms corresponding to the date of the Order shall apply to that specific Order and the Software provided thereunder.

"Version Limitation I" is a status reached by a Software Product on the earlier of the (i) the third anniversary of the Customer's first operation of that Software Product in a live Production environment or (ii) the fifth anniversary of Hexagon's first actual delivery of the Software Product to the Customer for implementation; provided that each time Customer upgrades the version of the Software Product used in Production to a Modern Release, a reset shall occur, such that Version Limitation I shall thereafter be reached upon the third anniversary of the Customer's first operation of such Modern Release in a live Production environment.

"Version Limitation II" is a status reached by a Software Product on the earlier of (i) the fourth anniversary of the Customer's first operation of that Software Product in a live Production environment or (ii) the sixth anniversary of Hexagon's first actual delivery of the Software Product to the Customer for implementation; provided that each time Customer upgrades the version of the Software Product used in Production to a Modern Release, a reset shall occur, such that Version Limitation II shall thereafter be reached upon the fourth anniversary of the Customer's first operation of such Modern Release in a live Production environment.

"Version Limitations" means, separately and collectively, limitations on Services to be provided hereunder based upon a Covered Product reaching Version Limitation I and/or Version Limitation II.

"Virus" means any thing or device (including any software, code, file or program) which may: (i) prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; (ii) prevent, impair or otherwise adversely affect access to or the operation of any program or data, including the reliability of any program or data (whether by rearranging, altering or erasing the program or data in whole or part or otherwise); or (iii) adversely affect the user experience or security, including worms, Trojan horses, viruses and other similar things or devices.

"Work" means, as applicable, the performance or providing of Services, Maintenance Services, or Cloud Services.

"XML Files" means the XML (Extensible Markup Language) files generated by the Software Product, where applicable.

"XSL Stylesheets" means the XSL (Extensible Stylesheet Language) presentation of a class of XML Files which, when included with the Software Product, describe how an instance of the class is transformed into an XML (Extensible Markup Language) document that uses the formatting vocabulary.

END OF EXHIBIT G

HEXAGON

Williamson County, TX

Statement of Work

for

HxGN OnCall Dispatch and Records On-Premise Implementation

PRESENTED BY:

Rebecca Villalona
Regional Sales Manager
Hexagon Safety, Infrastructure, & Geospatial
305 Intergraph Way
Madison, AL 35758 USA

December 5, 2024

Table of Contents

Introduction

This Statement of Work, including the attachments hereto, provided by Intergraph Corporation by and through its Hexagon Safety, Infrastructure & Geospatial division ("Hexagon") to Williamson County, TX ("Customer") describes the Products and Services that will be provided to implement an integrated computer aided dispatch ("CAD") system, mobile system, and records management system ("RMS") for the Customer (the "Project") in exchange for payment of the amount set forth in the Attachment A (Pricing Summary). This SOW sets forth the Products and Services Hexagon will provide as well as each Party's responsibilities and obligations to implement the Products. Except as otherwise provided herein, capitalized terms shall have the meaning set forth in the Common Terms Glossary and Attachment I (Glossary of Terms) hereto.

The Software provided by Hexagon will be the HxGN OnCall Dispatch Advantage Subsystem ("HxGN OnCall Dispatch System" or "OnCall Dispatch") and HxGN OnCall Records Subsystem ("OnCall Records", and collectively with OnCall Dispatch, "OnCall").

Purpose

The SOW guides the Tasks and Activities for the Project. It documents Project implementation requirements, identifies each Task within the implementation process, sets expectations for each Party, and identifies the Task Acceptance Criteria.

The SOW includes and incorporates the following Attachments:

- Attachment A – Pricing Summary
- Attachment B – Payment Schedule
- Attachment C – Initial Project Schedule
- Attachment D – Training Curriculum
- Attachment E-1 – OnCall Dispatch Specifications
- Attachment E-2 – OnCall Records Specifications
- Attachment F – System Configuration Diagram
- Attachment G -1 CAD/Mobile Functional Specifications Matrix
- Attachment G-2 Law Enforcement RMS Functional Specifications Matrix
- Attachment H – Interface Descriptions
- Attachment I – Glossary of Terms
- Attachment J – GIS Requirements
- Attachment K – Warranty
- Attachment L – Regional Provisions
    - Attachment L-1 – CJIS Security Addendum
- Attachment M – Performance Bond Terms

The remainder of this section details Project assumptions that impact the Project cost, schedule and scope, Project team composition, and Project management responsibilities.

Each Task identified in this SOW includes the following, as necessary: Task Description, Task Deliverables, Task Prerequisites, Task Assumptions, Hexagon/Customer Team Participation and Responsibilities, and Task Acceptance Criteria. The Tasks defined in the SOW may not be listed chronologically, and the actual Project implementation Tasks and timelines will follow the Project Schedule, unless otherwise noted.

Software Functionality and Support

As part of this Project, Hexagon shall provide licenses to Software identified in Attachment A ("Project Software"). The Project Software shall have the capabilities and functionality set forth in the Specifications corresponding to the Project Software, which reflects all of the functionality Hexagon is obligated to provide. The Project Software shall only be tested to evaluate conformity to the Benchmark Criteria The COTS versions of the Project Software will be provided, and, unless otherwise provided in the Software Requirements, this Order does not include any Product Change Requests or Customizations.

OnCall presents an iterative upgrading process that will also be reflected in the Project. Several times per year, Hexagon may publish a new release to OnCall Software Products. Until the end of the Testing Phase, Hexagon may periodically implement newer releases of OnCall within the Customer's environment, so the Customer may have a more current release of OnCall leading into the Training Phase and Deployment Phase.

Upon Cutover, the Warranty Period for the Project Software shall commence as described in Attachment K. Hexagon shall provide support for the Project Software during the Warranty Period in accordance with Exhibit B (Maintenance Terms) of the Agreement. .

Project Governance

Hexagon will assign a Project Manager at the beginning of the Project to act as the primary point of contact at Hexagon for the Customer and provide general oversight and guidance for the Hexagon Project team throughout Project.

To ensure successful delivery of the Project in accordance with the schedule, regular communications and an escalation path are necessary. Typically, all formal communications will occur between the Hexagon Project Manager and the Customer Project Manager. Generally, each Party's Project Manager will have, at minimum, a bi-weekly status conference with one another. On a monthly basis, Hexagon will provide a status report reflecting completed Activities, upcoming Activities, at-risk Activities, other pertinent matters affecting the Project, and, as necessary, an updated Project Schedule. The Customer may propose revisions to the status report and its attachments, but it must do so within five (5) Business Days, otherwise it is final and accepted by the Parties.

Finally, on a quarterly basis, or more frequently if deemed necessary by the Parties, the Department Sponsor for Customer, a Hexagon Director or Vice President responsible for operations, and the Customer's Project Managers shall hold a remote executive review meeting to discuss the status of the Project and particular challenges impacting the Project. The two senior officials for both parties shall also serve as the escalation point for disputes arising between the Project Managers.

Projects of this nature involve both Parties performing a variety of Tasks that are dependent upon one another. With that type of relationship and the number of Tasks involved, from time to time delays may occur. The Hexagon Project Manager and Customer Project Manager will address and take actions to mitigate such delays, to the extent reasonably possible.

The Hexagon Project Manager will manage the Project Schedule and provide copies of it to the Customer as updated. From time to time and outside of the status report process described above, the Project Managers may find an adjustment to the Project Schedule is necessary. If the adjustment is mutually agreeable, the Hexagon Project Manager shall update the Project Schedule and it will become the then current Project Schedule, superseding all prior Project Schedules. The Parties acknowledge that potentially material adjustments to the Project Schedule may need to be addressed through a Change Order due to its impact on other aspects of the Order. Unless otherwise noted between the Project Managers, all Tasks reflected in this SOW are regarded as having completed the Task Acceptance Process upon Cutover or commencement of a Task for which the earlier Task was a prerequisite as noted within the SOW and/or Project Schedule.

Within thirty (30) days of contract execution, Hexagon shall identify by name and title the Project Manager, CAD Technical Lead, and RMS Technical Lead. This shall serve as the key personnel assigned to the project. These individuals shall be the on-site staff for cutover and the post-cutover support. Any change to personnel shall be made only through written authorization by Customer except in the case of illness, death, or employment termination.

Customer Core Team(s)

The Customer shall provide qualified resources to staff the Core Team (described below) to facilitate a successful implementation of OnCall. The Core Team consists of an overall Customer project manager who is responsible for the day-to-day coordination of Customer's Project Activities and personnel divided amongst smaller discipline-oriented groups with particular roles and responsibilities appropriate to the discipline. Those subdivided groups are denoted with suggested team member resources below.

Core Team Roles and Responsibilities

Dispatch Core Team

Below is the defined group of Customer members responsible for decision making for the remainder of the Public Safety Access Point ("PSAP") user group(s) regarding configuration and use of the OnCall Dispatch solution. The "Dispatch Core Team" should consist of, at a minimum, the following resources with the corresponding qualifications:

- **9-1-1 Call-Taker** – This person intimately understands the process by which emergency calls for service are answered, triaged, created in the current CAD, and sent for dispatch.
- **Radio Dispatcher** – This person intimately understands the structure of the PSAP, the agencies for which it dispatches, and the methods in which dispatching occurs.
- **System Administrator (Operational)** – This person is responsible for the operational administration of the OnCall Dispatch system. Managing things like user accounts, permissions, parameter settings, user interface layouts, units, event types, etc.
- **Decision Maker (Operational)** – This person has authority, either by role or designation, to make decisions on behalf of the agency or agencies OnCall Dispatch is serving pertaining to the configuration of OnCall.

The ideal size of the Dispatch Core Team is six (6) members. Under no circumstances shall the Dispatch Core Team be larger than twelve (12) members.

Mobile Core Team

Below is the defined group of Customer members responsible for decision making for the remainder of the field operations user group(s) regarding configuration and use of the OnCall Dispatch mobile solutions (OnCall Mobile) including OnCall Dispatch Mobile Unit, and OnCall Dispatch Mobile Responder. The "Mobile Core Team" should consist of, at a minimum, the following resources with the corresponding qualifications:

- **Patrol / Firefighter** – This person is an active member of the patrol / operational division of the agency. They are tasked with responding to calls for service, field-initiated activities like traffic stops or inspections, and other duties in patrol / operations. This person should not be technology averse. They should embrace the use of technology and seek to find ways to leverage it to their benefit in their daily duties.
- **Patrol Supervisor / Fire Supervisor** – This person is an active member of the patrol / operational division of the agency and responsible for the day-to-day supervision of a group of patrol members or of a specific station/apparatus crew. This person is typically a rank of Sergeant or above in law enforcement and lieutenant or above in Fire/EMS, although actual rank structure in agencies may vary.
- **Investigations / Detective / Fire Marshal** – This person is an active member of the investigations division or fire marshal's office and has primary responsibility for long-term case work or other fire-related investigations.
- **Command Staff** – This person is an active member of the command staff at the agency. This person is typically a rank of Captain or higher in law enforcement or battalion chief or higher in fire departments, although actual rank structure in agencies may vary.
- **Decision Maker** – This person has authority, either by role or designation, to make decisions on behalf of the agency or agencies OnCall Dispatch Mobile Unit or Mobile is serving pertaining to the configuration of OnCall Dispatch mobile products.

The ideal size of the Mobile Core Team is six (6) members. Under no circumstances shall the Mobile Core Team be larger than twelve (12) members.

It is possible to have a Mobile Core Team duplicated for different responder roles, such as a law enforcement Mobile Core Team and a Fire Mobile Core Team.

Records Core Team

Below is the defined group of Customer members responsible for decision making for the remainder of the field operations user group(s) regarding configuration and use of the OnCall Records solution. The Records Core Team either needs knowledge of all applicable departments or has access to local subject matter experts. The Records Core Team should consist of, at a minimum, the following resources with the corresponding qualifications:

- **Subject Matter Experts (SME)** – Person or person(s) responsible for adapting local agency department needs into actionable configuration processes for the new system. This person or persons need access to other local SMEs for all departments that will be utilizing the new system.
- **Technical Support Staff** – The responsibility of Technical Support Staff lies with the adaptation and configuration of the system at a more technical level. Responsibilities potentially include [redacted], current technical understanding of current interfaces in use that are to be adapted to the new systems, etc.

- **Command Staff** – This person is an active member of the command staff at the agency. This person is typically a rank of Captain or higher in law enforcement, although actual rank structure in agencies may vary.
- **Decision Maker** – This person has the authority, either by role or designation, to make decisions on behalf of the agency or agencies OnCall Records is serving pertaining to the configuration of OnCall Records products.

The ideal size of the Records Core Team is twelve (12) members. Under no circumstances shall the Records Core Team be larger than twelve (12) members.

Project Assumptions

The following list of assumptions and Customer responsibilities reflect Hexagon's understanding of the Project. Changes in any of the assumptions and Customer responsibilities will affect the scope, Project Schedule, and/or cost of the Project.

Agreement and Schedule Assumptions

- The Agreement has been executed by both Parties and the Customer has provided either a notice to proceed or PO.
- Hexagon and the Customer will review the SOW and determine a mutually agreeable date for the Services to be performed, which shall be reflected in the then current Project Schedule.
- As reflected in Attachment C, the implementation of CAD and RMS are scheduled to occur concurrently; if the Project cannot be completed concurrently with a simultaneous Cutover, the SOW will need to be modified through a Change Order.
- The Customer shall perform its assigned responsibilities as identified within the Initial Project Schedule (Attachment C) and resulting Project Schedule in the time allotted. If the Customer does not reasonably comply with the Project Schedule, Hexagon is permitted with written notice to suspend its performance on this Project and redeploy its resources on other active projects until the Parties determine a mutually agreed upon date to re-start the Project and memorialize any changed circumstances in a Change Order.
- Hexagon will have timely access to the applicable members of the Core Teams and other Customer Project staff in accordance with the Project Schedule. Customer shall make additional personnel available on a priority basis, as needed, to provide subject matter expertise to complete this Project.
- Customer shall assign appropriately qualified personnel to the Core Teams and ensure they are actively engaged in the Project.
- Any work and effort ascribed to Hexagon in a given Task is confined to that specific Task and may not be used for or applied to any other Task.
- Customer shall provide Hexagon Project Manager with contact information for a Customer resource to resolve any issues that should arise from Hexagon's access of Customer's System during working and non-working hours.
- Any Service Request that is set to "NEED MORE INFO" or "RE-TEST" will be subject to escalation after ten (10) Business Days if the Customer does not update the SR to promote focus on pressing issues. If SR items are closed and the underlying issue continues, the Customer may re-open the SR.
- Any workshop having a duration of three (3) Business Days or less shall begin no earlier than Tuesday of the week of that workshop and will conclude that same week.
- The Customer shall provide Hexagon with access to all data, documents, plans, reports, diagrams, and analyses reasonably related to the Project or otherwise necessary to facilitate Hexagon's performance of its Activities.
- Unless expressly stated in this SOW, all Documentation, if any, provided by Hexagon under this SOW will be COTS Documentation, and the Documentation will not be customized by Hexagon. All Documentation delivered will be in Hexagon-approved format. Changes to Hexagon-format to accommodate specific Customer requests may be done with Hexagon's concurrence.
- Unless Hexagon and Customer mutually agree otherwise, all Documentation provided by Hexagon will only be provided in electronic format.

- Unless otherwise stated in the Task, all Tasks will be conducted remotely.
- All Hexagon personnel performing remote Activities will be identified and properly vetted prior to commencement of those remote Activities.
- As reflected herein, Hexagon may have proposed certain Activities or Tasks be performed on site. Hexagon and Customer may, by mutual agreement, alternatively choose or circumstances necessitate to have these Activities and Tasks performed remotely.
- If the title of a Task includes the name of a Subsystem (e.g., OnCall Records or OnCall Dispatch), that Task shall be construed as pertaining only to that Subsystem unless expressly stated otherwise.

Hardware and Software Assumptions

- All Software will be electronically delivered.
- All specifications provided with this SOW (Attachments E-1, E-2, and F) will assume a traditional on-premises solution (*i.e.*, not a hosted solution), and any change with respect to alternative hosting requires execution of a mutually agreed upon Change Order.
- The Customer shall purchase, install, and test all physical hardware, including the client/mobile hardware.
- The Customer will ensure its hardware, operating system software, database software, and other third-party products/environments conform with Attachment F. Deviations from Attachment F will not be considered due to the critical nature of the software supported by these systems.
- Hexagon and the Customer will verify the final system hardware configuration to ensure conformance with Attachment F.
- Except as expressly identified in Exhibit A, Customer shall purchase all applicable operating systems, database licenses, and Third-Party Software and ensure such operating systems, database licenses, and Third-Party Software meet the minimum requirements as defined in Attachment F.
- [redacted]
- Hexagon technology for this Project will be implemented in the Microsoft environment as specified in Attachment F.
- Customer shall purchase, install, configure, and administer its Network Infrastructure, including, but not limited to, its WAN/LAN and wireless infrastructure. Customer's wireless infrastructure shall meet minimum bandwidth requirements as stated in Attachment F.
- Customer shall be responsible for the wired and wireless connectivity between servers/clients and clients/clients.
- [redacted]
- Customer shall be responsible for, and purchase and maintain if necessary, any hardware and/or third-party software necessary for implementing interfaces.
- Except as specified in this SOW, including Attachment A: Pricing Summary, Hexagon is not required to provide any additional Software customizations, custom forms, forms modifications, third-party software, custom interfaces, or custom reports.

- To the extent the Customer desires to use the Software or other deliverables provided herein in a manner or in combination with software or hardware that is not certified or recommended by Hexagon, then the Customer shall be solely responsible for such use. Hexagon shall not be responsible for the correction of any errors, Defects, reduced performance, compromised functionality, or other unintended consequences arising from such use. The Customer also shall not withhold acceptance of any deliverable or the System due to such use.
- Customer has reviewed the SOW and acknowledges and agrees that Benchmark Criteria: (i) represents all the functionality required of the Hexagon Software; and (ii) is the only software functionality that is required to be delivered under this SOW
- Customer shall have its GIS system conform to the requirements set forth in Attachment J (GIS Requirements)
- Customer may use any supported third-party mapping provider for GIS information within OnCall Dispatch during this Project (see Attachment J). It is the Customer's responsibility to provide this.
- The mapping subsystem shall be dedicated only to supporting HxGN OnCall Dispatch.

System Access Assumptions

- Depending upon the Customer's jurisdiction, additional security guidelines and assumptions are provided in Attachment L.
- Customer consents to Hexagon's inspection and use of Customer's data and systems, including, but not limited to, log files and databases, for the limited purpose of providing the Services specified herein and any future maintenance or warranty services described within the Agreement.
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Third-Party Assumptions

- Customer shall schedule and coordinate third-party technical resources with the skills necessary to perform and/or support all Customer Responsibilities, provide necessary information, respond to Hexagon requests, and support the testing of interfaces, as required. Customer shall schedule and coordinate third-party technical resources in such a way as to ensure that a negative impact to the overall Project Schedule does not occur.
- Customer shall maintain, in good working order, all third-party systems which will integrate with Hexagon software or on which the Hexagon software depends as part of this Project.

- Customer shall be responsible for the operation and timely availability of external systems or third-party software necessary for the execution of the Project.
- If a delay in the Project is caused by a third-party vendor, Hexagon services not covered in this SOW may be required at additional costs.

Project Tasks

Project Initiation

Prior to the Kickoff Meeting and after execution of this SOW or Order, the Hexagon Project Manager will contact the Customer Project Manager to identify the Project Start date and coordinate scheduling the Kickoff Meeting. For the Project to be successful, the following initial Activities must be performed before any Tasks occur:

- Customer shall order hardware, database software, operating system software, or other third-party software consistent with the requirements set forth in Attachments E and F.
- The Hexagon Project Manager will contact the Customer Project Manager. During this initial contact, the Hexagon Project Manager will:
    - Schedule the kickoff meeting;
    - Identify the Project Start date;
    - Create a detailed agenda describing the goals of the kickoff meeting;
    - Discuss any mitigating factors that could affect the Project (e.g., scheduling conflicts, communication factors, and other risk factors);
    - Schedule a conference call before the kickoff to go over the kickoff agenda;
    - Ensure both Hexagon and Customer have appropriate Subject Matter Experts available for kickoff; and

Provide document titled “Infrastructure Build Document”, if not previously provided to the Customer.

- Hexagon’s Project Manager will prepare kickoff materials.
- Hexagon’s Project Manager shall have updated the Initial Project Schedule and provide the draft Updated Initial Project Schedule and sent a copy to the Customer Project Manager for review prior to the Kickoff meeting.

Planning Phase

1. Project Kickoff Meeting

Task Description

The objective of this Task is to discuss and address questions regarding Project Assumptions, discuss the updated Initial Project Schedule and agree to it at the meeting or shortly thereafter, and all requirements are understood prior to beginning any significant work. A meeting for Project Kickoff will be held after the SOW has been fully executed. The Project Kickoff meeting will be scheduled by each party's Project Manager as part of Project Initiation Activities.

Prior to the Kickoff Meeting and after written acceptance of the Agreement, the Hexagon Project Manager will contact the Customer Project Manager to identify the Project Start date and coordinate scheduling the Kickoff Meeting. The Project Kickoff Meeting shall last no more than one (1) Business Day.

During this Task, the Parties shall confirm the updated Initial Project Schedule as updated by the Hexagon Project Manager. The resulting updated Initial Project Schedule shall be substantially similar in durations as that provided within Attachment C. Prior to the Project Kickoff Meeting Task, the Customer Project Manager shall have reviewed the updated Initial Project Schedule and be in a position to succinctly identify any needed changes understanding material extensions of the Initial Project Schedule may require additional Hexagon Services to be added via a Change Order. Once the list of changes has been made to the updated Initial Project Schedule by the Hexagon Project Manager, the Hexagon Project Manager will thereafter provide the Project Schedule to the Customer Project Manager. From time to time, the Parties' Project Managers may modify the Project Schedule upon mutual written consent or upon transmission of an updated Project Schedule to the Customer Project Manager as part of a status report and the Customer Project Manager offers no objection to the updated Project Schedule within five (5) Business Days thereafter.

At the Project Kickoff Meeting, the Customer shall provide: (i) contact information for all members of its Core Team and Executive/Departmental Sponsor, (ii) proposed alterations to the updated Initial Project Schedule, (iii) contact information for any third-party vendors which OnCall will integrate as contemplated in Attachment H, and (iv) identify to Hexagon any perceived concerns or risks with the Project. During the Project Kickoff Meeting, Hexagon shall provide template COTS Interface Questionnaires and the OnCall Records Pre-BPA Questionnaire for Customer completion prior to required Tasks.

Task Deliverables

- Kickoff meeting agenda
- Project Schedule
- Kickoff meeting minutes, to include identified risks and action items
- COTS Interface Questionnaire
- OnCall Records Pre-BPA Questionnaire
- Dynamo e-learning licenses

Task Prerequisites

- Agreement executed by both Customer and Hexagon and PO issued (if applicable).
- Hexagon Project Manager has verbally communicated with the Customer to (i) identify the Project Start date and (ii) coordinate a date for the Project Kickoff Meeting.
- Customer has assigned a Customer Project Manager.

- The Core Team has reviewed this SOW.

Task Assumptions

- The Hexagon Project Manager will conduct the kickoff.
- This task will be conducted on site.
- Some members of the Hexagon Project Team may participate remotely.
- The Dynamo e-learning subscription commences during this Task and lasts for a duration of twelve (12) months from the date issued.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Review the Project organization, roles, and responsibilities with the Customer;
- Conduct an overview of the Project including a review of the SOW to verify all aspects of the Project approach;
- Review the draft Updated Initial Project Schedule and adjust the Updated Initial Project Schedule as needed and mutually agree upon it with Customer;
- Work with Customer to identify and document any potential Project risks;
- Provide meeting minutes that document risks and action items that affect the Project Schedule, resources, and/or the SOW;
- Inform the Customer of VPN requirements for Project implementation and continued System maintenance;
- Review of delivery methodology;
- Provide the Dynamo e-learning licenses for use by the Customer Core Team;
- Establish status reporting requirements; and
- Provide overview of Standard Interfaces being delivered as part of the Project as identified in Attachment H.

Customer Team Participation and Responsibilities

Customer shall:

- Review the SOW;
- Ensure its Core Teams attend the applicable portions of the Kickoff Meeting;
- Provide SMEs and any other resources as recommended by the Customer and Hexagon Project Managers;
- Provide Hexagon with VPN access and individualized user accounts to Customer's System as appropriate for this Project and continued software maintenance;
- Have previously reviewed the Updated Initial Project Schedule and work with Hexagon to finalize the Updated Initial Project Schedule;
- Provide location and logistical support for Kickoff Meeting; and
- Designate and prepare workspace for Hexagon personnel.

Task Acceptance Criteria

This Task is complete at the conclusion of the Project Kickoff Meeting and delivery of the Project Kickoff meeting minutes to Customer.

2. COTS Interface Questionnaire Completion

Task Description

Hexagon will provide an interface questionnaire (“COTS Interface Questionnaire”) to the Customer to complete. The Customer shall complete the COTS Interface Questionnaire within five (5) Business Days of receipt (“COTS Interface Review Period”) whereupon Hexagon will be able to install the COTS Interface and configure it based upon the information provided in the COTS Interface Questionnaire subject to the functionality and features within the COTS version of the Interface.

The following Interfaces are regarded as the COTS Interfaces (collectively, "COTS Interfaces”):

- ANI/ALI Interface (included with HxGN OnCall Dispatch | Advantage)
- HxGN OnCall Dispatch | ProQA
- HxGN OnCall Dispatch | Informer
  - For NCIC/TLETS
- HxGN OnCall Dispatch | Tracker
  - For [redacted]
- HxGN OnCall Dispatch | Notifications
  - [redacted]
  - [redacted]
- HxGN OnCall Dispatch | FireLink
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- HxGN OnCall Dispatch | CADLink
  - [redacted]
  - [redacted]
  - [redacted]
- HxGN OnCall Dispatch | PTT
  - To [redacted]
- HxGN OnCall Dispatch | [redacted]

For more information on, parameters of, and assumptions underlying the COTS Interfaces, see Attachment H, Interface Descriptions.

Task Deliverables

- Completed COTS Interface Questionnaires

Task Prerequisites

- Project Kickoff Meeting Task is complete.

- Hexagon has submitted COTS Interface Questionnaires to Customer.

Task Assumptions

- The Customer will direct its third-party vendors to provide any API or specification documentation required to configure the COTS Interfaces.
- If required, all NDAs between Hexagon and third parties will be executed and current. The Customer will exercise all reasonable efforts to facilitate its third-party vendors reasonable cooperation with this requirement.
- The Customer will exercise all reasonable efforts to facilitate cooperation and information from its third-party vendors and/or state agency as reasonably necessary for the configuration, testing, and Cutover of the COTS Interfaces.
- Unless otherwise provided in the Specifications, only COTS versions of the COTS Interfaces will be provided and configured.
- The Customer shall be responsible for underlying requirements pertaining to its third-party systems as described in Attachment H.
- The ANI/ALI interface component of the OnCall Dispatch System will provide the interface to an ANI/ALI controller. It will accept ANI/ALI packets containing ASCII data via an Ethernet Network (TCP/IP) or a Serial COM Port connection. If the Customer's ANI/ALI feed is via Serial COM Port the Customer will need to obtain an IP to Serial device.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Review completed COTS Interface Questionnaires.

Customer Team Participation and Responsibilities

Customer shall:

- Promptly review, complete, and submit COTS Interface Questionnaires and provide comments, questions, or approval within the COTS Interface Review Period.

Task Acceptance Criteria

This Task is complete upon Hexagon providing the COTS Interface Questionnaires and reviewing Customer's responses it provided within the COTS Interface Review Period.

3. OnCall Dispatch Launch

Task Description

OnCall Dispatch Launch ("Launch Workshop") is a workshop style session lasting up to three (3) Business Days that is intended to educate Dispatch and Mobile Core Team members on the features and functionality of OnCall Dispatch to support the collection and importation of data and information that CAD requires to execute its primary functions ("CAD Static Data"). During the Launch Workshop, Hexagon will provide limited instruction on the use of OnCall Dispatch and OnCall Dispatch Mobile Unit illustrating how the CAD Static Data elements identified below are utilized in the Subsystem. The Launch Workshop is limited in scope to facilitate upcoming System Build Tasks; it is not intended or designed to provide a comprehensive overview or instruction of the Subsystem. Such instruction and training will be provided at later stages of the Project. At the conclusion of the Launch Workshop, Hexagon shall provide to Customer OnCall Dispatch Static Data Collection Spreadsheet(s) to facilitate Customer's collection and eventual importation of CAD Static Data in subsequent Tasks.

Task Deliverables

- OnCall Dispatch Static Data collection spreadsheets

Task Prerequisites

- Project Kickoff Meeting Task is complete.
- Customer Dispatch Core Team is identified.
- Customer Mobile Core Team is identified.

Task Assumptions

- Launch Workshop is conducted using a Hexagon-provided default OnCall Dispatch environment.
- Hexagon responsibilities will be executed on site at a Facility.
- The Launch Workshop shall last no more than three (3) Business Days.
- Customer has provided a Facility.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide limited, focused instruction on the use of OnCall Dispatch, and OnCall Dispatch Administrator, on functional areas that utilize or display the following CAD Static Data elements:
  - Agencies
  - Unit Types (Patrol, Engine, etc.)
  - Units
  - Event Types
  - Disposition Codes
  - Out-of-Service Types
  - Facility Service Types
  - Known Caller Types
  - Special Situation Types
  - Personnel/User Accounts
  - Beats/Station Areas
  - Dispatch Groups
  - Stations (Police Stations, Sub-Stations, Fire Stations, etc.)
  - Number Formats (event, case, etc.)
  - Rotational Services (towing, ambulance, lock smith, etc.)
  - Vehicles
- Provide the Customer with Microsoft Excel based data collection spreadsheets ("OnCall Dispatch Static Data Collection Spreadsheets") to be used in assembling the CAD Static Data elements.

Customer Participation and Responsibilities

Customer shall:

- Provide a facility according to the requirements provided in Task Assumptions;
- Ensure appropriate members of the Dispatch Core Team and Mobile Core Team attend the workshop for the entire Launch Workshop; and
- Participate in discussions and engage with the Hexagon team member.

Task Acceptance Criteria

This Task is complete upon conclusion of the Launch Workshop and the delivery of the OnCall Dispatch Static Data Collection Spreadsheets.

4. OnCall Dispatch GIS Requirements Review – Web Conference

Task Description

Over the course of up to one (1) Business Day, Hexagon will present on the following topics during the "OnCall Dispatch GIS Requirements Review". This Task introduces the Customer GIS team to the GIS services the Customer must provide and which OnCall requires in order to function. Those services are, at a minimum an address locator service, a routing service, and a base map display service. Hexagon will also cover the deployment related polygon feature classes required to facilitate the assignment of geographic areas to specific agencies.

- Introduction to OnCall Dispatch GIS data requirements (see Attachment J)
- Optional GIS data elements that can be used by OnCall Dispatch

This session will use Hexagon-provided GIS data for the purposes of discussion. Hexagon will use its equipment to conduct any demonstrations that may occur. Customer attendance should be limited to GIS professionals with responsibility for the creation and maintenance of Customer GIS data. Up to six (6) Customer personnel may attend. Map content will be provided to the OnCall Dispatch system through map layers and web services to be provided by the Customer.

Task Deliverables

- OnCall Dispatch GIS Requirements Review

Task Prerequisites

- Project Kickoff Meeting Task is complete.

Task Assumptions

- Appropriate facilities have been identified to support the number of attendees (if co-located), including an LCD projector and a projection screen.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Conduct the OnCall Dispatch GIS Requirements Review.

Customer Team Participation and Responsibilities

Customer shall:

- Ensure its GIS/Map Administrator is involved throughout this Task;
- Supply facilities, including an LCD projector and a projection screen;
- Designate and assign no more than four (4) Customer mapping/GIS personnel to attend the entire workshop. Two (2) additional people may attend as observers/auditors; and
- Ensure that all appropriate Customer GIS professionals are sufficiently trained and experienced in GIS fundamentals.

Task Acceptance Criteria

The Task is complete after the OnCall Dispatch GIS Requirements Review is conducted.

5. OnCall Records Business Process Analysis (BPA) Workshop

Task Description

Hexagon will conduct the Business Process Analysis ("BPA") Workshop ("BPA Workshop") with the Customer's Records Core Team and SMEs. The BPA Workshop lasts up to four (4) Business Days and is designed to document current processes that will need to be reviewed during configuration workshops and provide a guidebook for the Records Core Team to use as they work to configure the Records Subsystem.

The BPA Workshop will be an interactive workshop with the Records Core Team and any SMEs that may be required. The BPA Workshop will provide the Customer with a system and process overview to prepare for the upcoming Records Core Team training and subsequent configuration workshops where the Records Core Team will set up OnCall Records for Production use. It is important to note that some current Customer processes may not be applicable to the new Subsystem, and adjustments will have to be made by the Customer's process and procedures to implement the COTS OnCall Records Subsystem. This knowledge will be critical during the configuration workshops. The BPA Workshop results will be documented by Customer staff.

BPA Workshop Agenda

The BPA agenda will be developed between the Hexagon and Customer Project Managers based on the functional areas, subject areas specific to the Customer, and number of BPA workshops purchased. The topic points will be based on the "Pre-BPA Questionnaire" that is completed by the Customer and focuses on the current business processes.

Task Deliverables

- BPA Workshop.

Task Prerequisites

- Customer has provided appropriate meeting/training facilities.
- Project Kickoff Meeting Task is complete.
- Customer has collected and or has available necessary operating procedures, policies, plans, and/or information applicable to the BPA Workshop.
- Customer has completed and returned the Pre-BPA Questionnaire.

Task Assumptions

- The sessions are typically done in six (6)-hour blocks over (4) days.
- No more than twelve (12) agency personnel may attend.
- Hexagon responsibilities will be executed on site at a Facility.
- The BPA Workshop will cover only COTS OnCall Records functionality.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Conduct the BPA Workshop.

Customer Team Participation and Responsibilities

Customer shall:

- Attend BPA Workshop;
- Provide a facility according to the requirements provided in Task Assumptions;
- Provide a Project Workstation for each attendee;
- Collect and have ready at the BPA Workshop all of Customer's documents and information pertaining to its business processes, operating procedures, and workflows;
- Document Customer business processes to be used in the Configuration Workshops; and
- Provide access and resources as identified.

Task Acceptance Criteria

This Task is complete once the BPA Workshop has been provided.

6. Custom Interface Requirements Gathering

Task Description

During this Task, Hexagon and Customer will meet via conference call to validate the assumptions and design of each Custom Interface identified in this SOW and Attachment H (Interface Descriptions). This Custom Interfaces Requirements Gathering workshop is intended to contain a series of discussions to validate the requirements and assumptions underlying the Custom Interfaces. These sessions should include third-party vendors where appropriate. During the sessions, the specific workflow and data requirements for each of the interfaces listed below will be discussed in detail.

The information obtained in combination with the information in Attachment H will be used to develop an Interface Control Document for each Custom Interface. If the assumptions reflected in Attachment H materially change, a Change Order may be appropriate. The ICDs will become the foundation for the Custom Interface development by Hexagon. Once an ICD is mutually approved, it should only be modified through a Change Order. The Customer shall not make any changes to and shall take appropriate actions to prevent its third-party vendor from making substantive changes to the third-party software that is the subject of a Custom Interface once that Custom Interface's respective ICD has been finalized.

The following are regarded as "Custom Interfaces" as the term is defined in Attachment I of this SOW:

- CAD Query Interface to [redacted] Address Query
- CAD Query Interface to [redacted] Address Query
- CAD Query Interface to [redacted] Query
- CAD Interface for Text to 911 (Intrado)
- CAD Interface for [redacted]
- Bi-Directional RMS interface for [redacted]
- RMS Import interface for CRIS
- RMS Import interface for [redacted]
- RMS Export Interface to TDEX
- RMS Import Interface for [redacted]
- RMS to NCIC

For descriptions and assumptions regarding each Custom Interface listed above, please see Attachment H: Interface Descriptions.

As it pertains to the development of the ICD, the parties shall follow the following process. After the Customer provides the necessary information regarding the Custom Interface, Hexagon will prepare a draft ICD for each Custom Interface. Hexagon will then provide the initial draft ICD to the Customer for its review. The Customer shall review the draft ICD and provide any feedback or comments within ten (10) Business Days. As appropriate, Hexagon will incorporate the feedback into the ICD or advise the Customer why certain requests could not be included (e.g. the request conflicted with Attachment H) and finalize the ICD. Hexagon will provide the finalized ICD to the Customer for its written acknowledgement. The Customer will provide a response within three (3) Business Days from Hexagon providing the finalized ICD.

Task Deliverables

- Workshop meeting minutes, to include notes on the specific workflow and data requirements for each custom interface proposed
- ICD documents

Task Prerequisites

- Project Kickoff Meeting Task is complete.

Task Assumptions

- The Customer will coordinate interactions with the third-party vendors, including obtaining and providing any API or specification documentation required to develop the proposed interfaces.
- If required, all NDAs between Hexagon and third parties will be executed and current. Customer is responsible for facilitating its third-party vendors reasonable cooperation with this requirement.
- The Customer is responsible for obtaining cooperation and information from its third-party vendors and/or state agency as reasonably necessary for the development, testing, and cutover of the interfaces.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Lead the interface requirements gathering process and track outstanding items requiring resolution;
- Confer with Customer and third-party points of contact to gather information required to develop ICDs;
- Validate the third-party points of contact are appropriate sources of information necessary to develop ICD;
- Mutually agree with the third-party vendors on the operational and technical interface requirements;
- Gather all available interface data detailed schema, protocols, and specifications, as needed;
- Prepare draft ICDs and submit to Customer for feedback;
- Incorporate Customer feedback into draft ICDs;
- Finalize ICDs for Customer review and approval; and
- Manage the approved ICDs consistent with the change control process.

Customer Team Participation and Responsibilities

Customer shall:

- Identify and set up appropriate facilities;
- Provide points of contacts who are knowledgeable of the workflow and data requirements for Customer hardware and software components with which the Custom Interfaces will interact;
- Provide or have available all necessary information during the workshop to facilitate the creation of the ICD;
- Promptly review all draft ICD submissions and provide comments, questions, or approval within ten (10) Business Days of receipt; and

- Agree to and sign the ICDs before any development work can begin. Failure to approve in a timely manner may impact Project Schedule and incur additional cost.

Task Acceptance Criteria

This Task is complete upon completion of all ICDs and execution of the ICDs by both Hexagon and the Customer.

7. Custom Interface Development

Task Description

During this Task, Hexagon will develop the Custom Interfaces based upon the ICDs that were created from the Custom Interface Requirements Gathering Task.

Task Deliverables

- Custom Interface documentation

Task Prerequisites

- Custom Interface ICDs have been executed by each Party.

Task Assumptions

- Any changes to a third-party interface developed by Hexagon that will alter the agreed-upon ICD will have to be reflected in a mutually executed document, which may include a Change Order.
- Development of the Custom Interface shall not commence until the signed/approved ICD is returned to Hexagon. Failure to approve in a timely manner may impact project schedule and incur additional cost.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Develop the Custom Interfaces based upon the ICD.

Customer Team Participation and Responsibilities

Customer shall:

- Ensure SMEs are available as needed; and
- Obtain third-party cooperation as reasonably requested by Hexagon.

Task Acceptance Criteria

This Task is complete when all Custom Interfaces are developed.

8. OnCall Dispatch Data Conversion Analysis and Mapping

Task Description

Hexagon will analyze legacy databases that are candidates for conversion into the new OnCall Dispatch system and produce an initial mapping of legacy data fields to the corresponding fields in the OnCall Dispatch database tables. Hexagon will convert up to five (5) years originating from no more than 20 tables and no more than 250 elements of data. Converted data shall only be present in the OnCall Dispatch Archive Database and only available for manual searches of said data.

Hexagon will spend one (1) week gathering information about the legacy database(s) that are candidates for conversion into the new System. During this period, Hexagon will:

- Interview Customer SMEs who can provide insight and detailed explanation as to the legacy system data, its meaning, and workflows used to create the data;
- View legacy data in the current system to see where it might fit in the OnCall Dispatch database;
- Demonstrate various parts of the Hexagon system to Customer SMEs to facilitate discussion of possible areas where data might be converted;
- Examine documentation and sample data from the legacy system(s).

At the conclusion of the analysis, Hexagon will produce a Data Conversion Study document that contains:

- A high-level discussion of the feasibility of converting legacy data into OnCall Dispatch;
- Identification of functional areas of the legacy system that are considered good candidates for conversion and those areas that are not considered good candidates, along with reasons why the functional areas are classified as “good” or “not good” candidates for conversion;
- The historical time frame of the data to be converted;
- An assessment of the adequacy and availability of required data based on its location;

Once the Data Conversion Study is completed, the Hexagon and Customer Project Managers, along with the Data Conversion Team, will discuss a schedule for moving forward with data conversion.

Task Deliverables

- OnCall Dispatch Data Conversion Study

Task Prerequisites

- Completion of Project Planning Meeting
- Completion of Project Schedule Review

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Spend one (1) week gathering information necessary to analyze legacy data conversion options; and
- Produce the OnCall Dispatch Data Conversion Study.

Customer Team Participation and Responsibilities

Customer shall:

- Supply a subset of data to the CAD Data Conversion Implementer for use in the analysis and data mapping;
- Ensure SMEs who understand the structure and use of legacy data are available to work with Hexagon for the duration of this task; and
- Provide additional data or scrubbed data based on feedback from Hexagon, if requested.

Task Acceptance Criteria

This Task is considered complete upon delivery of the OnCall Dispatch Data Conversion Study.

9. OnCall Dispatch Data Conversion Scripting

Task Description

The objective of this Task is to create scripts based on the data mapping completed in the Data Conversion Analysis and Mapping Task, run the scripts, reconcile any discovered script discrepancies, and provide feedback to the Customer ("Data Conversion Scripting Feedback"), so it can start making corrections to legacy data necessary to facilitate future data conversion to the Hexagon system. These scripts may include coding to reformat dates and/or parse name and address data but will not include any type of legacy data cleanup, such as reformatting free-form text fields or eliminating duplicate names, which is outside of Hexagon's scope.

Task Deliverables

- OnCall Dispatch data conversion scripts

Task Prerequisites

- OnCall Dispatch Data Conversion Analysis and Mapping Task is complete.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Create and run the OnCall Dispatch data conversion scripts; and
- Provide feedback to the Customer regarding any script discrepancies.

Customer Team Participation and Responsibilities

Customer shall:

- Ensure SMEs who understand the structure and use of legacy data are available to work with Hexagon for the duration of this task.

Task Acceptance Criteria

This Task is considered complete when Hexagon has created the data conversion scripts and provided the Data Conversion Scripting Feedback.

10. OnCall Dispatch Data Conversion Audit

Task Description

The OnCall Dispatch Data Conversion Audit Task focuses on uncovering any legacy data or conversion script issues. Prior to this Task, the Customer will need to provide Hexagon with a sample of legacy data large enough to allow Hexagon and the Customer to perform a quality audit on the imported data. During this Task, Hexagon will convert the representative sample of legacy data into the OnCall Dispatch application.

Task Deliverables

- Vetted scripting process to be used throughout the project

Task Prerequisites

- OnCall Dispatch Data Conversion Scripting Task is complete.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Work with the Customer SMEs to review the converted data in OnCall and revise scripts as necessary to resolve any issues that may arise.

Customer Team Participation and Responsibilities

Customer shall:

- Ensure SMEs who understand the structure and use of legacy data are available to work with Hexagon for the duration of this task.

Task Acceptance Criteria

This Task is considered complete when Hexagon has conducted the OnCall Dispatch data conversion audit.

11. OnCall Records Data Conversion

Task Description

The purpose of this Task is to convert Customer legacy RMS data into OnCall Records. The conversion will be of the following databases and restrictions:

- [redacted]

The conversion will follow a series of sub-tasks, as outlined below. The data conversion, unless otherwise stated, is a single, full dataset run, where the target database (OnCall Records) is purged of all data, prior to the import of the legacy RMS data.

Data Conversion Extraction

The Customer is responsible for the extraction of the data from the current systems into a readable format for the Hexagon-developed data conversion scripts. Upon delivery of all data to be converted, the time necessary for the extraction and delivery should also be given with the data. This information will help aid Hexagon in presenting the total time of conversion that will be used to calculate any outage for the Cutover conversion.

Data Conversion Mapping

Hexagon will conduct a Data Mapping and Analysis with the Customer. Based on the legacy data sets and tables, Hexagon will prepare two (2) documents outlining source and target conversion mappings and will deliver an Expectations Document to further outline the process. These mapping documents and Expectations Document will be signed off by all parties before continuing.

Data Conversion Scripting

Hexagon will create the data conversion scripts required to convert the data into OnCall Records. These scripts will be based on the agreed-upon mapping documents.

Data Conversion Run 1

Hexagon will begin the process by staging the source database(s), and a copy of the OnCall Records database within a CJIS controlled lab. Hexagon will then purge relevant data from the OnCall Records database and execute the developed data conversion scripts, moving the data into the OnCall Records database. This will be done, sequentially for all datasets identified. Data conversion results will be tested and evaluated by Hexagon and Customer for accuracy. Any issues identified will be documented within the tracking system during the period of performance as outlined by the schedule. Additionally initial run times for the conversion will be generated.

Data Conversion Run 2

Hexagon will correct any mutually agreed-upon data conversion issues through script modifications and execute Data Conversion Run 2, following the same process as Data Conversion Run 1. Data conversion results will be tested and evaluated by Hexagon and Customer for accuracy. Any issues identified will be documented within the tracking system during the period of performance as outlined by the schedule. Upon completion, as signoff by all parties will be obtained upon completion. Additionally run times for the conversion will be refined. This data will then be passed to the team to be incorporated into Cutover planning.

Final Run

Hexagon will correct any mutually agreed-upon data conversion issues through script modifications and prepare to execute the Final Data Conversion Run into OnCall Records. This Final Data Conversion Run will be the final run just prior to Cutover.

Task Deliverables

- Data Conversion Expectations Plan
- Data Conversion Mapping Document
- Documentation confirming completion data conversion tasks
- Conversion Run Times Document

Task Prerequisites

- Project Kickoff Meeting Task is complete.

Task Assumptions

- This RMS data conversion includes [redacted]
- No data clean-up or merging of data is part of this Task.
- Attachments are not to be manipulated in any way or converted.
- Attachments may be sourced from a separate network drive or be embedded in the source database. If there are differences, there may be an adjustment in scope.
- The Customer will need to provide expertise on source database. This will include purpose and definition of data elements in the source database to aid in mapping to the appropriate location in the target database.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Conduct the Data Mapping and Analysis;
- Create the data conversion scripts; and
- Conduct Data Conversion Run 1, Run 2, and the Final Run.

Customer Participation and Responsibilities

Customer shall:

- Provide extraction of the data from the current system into a readable format for the Hexagon-developed data conversion scripts;
- Sign off on relevant documents related to conversion plan; and
- Consult with Hexagon regarding any data migration questions.

Task Acceptance Criteria

This Task is complete once the Final Data Conversion Run has been conducted.

Staging Phase

[redacted]

Task Description

[redacted]

Task Deliverables

- [redacted]

Task Prerequisites

- [redacted]
- [redacted]
- [redacted]

Task Assumptions

- [redacted]

Hexagon Team Responsibilities

Hexagon shall:

- [redacted]
- [redacted]

Customer Team Responsibilities

Customer shall:

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted];

[redacted]

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
    - [redacted]
    - [redacted]
  - [redacted]

Task Acceptance Criteria

[redacted]

13. [redacted] and OnCall Software Staging

Task Description

[redacted]

Hexagon will initially confirm the hardware has been configured and set up according to Hexagon standards and able to receive the Software. If deviations are identified, Hexagon will notify the Customer and the Customer will take prompt action to address the deviation.

[redacted]

[redacted]

Hexagon will install and perform initial configuration of the Hexagon OnCall Product Suite included in this Project. [redacted]. Software installed during this Task does not constitute a fully configured system. Additional configuration Tasks are described later in this SOW.

[redacted].

As part of this Task, Hexagon will initiate the Site Configuration document. At this stage this document is a draft that will be updated throughout the Project.

Task Deliverables

- Draft Site configuration Document
- Installation of OnCall Product Suite(s)
- [redacted]
- Ability to login to most of the applications (Some require additional configuration before functional, like OnCall Analytics)

Task Prerequisites

- Customer has completed and returned the Infrastructure Build Document to Hexagon.

- [redacted]
- [redacted]
  - [redacted]
  - [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Task Assumptions

- [redacted]
- [redacted]
- [redacted]
  - [redacted]
  - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]

Hexagon Team Participation and Responsibilities

Hexagon shall:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Customer Team Participation and Responsibilities

Customer shall:

- [redacted]
- Answer questions as needed.
- Promptly address any deviations in hardware, operating system, database software from what is required in Attachment E and F.

Task Acceptance Criteria

This Task is complete when Hexagon has completed the Software Installation and provided the Draft Site Configuration Documentation to Customer.

14. OnCall Dispatch GIS Consulting

Task Description

A central feature of OnCall Dispatch is interoperation and use of Customer provided GIS services within OnCall Dispatch. The Customer may use whichever map provider they choose, subject to Attachment J. The objective of this Task is to collaborate with the Customer's GIS Administrator regarding use of the Customer-provided map services within OnCall Dispatch and management of the source map.

Over the course of up to three (3) consecutive weeks ("GIS Consulting Period") a Hexagon technical resource will host meetings with the Customer GIS Administrator and any other interested Customer SMEs, which in the aggregate shall last no more than twenty-four (24) Business Hours ("GIS Meeting Time"). The OnCall Dispatch GIS Consulting is intended to be a collaborative session and for Hexagon and the Customer GIS Administrator to discuss use of the map services within OnCall Dispatch and management of the map services in the context of OnCall Dispatch. As time permits, the parties can discuss other GIS related topics.

To facilitate a productive session, the Customer GIS Administrator, at a minimum, should have participated in the OnCall Dispatch GIS Requirements Review. The Customer shall also have complied with the mapping requirements prior to this Task.

As a result of the sessions, the Customer's GIS Administrator will have been provided additional insight and information on how to manage and use the map services in connection with OnCall Dispatch. For purposes of clarity, these sessions are not intended to result in configuration or modification of Customer's source map data. The Customer may configure the map services at its discretion up to the commencement of Functional Testing. At the commencement of Functional Testing, the Customer shall refrain from making any modification or configurations to the map services until after System Cutover.

Task Prerequisites

- OnCall Dispatch GIS Requirements Review Task is complete.

Task Assumptions

- The Customer GIS Administrator has sufficient authority to make decisions about the use, configuration, and integration of the source map data.
- Hexagon will not provide training or services specific to Esri software.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Conduct the GIS Consulting through a Hexagon technical resource.

Customer Team Participation and Responsibilities

Customer shall:

- Manage and make any desired configurations to the Customer-provided map data; and
- Ensure appropriate GIS resources attend GIS consulting session(s).

Task Acceptance Criteria

This Task is complete upon the earlier of: (i) use of all of the GIS Meeting Time or (ii) end of the GIS Consulting Period.

15. OnCall Records State NIBRS Validation Installation

Task Description

During this Task, Hexagon resources will upgrade the NIBRS validation changes to reflect state validations.

Task Deliverables

- Hexagon installation of the state-specific NIBRS validations

Task Prerequisites

- [redacted] and OnCall Software Staging Task is complete.
- Hexagon has completed any state-mandated changes on validations to core Federal IBRS product.

Task Assumptions

- N/A

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Install and test State NIBRS validations; and
- Support Customer testing and provide resolution of Blocker Defects.

Customer Team Participation and Responsibilities

Customer shall:

- Conduct testing and report any Blocker Defects back to each parties' representative via Hexagon's Customer Resource Management (CRM) issue tracking system within ten (10) Business Days of receiving notification from Hexagon that the software is ready for testing.

Task Acceptance Criteria

This Task is complete when the current version of State NIBRS has been installed.

16. OnCall Records Address Server Mapping Configuration

Task Description

During this Task, Hexagon will configure the OnCall Records Address Server components for OnCall Records and conduct the Address Server Mapping Review ("Address Server Review").

OnCall Records utilizes the native Esri GIS data files processed by the OnCall Records Address Server for geo-validation, standardization, and reverse geo-coding. The OnCall Records Address Server supports street centerline files, commonplace data, and address point information for geo-verification. OnCall Records does not directly synchronize with the maps used within the Customer's CAD solution because additional Location attributes and information may be obtained and captured within OnCall Records for a valid location (e.g., District, Post, Beat, Neighborhood, Community, Quadrants, etc.). The Address Server provides the ability to reverse geo-code a valid location to retrieve these additional data elements.

The Address Server Review is intended to cover the mapping attributes needed for OnCall Records, where the information will be pulled from, and necessary map layers and geocode conversions. The Address Server Review shall last no more than four (4) Business Days. The Customer shall ensure appropriate GIS personnel attend the Address Server Review. As may be requested during and outside of the Address Server Review, Customer shall provide assistance to Hexagon in the configuration of the Address Server within the Customer's environment.

Task Deliverables

- COTS OnCall Records Address Server configuration
- Address Server Review

Task Prerequisites

- [redacted] and OnCall Software Staging Task is complete.
- OnCall Dispatch GIS Requirements Review Task is complete.

Task Assumptions

- This workshop provides for a maximum of six (6) Core Team Members.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Conduct the Address Server Review;
- Configure and test the OnCall Records Address Server component; and
- Validate the COTS Address Server Configuration.

Customer Team Participation and Responsibilities

Customer shall:

- Ensure necessary GIS personnel (and others as needed) attend the Address Server Review;
- Identify and set up appropriate facilities for the Address Server Review; and
- Assist Hexagon with the Address Server configuration preparation.

Task Acceptance Criteria

This task is complete when the OnCall Records Address Server has been configured and the Address Server Review has been conducted.

17. OnCall Dispatch System Build 1

Task Description

OnCall Dispatch System Build 1 workshop ("System Build 1") builds upon the OnCall Dispatch and Mobile Unit Launch to begin the process of populating OnCall with required static data elements. System Build 1 is the first of two (2) static data workshops and primes OnCall Dispatch with base data to support the buildout of remaining static data elements addressed in OnCall Dispatch System Build 2 and the OnCall Dispatch Deployment & Response Planning Workshop.

At the commencement of System Build 1, the Customer shall have obtained information and documents (e.g., records, operating procedures, resources, etc.) to support the eventual entry or import of the Build 1 Data Elements. For any Build 1 Data Elements not entered or imported during System Build 1, the Customer will enter those after System Build 1 within ten (10) Business Days and prior to OnCall Dispatch System Build 2.

During System Build 1, the focus will be on the entry and import of Build 1 Data Elements (as defined below). System Build 1 will last no longer than three (3) Business Days. As part System Build 1, the Customer will be instructed in the use of OnCall Dispatch Administrator to facilitate the manual entry of static data elements. This instruction is critical to provide an understanding of the process of creating and managing static data and the relationships between static data elements. Some manual entry of all static data elements is required as part of the workshop. Bulk import of remaining data can occur after sufficient understanding of the data elements and relationships is obtained.

Following System Build 1, OnCall Dispatch will have foundational data elements to support future build activities.

Task Deliverables

- OnCall Dispatch System Build 1 workshop

Task Prerequisites

- OnCall Dispatch & Mobile Unit Launch Task is complete.
- [redacted] and OnCall Software Staging Task is complete.
- OnCall Dispatch GIS Consulting Task is complete.
- Initial GIS services published and configured for use by OnCall Dispatch:
  - Map display
  - Routing
  - Geocoding

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.
- System Build 1 is conducted using the Customer's OnCall Dispatch environment.
- System Build 1 will last no more than three (3) Business Days.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Host System Build 1 during which, limited, focused instruction on the use of OnCall Dispatch, OnCall Mobile Unit, and OnCall Dispatch Administrator, on functional areas that utilize or display the following static data elements (“Build 1 Data Elements”):
  - Agencies
  - Unit Types (Patrol, Engine, etc.)
  - Units
  - Event Types
  - Disposition Codes
  - Out-of-Service Types
  - Facility Service Types
  - Known Caller Types
  - Special Situation Types
  - Personnel/User Accounts
  - Beats/Station Areas
  - Dispatch Groups
  - Stations (Police Stations, Sub-Stations, Fire Stations, etc.)
  - Number Formats (event, case, etc.)
  - Rotational Services (towing, ambulance, lock smith, etc.)
  - Vehicles
- Provide the Customer with Microsoft Excel based data collection spreadsheets to be used in assembling the Build 1 Data Elements for importation into the Dispatch Subsystem.

Customer Participation and Responsibilities

Customer shall:

- Ensure appropriate Dispatch and Mobile Core Team members attend and actively participate during the System Build 1 for the entire duration;
- Provide a Facility;
- Provide a Project Workstation to each attendee;
- Provide all necessary information and documents to facilitate importation of Build 1 Data Elements at the outset of System Build 1; and
- Participate in discussions and engage with the Hexagon team member.

Task Acceptance Criteria

This Task is complete upon conclusion of System Build 1.

18. OnCall Dispatch Deployment & Response Planning Workshop

Task Description

This workshop, “Deployment and Response Planning Workshop,” builds upon System Build 1 to begin the process of creating the deployment and response planning components of OnCall Dispatch. The Deployment and Response Planning Workshop is intended to facilitate importation with deployment data necessary to successfully execute the OnCall Dispatch System Build 2 and the subsequent OnCall Dispatch configuration workshops.

As part of the Deployment and Response Planning Workshop, Customer will be taught about the OnCall Dispatch deployment model which details how OnCall Dispatch determines responding agencies for events. Customer will also be taught about the OnCall Dispatch unit recommendation model, how to build response plans, and briefed on the parameters which control how OnCall Dispatch processes response plans. The Deployment and Response Planning Workshop shall last no longer than three (3) Business Days. At the outset of Deployment and Response Planning Workshop, the Customer must have obtained and have necessary information and documents to facilitate eventual creation of the Deployment Plans, and Response Plans (as defined below). The Deployment and Response Planning Workshop is intended to provide the Customer experience on how to build Deployment Plans and Response Plans; it is not expected or intended that all such Deployment Plans and Response Plans will be completed during the Deployment and Response Planning Workshop. The Customer will be expected to complete the build of any necessary Deployment Plans and Response Plans within ten (10) Business Days prior to the commencement of System Build 2.

Task Deliverables

- OnCall Dispatch Deployment & Response Planning Workshop

Task Prerequisites

- OnCall Dispatch System Build 1 Task is complete.
- Necessary Build 1 Data Elements have been imported into the Dispatch Subsystem to facilitate the build of Deployment Plans and Response Plans.

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.
- Workshop is conducted using the Customer’s OnCall environment.
- Deployment and Response Planning Workshop shall last no longer than (3) Business Days.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide formal instruction on the OnCall Dispatch deployment model (“Deployment Plans”):
  - Deployment plans
  - Emergency Service Zones
  - Beats & Backup Beats
  - Dispatch Groups
- Provide formal instruction on the OnCall Dispatch response planning model (“Response Plans”):
  - Recommend unit service:
    - Number of recommend unit services needed

        - Recommend search area
        - Recommend method (beats, street network, closest)
        - Recommend unit parameters
      - Response plans:
        - Requirements
        - Requirement Groups
        - Conditions
        - Nested plans
- Support Customer buildout of deployment and response plans.

Customer Participation and Responsibilities

Customer shall:

- Provide a Facility;
- Provide a Project Workstation for each attendee;
- Ensure appropriate Dispatch and Mobile Core Team members attend and actively participate during the Deployment and Response Workshop over the entire duration;
- Bring maps, documents, or other materials that detail the agency deployment model(s) and Deployment Plans;
- Bring materials that document or detail the agency unit recommendation model(s) and Response Plans; and
- Build deployment and response plans with Hexagon guidance during the Deployment and Response Planning Workshop and independently following Deployment and Response Planning Workshop.

Task Acceptance Criteria

This Task is complete at the conclusion of the Deployment and Response Planning Workshop.

19. OnCall Dispatch System Build 2

Task Description

This OnCall Dispatch System Build 2 Workshop ("System Build 2") finalizes Hexagon-led system build activities and completes the enablement of the Dispatch and Mobile Core Teams to continue build related activities for the remainder of the project. The same Dispatch and Mobile Core Team members who participated in System Build 1 and the Deployment and Response Planning Workshop shall attend System Build 2 to ensure continuity of decisions and facilitating continuing to build upon previous workshops.

Additionally, System Build 2 focuses on reviewing data entered into the Subsystem for level of completion and analyzing whether data was entered/imported correctly. New topics to be covered as part of System Build 2 are contact directory, message groups, message templates, lineups, ORIs, special addresses, and common place names. System Build 2 shall last no longer than three (3) Business Days. While certain updates or modifications to the static data may occur during the Configuration Phase, the Customer shall upload all of its static data within ten (10) Business Days following System Build 2.

Task Deliverables

- OnCall Dispatch System Build 2 Workshop

Task Prerequisites

- OnCall Dispatch Deployment & Response Planning Workshop Task is complete.

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.
- Workshop is conducted using the Customer's OnCall environment.
- System Build 2 will last no more than three (3) Business Days.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Load deployment polygons into the OnCall Dispatch database;
- Provide support to Customer teams while continuing the system build efforts;
- Review with the Customer teams the data entered to date for accuracy and level of completion; and
- Provide feedback on the build progress and areas that need focus or attention.

Customer Participation and Responsibilities

Customer shall:

- Provide a Facility;
- Provide a Project Workstation for each attendee;
- Ensure past participants in System Build 1 and Deployment and Response Workshop attend System Build 2 for the entire duration;
- Provide at the outset of System Build 2 all necessary information and documents to: facilitate review of Build 1 Data Elements, Response Planning Parameters, Deployment Parameters, and new elements stated above;

- Participate in discussions and engage with the Hexagon team member;
- Complete any outstanding entry or import of static data within ten (10) Business Days following the end of System Build 2.

Task Acceptance Criteria

This Task is complete upon conclusion of System Build 2.

Configuration Phase

20. OnCall Dispatch Fundamentals for Core Team

Task Description

The OnCall Dispatch Fundamentals for Core Team course is presented directly to Dispatch and Mobile Core Team personnel to provide complete instruction on the use of the OnCall Dispatch and Mobile Unit applications. The course shall last no longer than four (4) Business Days. This course is intended to instruct the Dispatch and Mobile Core Teams with the features of OnCall Dispatch and Mobile Unit, including event processing and dispatching, map utilization, and inquiries. The following major topics will be reviewed, as applicable:

HxGN OnCall Dispatch | Advantage functions:

- Event Creation and Updates
- Map View Control
- Inquiries
- Messaging
- Recommending and Dispatching Units
- Updating Unit Statuses and Properties
- HxGN OnCall Dispatch | Mobile Unit functions:
  - Accessing the system
  - Event Updates
  - Unit Status Changes
  - Messaging

Task Deliverables

- OnCall Dispatch Fundamentals for Core Team course

Task Prerequisites

- System Build 2 is complete.
- Completion by Customer attendees of an introductory Microsoft Windows course or equivalent knowledge and familiarity with the Microsoft Windows user interface.

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.
- The course shall last no longer than three (4) Business Days.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Conduct OnCall Dispatch Fundamentals for Core Team course.

Customer Team Participation and Responsibilities

Customer shall:

- Provide a Facility;
- Provide a Project Workstation for each attendee;
- Ensure appropriate personnel who have attended an introductory MS Windows course, or have comparable education, training, or experience, participate fully and collaboratively in the session;

- Designate the Dispatch and Mobile Core Team members for attendance and ensure those same participants participate in subsequent Dispatch and Mobile configuration and testing Tasks;
- Provide sufficient copies of the training materials supplied by Hexagon to support all students in the Core Team Training;
- Ensure that all training workstations and servers are operational prior to the agreed start of training classes; and
- Provide internal training to users that are unable to attend the Hexagon-provided training.

Task Acceptance Criteria

This Task is complete upon delivery of the OnCall Dispatch Fundamentals for Core Team course.

21. COTS Interface Product Installation and Configuration

Task Description

During this Task, Hexagon will install and unit test the COTS Interfaces in the Customer's Production Environment. Hexagon will be able to install the COTS Interface and configure it based upon the information provided in the COTS Interface Questionnaire subject to the functionality and features existing within the COTS version of the COTS Interface. To facilitate Hexagon's implementation and configuration of the COTS Interfaces, the Customer shall make available or provide access to all third party software components which are intended to integrate with the Dispatch Subsystem through the COTS Interface(s).

Although the Customer is expected to participate in Hexagon's internal testing of the COTS Interfaces, the Customer will formally test interface functionality during Functional Testing Task.

Task Deliverables

- Installation and configuration of the COTS Interfaces which are listed in the COTS Interface Questionnaire Completion Task above.

For more information on the COTS Interfaces, see Attachment H, Interface Descriptions.

Task Prerequisites

- Operation or availability of all external systems or Third-Party Software.
- Completed COTS Interface Questionnaires provided to Hexagon during the COTS Interface Review Period.
- [redacted] and OnCall Software Staging Task is complete.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Install COTS Interfaces in the Customer's Production and Disaster Recovery Environments; and
- Unit test interfaces in accordance with the COTS Interface Questionnaires.

Customer Team Participation and Responsibilities

Customer shall:

- Ensure SMEs are available to support Hexagon Activities as needed;
- Verify that physical connectivity and communication has been achieved from Customer's Communication/Interface server to remote system servers and all other third-party systems (such as Customer message switch(es), State/NCIC, RMS systems etc.);
- Provide availability and confirm operation of external systems or third-party software;
- Provide the following information to Hexagon:
    - IP address for remote databases/systems
    - Socket value for remote databases/systems
    - Enter operator IDs (ORIs), terminal mnemonics, etc., as needed by remote databases/systems

- Ensure the system and network administrators are available to work closely with the Hexagon team for the duration of the Task; and
- Ensure third-party cooperation with Hexagon's reasonable requests.

Task Acceptance Criteria

This Task is complete when each COTS Interface is installed and configured in accordance with the COTS Interface Questionnaire, and subject to the functionality and features within the COTS version of the COTS Interface.

22. CommSys ConnectCIC Installation

Task Description

During this Task, Hexagon will utilize the CommSys ConnectCIC State Interface middleware product to interface with the state message switch for the following state and national transactions. The CommSys ConnectCIC middleware product will work with the Customer's Informer interface to support the transactions listed below.

- Person (In State and NLETS) (QW, DQ, QM)
    - Wanted/Warrants
    - Missing
    - Driver's license
- Vehicle (In State and NLETS) (QV, RQ)
    - Wanted/stolen
    - Registration
    - Vehicle Parts
- Gun by (serial, caliber, make) (QG)
- Article (serial, type) (QA)
- Boat (In State and NLETS) (QB, BQ)
    - Hull Number
    - Registration ID
- Hazmat (MQ)
- Administrative Message (AM)
- Canadian Queries
    - Person Driver's License/Want (WQ, UQ)
    - Vehicle Registration/Want (VQ, XQ)
    - Boat by License, Hull, Registration (CBQ)
    - Gun by Serial (CGQ)
    - Article by Serial (CAQ)
- Secondary Person (Nested Query)
- Surrounding States Parsing
- Enter, Modify, Locate, Cancel, Clear
    - Person
    - Vehicle
    - Gun
    - Article

HxGN OnCall Dispatch | Informer Interface will support the queries to NCIC (via CommSys ConnectCIC) from Dispatch and Mobile Unit.

Task Deliverables

- CommSys ConnectCIC setup and installation

Task Prerequisites

- COTS Interface Product Installation and Configuration Task is complete.

Task Assumptions

- Primary agency shall be the Customer.
    - Williamson County Emergency Communications Center
- The supported transactions include basic queries.
- This Project does not include the development of any new forms, queries, or transactions for Informer unless specifically identified herein.
- Additional agencies that may initiate queries:
    - Williamson County Sheriff's Office
    - Hutto Police Department
    - Liberty Hill Police Department
    - Granger Police Department
    - Thrall Police Department
    - Jarrell Police Department
    - Florence Police Department
    - Liberty Hill School Police Department
    - Round Rock ISD Police Department
    - Constables Pct 1
    - Constables Pct 2
    - Constables Pct 3
    - Constables Pct 4
    - Hutto ISD Police Department
    - Jarrell ISD Police Department
    - Haz Mat Fire Marshall
- First year maintenance for CommSys ConnectCIC shall begin upon Cutover.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Ensure CommSys has installed ConnectCIC State Interface middleware; and
- Work with CommSys to verify the ConnectCIC State Interface middleware product is set up and installed for the Customer agencies listed above.

Customer Team Participation and Responsibilities

Customer shall:

- Ensure that documentation detailing the format, development\design, and connection information (IP, protocol, credentials, etc.) is current and provided to Hexagon either by the State or by Customer. If this information is not provided by the State, Customer is responsible for collecting and determining if this information is valid and providing it to Hexagon. If the documentation is not provided to Hexagon, additional services\charges may be incurred by Customer;
- Have CJIS-related security in place as it relates to Informer data, transactions, and responses;
- Provide points of contact who are knowledgeable of the workflow and data requirements for Customer hardware and software components with which Hexagon deliverables will interface;
- Provide test connections to State/NCIC, as well as other external systems required for the Project;
- Provide live connections to State/NCIC, as well as other external systems required for the Project;
- Enter associated ORI, user credentials (if applicable), and terminal mnemonics;
- Provide test records to ensure that the transactions received by the System in a test environment are in the same format and contain the same information as those received in a Production environment; and
- Test and report any Defects to Hexagon within ten (10) Business Days of installation of ConnectCIC in Customer's environment.

Task Acceptance Criteria

This Task is complete upon installation of the CommSys ConnectCIC product.

23. OnCall Dispatch Configuration Consulting 1

Task Description

The primary purpose of OnCall Dispatch Configuration Consulting is to teach the Customer how to use the features of OnCall Dispatch Administrator related to configuration. This includes the User Interface Editor, the Layout Manager, and Configuration Parameters. The Customer is solely responsible for completing all desired configurations of OnCall Dispatch and OnCall Mobile Unit necessary to achieve the Customer's desired outcomes. Hexagon provides direct support in a time-boxed method as described in this task.

During this Task, Hexagon will conduct the "Configuration 1 Workshop," which will last no longer than three (3) Business Days. Hexagon will provide support for the Customer's configuration activities for up to three (3) Business Days following the Configuration 1 Workshop ("Configuration 1 Period"). During the Configuration 1 Workshop, Hexagon and Customer will work collaboratively with one another to configure the Basic Settings, Viewing Settings, Call Taking Process Settings, Event Creation Settings, and UI Layouts (as defined below) with Hexagon providing instruction and guidance and the Customer executing the desired configuration changes.

Up to the end of the Configuration 1 Period, Hexagon will support the Customer's effort to configure the Configuration 1 Settings (as defined below) and subject to the Benchmark Criteria. After the Configuration 1 Period has expired, the Customer will be responsible for working independently on making any configuration changes to the Configuration 1 Settings that were not otherwise completed during the Configuration 1 Period or that Customer seeks to further configure. Scope of the configuration is limited to the capabilities described in the Benchmark Criteria. Not all requested product configuration may be possible.

Task Deliverables

- OnCall Dispatch Configuration 1 Workshop

Task Prerequisites

- Customer's OnCall Dispatch Subsystem is available for use.
- Initial GIS services published and configured for use by OnCall Dispatch:
  - Base Map display
  - Routing
  - Geocoding
- OnCall Dispatch Fundamentals for Core Team Task is complete.

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.
- The Configuration 1 Workshop will last no longer than three (3) Business Days.
- The Configuration 1 Workshop will be interactive with up to twelve (12) Customer attendees for up to seven (7) Business Hours per day.
- Customer Dispatch Core Teams will record the list of requested configurations from each day, placing them in order of priority to be completed.
- Requested configurations to the Configuration 1 Settings not completed by the end of the Configuration 1 Period can be independently completed by the Customer, if so desired, which must be done prior to Configuration 2 Workshop.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide consulting and configuration services to review (collectively, “Configuration 1 Settings”):
  - Customer’s preferences for basic settings, including but not limited to (collectively, “Basic Settings”):
    - Colors for unit statuses
    - Colors for event priorities
    - Icons for event types on the map and event cards/boards
    - Icons for unit types
  - Customer’s needs for viewing event and unit related data in real-time lists (status monitors) (collectively, “Viewing Settings”):
    - Filters
    - Visible columns
    - Context (right-click) menus
  - Customer’s emergency and non-emergency call-taking processes, including but not limited to (collectively, “Call Taking Process Settings”):
    - Location validation
    - Event-type selection
    - Jurisdiction determination
  - Customer’s event creation processes, including but not limited to (collectively, “Event Creation Settings”):
    - Single Agency Response
    - Multiple Agency Response
    - Nearby or possible duplicate detection
  - User Interface Layouts (“UI Layouts”)

Customer Participation and Responsibilities

Customer shall:

- Provide a Facility;
- Provide a Project Workstation for each attendee;
- Ensure the attendance and active participation of the Dispatch Core Team members and other SMEs for the duration of the Configuration 1 Workshop;
- Participate in discussions and engage with the Hexagon team member;
- Track and prioritize requests for configuration of the Configuration1 Settings on a daily basis during the Configuration 1 Workshop; and
- Complete any changes to Configuration 1 Settings prior to the commencement of Configuration 2 Workshop.

Task Acceptance Criteria

This Task is complete upon: (i) the conclusion of the Configuration 1 Workshop and (ii) upon the earlier of, expiration of the Configuration 1 Period or configuration of the Configuration 1 Settings.

24. OnCall Dispatch Configuration Consulting 2

Task Description

The primary purpose of OnCall Dispatch Configuration Consulting is to teach the Customer how to use the features of OnCall Dispatch Administrator related to configuration. This includes the User Interface Editor, the Layout Manager, and Configuration Parameters. The Customer is solely responsible for completing all desired configurations of OnCall Dispatch and OnCall Mobile Unit necessary to achieve the Customer's desired outcomes. Hexagon provides direct support in a time-boxed method as described in this Task.

During this Task, Hexagon will conduct the "Configuration 2 Workshop", which will last no longer than three (3) Business Days. Hexagon will provide support for the Customer's configuration activities for up to three Business Days following the Configuration 2 Workshop ("Configuration 2 Period"). During the Configuration 2 Workshop, Hexagon and Customer will work collaboratively with one another to configure the Configuration 2 Settings (as defined below) with Hexagon providing instruction and guidance and the Customer executing the desired configuration changes.

Up to the end of the Configuration 2 Period, Hexagon will support the Customer's effort to configure the Configuration 2 Settings (as defined below) and subject to the Benchmark Criteria. After the Configuration 2 Period has expired, the Customer will be responsible for working independently on making any configuration changes to the Configuration 2 Settings that were not otherwise completed during the Configuration 2 Period or that Customer seeks to further configure. Scope of the configuration is limited to the capabilities described in the Benchmark Criteria. Not all requested product configuration may be possible.

Task Deliverables

- OnCall Dispatch Configuration 2 Workshop

Task Prerequisites

- Configuration 1 Workshop and Configuration 1 Period are complete, and Customer has completed any and all additional configurations to the Configuration 1 Settings.
- Connection established to Customer's state crime system.

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.
- Configuration 2 Workshop will last no more than three (3) Business Days.
- The Configuration 2 Workshop will be interactive with Customer attendees for up to seven (7) Business Hours per day.
- Customer Dispatch Core Team will record the list of requested configurations from each day, placing them in order of priority to be completed.
- Requested configurations to the Configuration 2 Settings not completed by the end of the Configuration 2 Period can be completed by the Customer, if so desired, which must be done prior to Configuration 3 Workshop.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide consulting and configuration services to review the settings below (collectively, "Configuration 2 Settings"):

- Customer's event triage and dispatching processes
- Customer's event management processes, including but not limited to:
  - Unit recommendation & assignment
  - Unit on event management
  - Unit location changes
  - Staging areas
  - Case numbers
  - Remote inquiries
  - Queued events
  - Rotational services (e.g., Tow trucks, lock smiths, etc.)
- Call back process
- Known callers
- Unit relocation (a.k.a. Move Ups)
- Shared Crews (a.k.a. Cross-staffing)
- Field Events (a.k.a. Officer Initiated Events)
- Associated Events
- Copied Events

Customer Participation and Responsibilities

Customer shall:

- Provide a Facility;
- Provide a Project Workstation for each attendee;
- Ensure the attendance and active participation of the Dispatch Core Team members and other SMEs for the duration of the Configuration 2 Workshop;
- Participate in discussions and engage with the Hexagon team member;
- Track and prioritize requests for configuration of the Configuration 2 Settings on a daily basis during the Configuration 2 Workshop; and
- Complete any configurations changes to the Configuration 2 Settings prior to the commencement of Configuration 3 Workshop.

Task Acceptance Criteria

This Task is complete upon: (i) the conclusion of the Consulting 2 Workshop and (ii) upon the earlier of, expiration of the Configuration 2 Period or configuration of the Configuration 2 Settings.

25. OnCall Dispatch Configuration Consulting 3

Task Description

The primary purpose of OnCall Dispatch Configuration Consulting is to teach the Customer how to use the features of OnCall Dispatch Administrator related to configuration. This includes the User Interface Editor, the Layout Manager, and Configuration Parameters. The Customer is solely responsible for completing all desired configurations of OnCall Dispatch and OnCall Mobile Unit necessary to achieve the Customer's desired outcomes. Hexagon provides direct support in a time-boxed method as described in this task.

During this Task, Hexagon will conduct the "Configuration 3 Workshop", which will last no longer than three (3) Business Days. Hexagon will provide support for the Customer's configuration activities for up to three Business Days following the Configuration 3 Workshop ("Configuration 3 Period"). During the Configuration 3 Workshop, Hexagon and Customer will work collaboratively with one another to configure the Configuration 3 Settings (as defined below) with Hexagon providing instruction and guidance and the Customer executing the desired configuration changes.

Up to the end of the Configuration 3 Period, Hexagon will support the Customer's effort to configure the Configuration 3 Settings (as defined below) and subject to the Benchmark Criteria. After the Configuration 3 Period has expired, the Customer will be responsible for working independently on making any configuration changes to the Configuration 3 Settings that were not otherwise completed during the Configuration 3 Period or that Customer seeks to further configure. Scope of the configuration is limited to the capabilities described in the Benchmark Criteria. Not all requested product configuration may be possible. The Customer shall complete any desired configurations prior to the commencement of Customer Functional Testing Task.

Task Deliverables

- OnCall Dispatch Configuration 3 Workshop

Task Prerequisites

- Configuration 2 Workshop and Configuration 2 Period have been completed, and Customer has completed any additional configurations to the Configuration 2 Settings.

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.
- The Configuration 3 Workshop will last no more than three (3) Business Days.
- The Configuration 3 Workshop will be interactive with Customer attendees for up to seven (7) hours per day.
- Dispatch Core Team will record the list of requested configurations from each day, placing them in order of priority to be completed.
- Requested configurations not completed upon consumption of all allocated labor hours can be completed by the Customer, if so desired, which must be done prior to the commencement of Customer Functional Testing.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide consulting and configuration services ("Configuration 3 Settings") to review:
    - Biased based profiling data collection

- Notifications
- Standard Operating Procedures (SOPs)
- Event Tags
- Special Situations
- Event Security
- Unit Management
  - Logging on
  - Logging off
  - Unit properties
  - Logon Group (Lineup)
- CAD Searches
  - Event search
  - Unit history search
  - Equipment Search
- Broadcasts (a.k.a. BOLOs)

Customer Participation and Responsibilities

- Provide a Facility;
- Provide a Project Workstation for each attendee;
- Ensure the attendance and active participation of the Dispatch Core Team members and other SMEs for the duration of the Configuration 3 Workshop;
- Participate in discussions and engage with the Hexagon team member;
- Track and prioritize requests for configuration of the Configuration 3 Settings on a daily basis during the Configuration 3 Workshop; and
- Complete any configurations changes prior to the commencement of Customer Functional Testing.

Task Acceptance Criteria

This Task is complete upon: (i) the conclusion of the Consulting 3 Workshop and (ii) upon the earlier of, expiration of the Configuration 3 Period or configuration of the Configuration 3 Settings.

26. OnCall Dispatch | Smart Advisor Workshop

Task Description

During the Smart Advisor Workshop, Hexagon will provide limited instruction on the use of OnCall and Smart Advisor and the use of the Smart Advisor configuration tools.

Task Deliverables

- Smart Advisor Workshop

Task Prerequisites

- OnCall Dispatch Configuration Consulting 3 Task is complete.

Task Assumptions

- Customer attendees are familiar with OnCall Dispatch.
- Each Customer attendee will have access to their own Project Workstation.
- The Smart Advisor Workshop shall last no more than one (1) Business Day.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide limited, focused instruction on the use of OnCall Dispatch and Smart Advisor Agents on functional areas such as:
    - Fine-tuned alerts and notifications

Customer Participation and Responsibilities

Customer shall:

- Provide a Facility;
- Provide a Project Workstation for each attendee;
- Ensure appropriate members of the Dispatch Core Team attend the workshop; and
- Participate in discussions and engage with the Hexagon team member.

Task Acceptance Criteria

This Task is complete upon conclusion of the Smart Advisor Workshop.

27. OnCall Dispatch | Customer Rules Engine Configuration Workshop

Task Description

The objective of this Task is to familiarize the Customer with configurability of the OnCall Dispatch | Customer Rules Engine (CRE), an add-on component to the HxGN OnCall Dispatch product suite. CRE allows customized business rules to be created using a drag-and-drop editor. The customized business rules can be used to implement workflows that are specific to a particular customer and therefore not available out-of-the-box in the core HxGN OnCall Dispatch product suite.

The Customer is responsible for configuring CRE. Hexagon will provide specific consulting sessions as part of the Project, but the Customer Core Team's understanding of configuration will correspondingly allow the Customer to use CRE to create custom workflows. Hexagon will also provide an example of how to implement a CRE-based configuration in the Customer's Environment.

Hexagon will conduct a workshop ("CRE Workshop") to familiarize the Customer with CRE, provide an example of a CRE configuration, and, if time permits, begin working on implementing CRE-based configurations. The CRE Workshop shall last no more than three (3) Business Days. Any CRE-based configuration not completed at the end of the CRE Workshop shall be the responsibility of Customer. The Customer shall complete configuration of CRE within ten (10) Business Days after the CRE Workshop (the "CRE Configuration Period"). If the Customer has questions as it configures CRE, it may contact Hexagon to address the question.

Task Deliverables

- CRE Workshop

Task Prerequisites

- OnCall Dispatch Configuration Consulting 3 Task is complete.

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.
- Attendance by the Customer's personnel will be limited to no more than twelve (12) people and must consist of field users and stakeholders capable of making finalized decisions about configurations within OnCall Dispatch.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Conduct the CRE Workshop; and
- Provide support (question and answer support) as Customer configures CRE.

Customer Team Participation and Responsibilities

Customer shall:

- Provide a Facility;
- Provide a Project Workstation for each attendee;
- Ensure appropriate personnel attend, and fully participate in all the CRE Workshop;
- Provide department-specific CAD configuration and workflow data as needed; and
- Configure CRE within the CRE Configuration Period.

Task Acceptance Criteria

This Task is considered complete when Hexagon has conducted the CRE Workshop.

28. OnCall Dispatch | Mobile Unit Configuration Consulting Session – Law

Task Description

Hexagon will conduct one (1) consulting session with the Customer lasting no more than three (3) Business Days as part of the Project ("Mobile Unit Law Configuration Session"). During the Mobile Unit Law Configuration Session, Hexagon will provide information regarding configuration options for Mobile Unit workflows as they pertain to the mobile environment. The Mobile Unit Law Configuration Session will address:

- Sign on/Sign off
- Brief Overview of Application
- Screen Layout
- Navigation Buttons
- Alerts
- Toolbars
- Event Search
- Menus and Submenus
- Map
- Messaging
- Unit Board
- Event Board
- The included Dispatch Report
- Network requirements and ports to ensure the Mobile Unit client can communicate appropriately

The Customer will need to make available one dispatcher familiar with OnCall Dispatch to perform dispatching and other related tasks as necessary during the Mobile Unit Law Configuration Session.

Following the Mobile Unit Law Configuration Session, the Customer will configure Mobile Unit during the next ten (10) Business Days ("Mobile Unit Law Configuration Period"). Hexagon will provide remote support for the Customer's Mobile Unit Law configuration efforts ("Mobile Unit Law Configuration Consultation") up to a maximum of two (2) Business Days.

The Customer is responsible for configuring the Mobile Unit subsystem. Upon completion of this Task, the Customer will have one (1) mobile configuration of Mobile Unit for testing.

Task Deliverables

- OnCall Dispatch | Mobile Unit Law Configuration Session
- OnCall Dispatch | Mobile Unit Law Configuration Consultation

Task Prerequisites

- OnCall Dispatch Configuration Consulting 3 Task is complete.

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.

- Attendance by the Customer's personnel will be limited to no more than twelve (12) people and must consist of field users and stakeholders capable of making final decisions about product behavior and functionality.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Conduct one (1) instance of Mobile Unit Law Configuration Session and the Mobile Unit Law Configuration Consultation.

Customer Team Participation and Responsibilities

Customer shall:

- Provide a Facility;
- Provide a Project Workstation for each attendee;
- Provide mobile SME to support Hexagon as needed;
- Provide a Dispatcher SME to give feedback on how Mobile Unit will affect dispatchers and to assist with various dispatching Activities;
- Participate fully and collaboratively in the Mobile Unit Law Configuration Session with the understanding that Mobile Unit client configuration decisions must be documented and agreed upon at the conclusion of these sessions;
- Configure Mobile Unit during the Mobile Unit Law Configuration Period; and
- Begin the Mobile Unit Law Configuration Document.

Task Acceptance Criteria

The Task is complete when Hexagon has conducted the Mobile Unit Law Configuration Session and the Mobile Unit Law Configuration Consultation.

29. OnCall Dispatch | Mobile Unit Configuration Consulting Session – Fire

Task Description

Hexagon will conduct one (1) consulting session with the Customer lasting no more than three (3) Business Days as part of the Project (“Mobile Unit Fire Configuration Session”). During the Mobile Unit Fire Configuration Session, Hexagon will provide information regarding configuration options for Mobile Unit workflows as they pertain to the mobile environment. The Mobile Unit Fire Configuration Session will address:

- Sign on/Sign off
- Brief Overview of Application
- Screen Layout
- Navigation Buttons
- Alerts
- Toolbars
- Event Search
- Menus and Submenus
- Map
- Messaging
- Unit Board
- Event Board
- The included Dispatch Report
- Network requirements and ports to ensure the Mobile Unit client can communicate appropriately

The Customer will need to make available one dispatcher familiar with OnCall Dispatch to perform dispatching and other related tasks as necessary during the Mobile Unit Fire Configuration Session.

Following the Mobile Unit Fire Configuration Session, the Customer will configure Mobile Unit during the next ten (10) Business Days (“Mobile Unit Fire Configuration Period”). Hexagon will provide remote support for the Customers Mobile Unit Fire configuration efforts (“Mobile Unit Fire Configuration Consultation”) up to a maximum of two (2) Business Days.

The Customer is responsible for configuring the Mobile Unit subsystem. Upon completion of this Task, the Customer will have one (1) mobile configuration of Mobile Unit for testing.

Task Deliverables

- OnCall Dispatch | Mobile Unit Fire Configuration Session
- OnCall Dispatch | Mobile Unit Fire Configuration Consultation
-

Task Prerequisites

- OnCall Dispatch Configuration Consulting 3 Task is complete.

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.
- Attendance by the Customer's personnel will be limited to no more than twelve (12) people and must consist of field users and stakeholders capable of making final decisions about product behavior and functionality.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Conduct one (1) instance of Mobile Unit Fire Configuration Session and Mobile Unit fire Configuration Consultation.

Customer Team Participation and Responsibilities

Customer shall:

- Provide a Facility;
- Provide a Project Workstation for each attendee;
- Provide mobile SME to support Hexagon as needed;
- Provide a Dispatcher SME to give feedback on how Mobile Unit will affect dispatchers and to assist with various dispatching Activities;
- Participate fully and collaboratively in the Mobile Unit Fire Configuration Session with the understanding that Mobile Unit client configuration decisions must be documented and agreed upon at the conclusion of these sessions;
- Configure Mobile Unit during the Mobile Unit Fire Configuration Period; and
- Begin the Mobile Unit Fire Configuration Document.

Task Acceptance Criteria

The Task is complete when Hexagon has conducted the Mobile Unit Fire Configuration Session and the Mobile Unit Fire Configuration Consultation.

30. OnCall Dispatch | Mobile Responder Configuration – Law

Task Description

Hexagon will conduct one (1) remote session to consult on the configuration options outlined in the OnCall Mobile Configuration Options form lasting no more than one (1) Business Day as part of the Project. Hexagon will work with the Customer to complete this form during this session.

After completing the overview of the configuration options, Hexagon will configure OnCall Mobile based on the completed OnCall Mobile Configuration Options form. Hexagon will provide up to one (1) Business Day of configuration time and deliver the completed configuration changes for OnCall Mobile for Law.

Task Deliverables

- One (1) OnCall Dispatch | Mobile Responder Law Configuration

Task Prerequisites

- COTS Interface Product Installation and Configuration Task is complete.

Task Assumptions

- N/A

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Conduct one (1) remote session of OnCall Dispatch | Mobile Responder Configuration for Law review lasting no more than one (1) Business Day
- Configure Mobile Responder based on the corresponding OnCall Mobile Configuration Options.

Customer Team Participation and Responsibilities

Customer shall:

- Provide mobile SME to Hexagon as needed; and
- Provide a Dispatcher SME to give feedback on how OnCall Dispatch | Mobile Responder will affect dispatchers and assist with various dispatching tasks.

Task Acceptance Criteria

The Task is complete when Hexagon has delivered the configured OnCall Dispatch | Mobile Responder for Law based on the corresponding OnCall Mobile Configuration Options form.

31. OnCall Dispatch | Mobile Responder Configuration – Fire

Task Description

Hexagon will conduct one (1) remote session to consult on the configuration options outlined in the OnCall Mobile Configuration Options form lasting no more than one (1) Business Day as part of the Project. Hexagon will work with the Customer to complete this form during this session.

After completing the overview of the configuration options, Hexagon will configure OnCall Mobile based on the completed OnCall Mobile Configuration Options form. Hexagon will provide up to one (1) Business Day of configuration time and deliver the completed configuration changes for OnCall Mobile for Fire.

Task Deliverables

- One (1) OnCall Dispatch | Mobile Responder Fire Configuration

Task Prerequisites

- COTS Interface Product Installation and Configuration

Task Assumptions

- N/A

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Conduct one (1) remote session of OnCall Dispatch | Mobile Responder Configuration for Fire review lasting no more than one (1) Business Day
- Configure Mobile Responder based on the corresponding OnCall Mobile Configuration Options.

Customer Team Participation and Responsibilities

Customer shall:

- Provide mobile SME to Hexagon as needed; and
- Provide a Dispatcher SME to give feedback on how OnCall Dispatch | Mobile Responder will affect dispatchers and assist with various dispatching tasks.

Task Acceptance Criteria

The Task is complete when Hexagon has delivered the configured OnCall Dispatch | Mobile Responder for Fire based on the corresponding OnCall Mobile Configuration Options form.

32. OnCall Records Fundamentals for Core Team

Task Description

The purpose of this Task is to provide participants from the Records Core Team base level knowledge of the Subsystem to allow the attendees to properly configure the Subsystem. During this Task, Hexagon will conduct one (1) OnCall Records Fundamentals class for system administrators and Users who are part of the Records Core Team ("Core Team Training"). The Core Team Training shall last no more than four (4) Business Days. The Core Team Training will include the following topics for the COTS version of OnCall Records:

Core Team Training

- OnCall Records Solution overview and global features
- Modules overview
- Overview of configuration options
- Overview of NIBRS validations and reporting
- Overview of output reporting and customizations
- Discussion on best practices to follow during configuration workshops
- Adaptation of business processes into OnCall Records and planning for upcoming workshops

The personnel attending Core Team Training shall have completed MS Windows training or have comparable education, training, and experience with MS Windows and its user interface. The personnel designated by the Customer to attend this training shall be the primary participants in Functional Testing for OnCall Records.

Task Deliverables

- Records Core Team Training session

Task Prerequisites

- Business Process Analysis Workshop Task is complete.
- [redacted] and OnCall Software Staging Task is complete.
- OnCall Records NIBRS Validation Installation Task is complete.
- Completion of an introductory Microsoft Windows course or equivalent knowledge and familiarity with the Microsoft Windows user interface.

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.
- The training course shall last no longer than four (4) Business Days.
- Session is a formal training presentation based on the COTS version of OnCall Records.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide OnCall Records training for the Records Core Team Members on the installed COTS OnCall Records Software.

Customer Team Participation and Responsibilities

Customer shall:

- Provide a Facility;
- Provide a Project Workstation for each attendee;
- Designate the Records Core Team for attendance and ensure those same participants participate in subsequent Records configuration and testing Tasks;
- Ensure that attendees have attended an introductory MS Windows course, or have comparable education, training, or experience, are available to actively participate in the scheduled training program and attendees attend scheduled training class in their entirety;
- Ensure that all training workstations and servers are operational prior to the agreed start of training classes; and
- Provide internal training to users that are unable to attend the Hexagon-provided training.

Task Acceptance Criteria

This Task is complete when the OnCall Records Fundamentals for Core Team training has been provided.

33. OnCall Records System Configuration Workshop 1

Task Description

During this Task, Hexagon will provide the first System Configuration Workshop ("Configuration Workshop 1"). This Task includes a System/training review for the setups that will be covered. This will provide the Customer Records Core Team assistance as they configure and setup the OnCall Records system. Customer will be responsible for the overall configuration of the OnCall Records Subsystem. This is a hands-on workshop, and Customer's staff will have ongoing configuration and other assignments resulting from this Task. The Configuration Workshop 1 shall last no more than four (4) Business Days. Following completion of the Configuration Workshop 1, Customer will complete its setup of the assigned configuration topics below prior to the scheduled System Configuration Workshop 2 ("Configuration 1 Period").

Configuration Workshop 1 Topics

- OnCall Records Regional Configuration Overview
- OnCall Records Agency Configuration Overview
- Access configuration for Groups and Users
- Code Maintenance & Administration Overview
- Address Server – Overview
- Adaptation of Business Processes into OnCall Records

Task Deliverables

- Configuration Workshop 1 for the Customer OnCall Records Core Team
- Customized documentation on expectations for completion before Configuration Workshop 2.

Task Prerequisites

- OnCall Records Fundamentals for Core Team Task is complete.
- Custom Interface Requirements Gathering Task is complete.

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.
- The Configuration Workshop 1 shall last no more than four (4) Business Days of the given week.
- The workshop provides for a maximum of twelve (12) Core Team Members.
- This workshop is a formal presentation based on the COTS version of OnCall Records.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide OnCall Records Configuration Workshop 1.

Customer Team Participation and Responsibilities

Customer shall:

- Provide a Facility;
- Provide a Project Workstation for each attendee;

- Ensure, at minimum, the same Records Core Team members who attended OnCall Records Fundamentals for Core Team attend Configuration Workshop 1;
- Ensure that appropriate personnel and system administrator are available to actively participate in the scheduled training program and attendees attend scheduled training class in their entirety;
- Ensure that all workshop workstations and servers are operational prior to the agreed start of training classes; and
- As it pertains to the topics listed for Configuration Workshop 1 above, configure OnCall Records based upon the information provided in OnCall Records System Configuration Workshop 1 during the Configuration 1 Period.

Task Acceptance Criteria

This Task is complete when Hexagon has delivered the Configuration Workshop 1.

34. OnCall Records System Configuration Workshop 1 Follow-up Session

Task Description

Hexagon will provide a Configuration Workshop 1 Follow-up after completion of the Configuration Workshop 1, and it is intended to held two (2) weeks following Configuration Workshop 1. This discussion will be provided to offer assistance and answer questions that may arise after the Configuration Workshop 1 and after the Customer has started configuring OnCall Records, so the Customer's Records Core Team can continue to complete their system setup. This Task occurs during the Configuration 1 Period.

Task Deliverables

- Configuration Workshop 1 Follow-up Session

Task Prerequisites

- OnCall Records System Configuration Workshop 1 Task is complete.
- Customer has commenced configuring OnCall Records reflective of the information provided in OnCall Records System Configuration Workshop 1.

Task Assumptions

- The sessions is intended to be scheduled the two (2) weeks following Configuration Workshop 1 as appropriate.
- The session is provided for a maximum of twelve (12) Team Members with a maximum of one (1) student per Project Workstation, unless otherwise agreed to by Hexagon;
- This session is a formal presentation based on the version of OnCall Records covered in the Configuration Workshop 1.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide OnCall Records Configuration Workshop 1 Follow-up for the Core Team Members.

Customer Team Participation and Responsibilities

Customer shall:

- Provide a Project Workstation for each attendee;
- Designate the Customer OnCall Records Core Team members for attendance, which at minimum, shall include the Records Core Team members who attended the Configuration Workshop 1;
- Provide the facilities, supplies, and equipment necessary to support a session conference call. A single room with a projector or LCD screen is recommended; and
- Ensure that appropriate personnel and system administrator are available to actively participate in the scheduled conference and attendees attend in their entirety.

Task Acceptance Criteria

This Task is complete when Hexagon has completed the Configuration Workshop 1 Follow-up Session.

35. OnCall Records COTS Reports Review

Task Description

This Task is a Hexagon-led class on how to create and edit [redacted] reports within the OnCall Records System (the "Records Reports Review"). As part of the Records Reports Review, new report creation will be shown and discussed to allow for adaptation of existing [redacted] report knowledge to the new system. The Records Reports Review shall last no longer than two (2) Business Days. For clarity, the Records Reports Review is not intended to provide instruction on how to load and edit reports within OnCall Records or [redacted] report training, which the participants should already know prior to their attendance.

Task Prerequisites

- OnCall Records System Configuration Workshop 1 Task is complete.

Task Assumptions

- Customer attendees have appropriate education, training, and experience with [redacted]
- The Records Reports Review is provided for up to twelve (12) people with a maximum of one (1) student per Project Workstation, unless otherwise agreed to by Hexagon.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide the Records Reports Review

Customer Team Participation and Responsibilities

Customer shall:

- Provide a facility according to the requirements provided in Task Assumptions;
- Provide a Project Workstation for each attendee; and
- Ensure appropriate personnel, with the requisite knowledge attend the Records Reports Review.

Task Acceptance Criteria

This Task is complete when the Records Report Review is completed.

36. OnCall Records System Configuration Workshop 2

Task Description

During this Task, Hexagon will provide the second System Configuration Workshop ("Configuration Workshop 2"). This Task includes a System/training review on the topics specified below. The Configuration Workshop 2 will provide instruction to facilitate the Customer continuing to configure OnCall Records This is a hands-on workshop. Customer's staff will have ongoing configuration and other assignments resulting from this Task. The Configuration Workshop 2 shall last no more than four (4) Business Days. Following completion of the Configuration Workshop 2, Customer will complete its setup of the assigned configuration topics below prior to the scheduled System Configuration Workshop 3 ("Configuration 2 Period").

Configuration Workshop 2 Topics

- Base UI Configuration Adaptations
- Alert and Notification Configuration
- Workflow Approval process
- Continued Adaptation of Business Processes into OnCall Records

Task Deliverables

- OnCall Records Configuration Workshop 2
- Customized documentation on expectations for completion before the end of the Configuration 2 Period

Task Prerequisites

- OnCall Records System Configuration Workshop 1 Follow-up Session Task is complete.
- Customer has completed configuration activities from OnCall Records Configuration Workshop 1.
- Customer has configured the items identified in Configuration Workshop 1 within OnCall Records.
- The address server will be operational and turned on. Customer will verify that the address verification is working properly.
- Hexagon has installed the Clevest software.

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.
- The Configuration Workshop 2 shall last no more than four (4) Business Days.
- The workshop provides for a maximum of twelve (12) Team Members.
- This is a formal workshop presentation based on the COTS version of OnCall Records.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide OnCall Records Configuration Workshop 2 in the installed OnCall Records Software.

Customer Team Participation and Responsibilities

Customer shall:

- Provide a Facility;
- Provide a Project Workstation for each attendee;
- Designate the Customer OnCall Records Core Team members for attendance, which shall, at a minimum, include past participants from Configuration Workshop 1;
- Ensure that appropriate personnel and system administrator are available to actively participate in the scheduled training program and attendees attend scheduled training class in their entirety;
- Ensure that all workshop workstations and servers are operational prior to the agreed start of training classes; and
- As it pertains to the topics listed for Configuration Workshop 2 above, configure OnCall Records based upon the information provided in OnCall Records System Configuration Workshop 2 during the Configuration 2 Period.

Task Acceptance Criteria

This Task is complete when Hexagon has delivered the Configuration Workshop 2.

37. OnCall Records System Configuration Workshop 2 Follow-up Session

Task Description

Hexagon will provide a Configuration Workshop 2 Follow-up session after completion of the Configuration Workshop 2 during the following two (2) weeks. This session will be provided to offer assistance and answer questions that may arise from the Configuration Workshop 2 and Customer configuration of OnCall Records based upon the information provided in OnCall Records Configuration Workshop 2, so that the Records Core Team can continue to complete configuration of the Subsystem. This Task occurs during the Configuration 2 Period.

Task Deliverables

- Configuration Workshop 2 Follow-up Session

Task Prerequisites

- OnCall Records System Configuration Workshop 2 Task is complete.
- Customer has commenced configuring OnCall Records reflective of the information provided in OnCall Records System Configuration Workshop 2.

Task Assumptions

- The session will be scheduled the two (2) weeks following Configuration Workshop 1 as appropriate..
- The session is provided for a maximum of twelve (12) Team Members with a maximum of one (1) student per Project Workstation, unless otherwise agreed to by Hexagon;
- Session is a formal presentation based on the COTS version of OnCall Records covered in the Configuration Workshop 2.

Task Deliverables

- Configuration Workshop 2 Follow-up Session for the Customer OnCall Records Core Team

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide a OnCall Records Configuration Workshop 2 Follow-up session for the Core Team Members.

Customer Team Participation and Responsibilities

Customer shall:

- Provide a facility according to the requirements provided in Task Assumptions;
- Provide a Project Workstation for each attendee;
- Designate the Customer OnCall Records Core Team members for attendance, which at minimum, shall include the Records Core Team members who attended the Configuration Workshop 2;
- Ensure that appropriate personnel and system administrator are available to actively participate in the scheduled session and attendees attend in their entirety.

Task Acceptance Criteria

This Task is complete when Hexagon has delivered the Configuration Workshop 2 Follow-Up Session.

38. OnCall Records System Configuration Workshop 3

Task Description

During this Task, Hexagon will provide the third System Configuration Workshop ("Configuration Workshop 3"). This Task includes the topics specified below. The Configuration Workshop 3 will provide instruction to facilitate the Customer continuing to configure OnCall Records. This is a hands-on workshop. Customer's staff will have ongoing configuration and other assignments resulting from this Task. The Configuration Workshop 3 shall last no more than four (4) Business Days. Following completion of the Configuration Workshop 3, Customer will complete its setup of the assigned configuration topics below ("Configuration 3 Period") prior to the scheduled OnCall Records Customer Functional Testing.

Configuration Workshop 3 Topics

- Advanced UI Configuration Adaptations
- NIBRS review and configuration Continued Adaptation of Business Processes into OnCall Records
- Planning for Testing and Training

Task Deliverables

- OnCall Records Configuration Workshop 3
- Customized documentation on expectations for completion before next Workshop session

Task Prerequisites

- OnCall Records System Configuration Workshop 2 Follow-up Session Task is complete.
- Customer has configured the items identified in Configuration Workshop 2 within OnCall Records.
- The Customer has completed all configuration activities arising from OnCall Records System Configuration Workshop 2.

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.
- The Configuration Workshop 3 duration shall not exceed four (4) Business Days.
- Configuration Workshop 3 provides for a maximum of twelve (12) Team Members.
- This is a formal workshop presentation based on the COTS version of OnCall Records.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide OnCall Records Configuration Workshop 3 in the installed OnCall Records Software.

Customer Team Participation and Responsibilities

Customer shall:

- Provide a Facility;
- Provide a Project Workstation for each attendee;
- Designate the Customer OnCall Records Core Team members for attendance, which at a minimum, shall include Customer' participants from Configuration Workshops 1 and 2;

- Ensure that appropriate personnel and system administrator are available to actively participate in the scheduled training program and attendees attend scheduled training class in their entirety;
- Ensure that all workshop workstations and servers are operational prior to the agreed start of training classes; and
- As it pertains to the topics listed for Configuration Workshop 3 above, configure OnCall Records based upon the information provided in OnCall Records System Configuration Workshop 3 during the Configuration 3 Period.

Task Acceptance Criteria

This Task is complete when Hexagon has delivered the Configuration Workshop 3.

39. OnCall Records System Configuration Workshop 3 Follow-up Session

Task Description

Hexagon will provide a Configuration Workshop 3 Follow-up after completion of the Configuration Workshop 3 during the following two (2) weeks. This session will be provided to offer assistance and answer questions that may arise from the Configuration Workshop 3 so that the Customer's Records Core Team can continue to complete the system setup. This Task occurs during the Configuration 3 Period.

Task Deliverables

- OnCall Records Configuration Workshop 3 Follow-up session

Task Prerequisites

- OnCall Records System Configuration Workshop 3 Task is complete.
- Customer has commenced configuring OnCall Records reflective of the information provided in OnCall Records System Configuration Workshop 3.

Task Assumptions

- The session will be scheduled the two (2) weeks following Configuration Workshop 1 as appropriate..
- The session is provided for a maximum of twelve (12) Team Members with a maximum of one (1) student per Project Workstation, unless otherwise agreed to by Hexagon;
- Session is a formal workshop presentation based on the version of OnCall Records covered in the Configuration Workshop 3.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide a OnCall Records Configuration Workshop 3 follow-up session for the Core Team Members.

Customer Team Participation and Responsibilities

Customer shall:

- Provide a facility according to the requirements provided in Task Assumptions;
- Provide a Project Workstation for each attendee;
- Designate the Customer OnCall Records Core Team members for attendance, which at a minimum, shall include the Customer's participants from Configuration Workshop 3;
- Ensure that appropriate personnel and system administrator are available to actively participate in the scheduled session and attendees attend in their entirety.

Task Completion Criteria

This Task is complete when Hexagon has completed the Configuration Workshop 3 Follow-up Session.

40. OnCall Records | Citizen Reporting System Configuration Workshop

Task Description

The HxGN OnCall Records | Citizen Reporting is an add-on product to OnCall Records that enables citizens in the Customer's jurisdiction to interact with the agency. Citizen Reporting is delivered as a website add-on that the Customer can host as part of their existing website. It includes the OnCall Records Connect API to facilitate integration with OnCall Records.

During this Task, Hexagon will provide the System Configuration Workshop for Citizen Reporting ("Citizen Reporting Configuration Workshop"). This task includes a System/training review for the setups that will be covered. This will reinforce the previous training and provide the Customer Core team assistance as they configure and setup the OnCall Records | Citizen Reporting Subsystem. The workshop will provide the knowledge needed and enable the Customer staff to complete the OnCall Records | Citizen Reporting configuration and support the Subsystem. This is a hands-on workshop. Customer's staff will have ongoing configuration and other assignments resulting from this task. Following completion of the Citizen Reporting Configuration Workshop, Customer will complete its setup of the assigned configuration topics ("Citizen Reporting Configuration Period") prior to Customer Functional Testing – OnCall Records.

Task Deliverables

- Configuration Workshop for the Customer OnCall Records | Citizen Reporting Core Team

Task Prerequisites

- OnCall Records System Configuration Workshop 3 Follow-up Session Task is complete.
- The Customer has installed and configured at least one (1) workstation per student attending the session.

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.
- The Citizen Reporting Configuration Workshop duration is four (4) Business Days.
- The workshop provides for a maximum of twelve (12) Team Members.
- The Customer shall be responsible for ensuring any data it makes available through Citizen Reporting is compliant with applicable laws and regulations.
- This is a formal workshop presentation based on the COTS version of OnCall Records.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide the Citizen Reporting Configuration Workshop in the installed OnCall Records | Citizen Reporting Software.

Customer Team Participation and Responsibilities

Customer shall:

- Provide a Facility;
- Provide a Project Workstation for each attendee;
- Designate the Customer OnCall Records | Citizen Reporting Core Team for attendance;
- Ensure that appropriate personnel and system administrator are available to actively participate in the scheduled training program and attendees attend scheduled training class in their entirety;

- Ensure that all workshop workstations and servers are operational prior to the agreed start of training classes; and
- As it pertains to the topics listed above, configure OnCall Records based during the Citizen Reporting Configuration Period.

Task Acceptance Criteria

This Task is complete when Hexagon has delivered the Citizen Reporting Configuration Workshop to the Customer.

41. OnCall Records State NIBRS Reporting Installation

Task Description

During this Task, Hexagon resources will upgrade the IBRS reporting client to reflect state-specific product changes to support state reporting.

Task Deliverables

- Hexagon installation of the state-specific NIBRS reporting.

Task Prerequisites

- State NIBRS Validation Installation Task is complete.

Task Assumptions

- OnCall Records will use existing State NIBRS software. No new development or additional customizations are included.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide COTS documentation on the NIBRS submission tool;
- Support Customer testing and provide resolution of Blocker Defects; and
- Prepare and submit a NIBRS test submission to the State.

Customer Team Participation and Responsibilities

- None

Task Acceptance Criteria

This Task is complete when the current version of State NIBRS has been installed and tested to validate its conformance with State requirements.

42. OnCall Records Additional Agency Cloning

Task Description

After the Configuration Phase, Hexagon will create sixteen (16) additional agencies in OnCall Records. The creation process will entail Hexagon duplicating the Customer's (the lead agency) ("Primary Agency") configurations into the newly created agencies. This process will facilitate duplication of most of the configurations created in the Primary Agency; however, a full list of work done, and what will be left for the Customer to configure will be delivered as part of the process ("Agency Cloning Document"). The cloned agencies are as follows:

- Williamson County Sheriff's Office
- Hutto Police Department
- Liberty Hill Police Department
- Granger Police Department
- Thrall Police Department
- Jarrell Police Department
- Florence Police Department
- Liberty Hill School Police Department
- Round Rock ISD Police Department
- Hutto ISD Police Department
- Jarrell ISD Police Department
- Constables Pct 1
- Constables Pct 2
- Constables Pct 3
- Constables Pct 4
- Southwestern University Police Department

Task Deliverables

- Current configured Primary Agency cloned to all additional agencies.
- Agency Cloning Document

Task Prerequisites

- OnCall Records Configuration Tasks are complete.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Review the steps with all stakeholders and plan any related outage;
- Create/clone data for the Primary Agency and review for accuracy;
- Create/clone remaining agencies; and
- Prepare a document outlining all configurations that were replicated, and what will be left for the Customer to manage.

Customer Team Participation and Responsibilities

Customer shall:

- Review all steps during the process;
- Finalize all newly created agencies based on documentation provided by Hexagon; and
- Test agencies in OnCall Records.

Task Acceptance Criteria

This Task is complete when Hexagon has duplicated the Primary Agency configurations for other agencies and provided the Agency Cloning Document to Customer.

43. OnCall Dispatch Archive Database Staging

Task Description

Hexagon resources will create an OnCall archive database using the CAD Database Utility and the Customer's staging hardware.

Task Deliverables

- OnCall archive database on the Production staging system

Task Prerequisites

- [redacted] and OnCall Software Staging Task is Complete.
- The Customer has provided full database backup to Hexagon or given permission for Hexagon to take the backup on the Customer's behalf.
- Code Freeze in place on Production Environment.

Task Assumptions

- N/A

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Process update to OnCall archive database schema using Customer's staging hardware; and
- Use a copy of the 'production' database as an initial start point for the archive database.

Customer Team Participation and Responsibilities

Customer shall:

- Ensure Hexagon is provided with full backup of existing Production database to be used as start point for the OnCall archive database.

Task Acceptance Criteria

This Task is complete when the OnCall archive database has been delivered on the Production staging system.

44. OnCall Analytics | Dispatch Configuration

Task Description

This Task is Hexagon-led and involves configuring OnCall Analytics | Dispatch with Customer's site-specific parameters.

OnCall Analytics is business intelligence software for reporting, analysis, and evidence-based decision making. It provides reporting and analysis capabilities, which are fully described within a document titled: "HxGN OnCall Analytics | Dispatch: Delivered Models and Reports," which is available upon request. That document describes the types of reports and models available within OnCall Analytics, which may require additional configuration and work by the Customer. Only those reports corresponding to the type of reporting model and Software product included within the Project are available to the Customer.

Task Deliverables

- Configuration of OnCall Analytics | Dispatch software and components for Customer testing and verification

Task Prerequisites

- OnCall Dispatch Archive Database Staging Task is complete.
- OnCall Dispatch Configuration Consulting 3 Task is complete.

Task Assumptions

- Hexagon will install the OnCall Analytics | Dispatch solution.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Configure the OnCall Analytics | Dispatch software components; and
- Confirm that the software installation and delivery has been completed, the data connections have been tested, and data is accessible in reports.

Customer Team Participation and Responsibilities

Customer shall:

- [redacted] license keys to Hexagon for the database installation if not already provided.

Task Acceptance Criteria

This Task is complete when Hexagon has configured and tested the OnCall Analytics | Dispatch software and data is accessible for reports and analytics.

45. OnCall Analytics | Records Configuration

Task Description

This Task is Hexagon-led and involves configuring OnCall Analytics | Records Advantage with Customer's site-specific parameters.

HxGN OnCall Analytics is business intelligence software for reporting, analysis, and evidence-based decision making. It provides reporting and analysis capabilities, which are fully described within a document titled: "HxGN OnCall Analytics | Records: Delivered Models and Reports," which available upon request. That document describes the types of reports and models available within OnCall Analytics, which may require additional configuration and work by the Customer. Only those reports corresponding to the type of reporting model and Software product included within the Project are available to the Customer.

Task Deliverables

- Configuration of OnCall Analytics | Records Advantage software and components for Customer testing and verification

Task Prerequisites

- [redacted] and OnCall Software Staging Task is complete.
- OnCall Records System Configuration Workshop 2 Task is complete.
- Data Conversion Audit 1 in OnCall Records Data Conversion Task above.

Task Assumptions

- Hexagon will install the OnCall Analytics | Records Advantage solution.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Configure the OnCall Analytics | Records Advantage software; and
- Confirm that the software installation and delivery has been completed, the data connections have been tested, and data is accessible in reports.

Customer Team Participation and Responsibilities

Customer shall:

- [redacted] license keys to Hexagon for the database installation if not already provided.

Task Acceptance Criteria

This Task is complete when Hexagon has configured and tested the OnCall Analytics | Records Advantage software and data is accessible for reports and analytics.

46. OnCall Analytics | Dispatch Training

Task Description

During this Task, Hexagon will train end users and system administrators on HxGN OnCall Analytics | Dispatch.

The OnCall Analytics User Training will provide instruction on accessing, viewing, and creating reports from the OnCall Analytics Report portal. It will also provide an overview of the delivered reports and data models. The delivered report provides out-of-the box access to key performance metrics while the data models provide an easy and powerful way for users to ask their own questions of the data and create new reports.

The OnCall Analytics System Administrator Training is designed for system administrators, to provide instructions on the setup, site-specific configurations, and administrative tasks needed to maintain the OnCall Analytics Dispatch product.

Task Deliverables

- HxGN OnCall Analytics | Dispatch User Training (Qty: 1)
- HxGN OnCall Analytics | Dispatch System Administrator Training (Qty: 1)

Task Prerequisites

- OnCall Analytics | Dispatch Configuration Task is complete.
- The attendees are familiar with Microsoft Windows-based applications, administrative tasks, and agency workflows.

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.
- Both training courses are intended to be conducted the same week.
- The User Training will last for a maximum of three (3) Business Days and is provided for a maximum of ten (10) attendees.
- The System Administrator Training will last for a maximum of one (1) Business Day and is provided for a maximum of four (4) attendees.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide the OnCall Analytics User and System Administrator Training sessions.

Customer Team Participation and Responsibilities

Customer shall:

- Provide a Facility;
- Provide a Project Workstation for each attendee;
- Ensure that appropriate personnel and system administrator are available to actively participate in the scheduled training program and attendees attend scheduled training class in their entirety; and
- Ensure that all workshop workstations and servers are operational prior to the agreed start of training classes.

Task Acceptance Criteria

This Task is complete when Hexagon has delivered both the OnCall Analytics Dispatch User Training and System Administrator Training.

47. OnCall Analytics | Records Training

Task Description

During this Task, Hexagon will train end users and system administrators on HxGN OnCall Analytics | Records.

The OnCall Analytics User Training will provide instruction on accessing, viewing, and creating reports from the OnCall Analytics Report portal. It will also provide an overview of the delivered reports and data models. The delivered report provides out-of-the box access to key performance metrics while the data models provide an easy and powerful way for users to ask their own questions of the data and create new reports.

The OnCall Analytics System Administrator Training is designed for system administrators, to provide instructions on the setup, site-specific configurations, and administrative tasks needed to maintain the OnCall Analytics Records product.

Task Deliverables

- HxGN OnCall Analytics | Records User Training (Qty: 1)
- HxGN OnCall Analytics | Records System Administrator Training (Qty: 1)

Task Prerequisites

- OnCall Analytics | Records Configuration Task is complete.
- OnCall Records COTS Reports Review Task complete.
- The attendees are familiar with Microsoft Windows-based applications, administrative tasks, and agency workflows.

Task Assumptions

- Hexagon responsibilities will be executed on site at a Facility.
- Both training courses are intended to be conducted the same week.
- The User Training will last for a maximum of three (3) Business Days and is provided for a maximum of ten (10) attendees.
- The System Administrator Training will last for a maximum of one (1) Business Day and is provided for a maximum of four (4) attendees.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide the OnCall Analytics User and System Administrator Training sessions.

Customer Team Participation and Responsibilities

Customer shall:

- Provide a Facility;
- Provide a Project Workstation for each attendee;
- Ensure that appropriate personnel and system administrator are available to actively participate in the scheduled training program and attendees attend scheduled training class in their entirety; and
- Ensure that all workshop workstations and servers are operational prior to the agreed start of training classes.

Task Acceptance Criteria

This Task is complete when Hexagon has delivered both the OnCall Analytics Records User Training and System Administrator Training.

48. Custom Interface Product Installation and Configuration

Task Description

During this Task, Hexagon will install, configure, and test the Custom Interfaces. Although the Customer is expected to participate in Hexagon's internal testing of the Custom Interfaces, the Customer will formally test the Custom Interfaces' functionality during Functional Testing.

Task Deliverables

- Documentation of Custom Interfaces installation/testing

Task Prerequisites

- Operation or availability of the external system or Third-Party Software.
- Custom Interface Development Task is complete.
- OnCall Dispatch Configuration Consulting 1 Task is complete.
- OnCall Records System Configuration Workshop 1 Task is complete.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Install Custom Interfaces; and
- Test Custom Interfaces in accordance with the approved ICDs.

Customer Team Participation and Responsibilities

Customer shall:

- Ensure SMEs are available to support Hexagon Activities as needed;
- Verify that physical connectivity has been achieved from Customer's communication server to OnCall;
- Provide availability and confirm operation of external systems or third-party software;
- Provide the following information to Hexagon:
    - IP address for remote databases
    - Socket value for remote systems
    - Operator IDs (ORIs), terminal mnemonics, etc., as needed by remote systems
- Ensure the system and network administrators are available to work closely with the Hexagon team for the duration of the Task; and
- Ensure third-party cooperation with Hexagon's reasonable requests.

Task Acceptance Criteria

This Task is complete when each Custom Interface is installed and configured in accordance with the applicable ICD.

49. Standard Interface Product Installation and Configuration

Task Description

During this Task, Hexagon will install and configure the Standard Interfaces. The Customer will formally test the interface functionality and reliability during Functional Testing.

The following are regarded as “Standard Interfaces” as the term is defined in Attachment H of this SOW:

- Fire Station Alerting OnCall Dispatch Interface
  - [redacted]
- Dispatch Alerts OnCall Dispatch Interface
  - [redacted]
- External Alarms OnCall Dispatch Interface
  - [redacted]
- PLT OnCall Dispatch Interface
  - [redacted]
- CAD to CAD OnCall Dispatch Interface
  - [redacted]
- [redacted]
- Anti-Bias Reporting (Texas)

As part of this Task, Hexagon will provide consulting services to advise [redacted].

Task Deliverables

- Documentation of Standard Interfaces installation

Task Prerequisites

- Operation or availability of the external system or Third-Party Software
- OnCall Dispatch Configuration Consulting 3 Task is complete.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Install Standard Interfaces.

Customer Team Participation and Responsibilities

- Ensure SMEs are available to support Hexagon Activities as needed;
- Verify that physical connectivity has been achieved from Customer’s communication server to OnCall;
- Provide availability and confirm operation of external systems or third-party software;
- Provide the following information to Hexagon:
  - IP address for remote databases
  - Socket value for remote systems

- Operator IDs (ORIs), terminal mnemonics, etc., as needed by remote systems

- Ensure the system and network administrators are available to work closely with the Hexagon team for the duration of the Task; and
- Ensure third-party cooperation with Hexagon's reasonable requests.

Task Acceptance Criteria

This Task is complete when each Standard Interface is installed and configured.

50. Sustaining Coordination Services for the CommSys ConnectCIC ASAP Interface

Task Description

During this Task, CommSys will provide consulting and sustaining coordination services for the ConnectCIC ASAP implementation.

- CommSys will provide the Customer with professional services for only the following aspects of the project (the “Sustaining Coordination Services”):
  - Coordinate efforts with the agency’s executive stakeholders, Hexagon, state message switch/control point officials, The Monitoring Association (TMA), and the alarm monitoring companies;
  - Coordinate with Hexagon for the installation of updates to Hexagon’s External Alarms OnCall Dispatch Interface in both a test environment and a production environment as applicable;
    - These may be done at separate times
    - A test plan as appropriate will be used
  - Work with agency officials to identify connectivity issues to The State and The National Law Enforcement Teletype Service (NLETS) network via the state CJIS Message Switch or other transport method if available;
  - Coordinate with new alarm companies that begin operating in production with the ASAP project and with agency officials through introductions, testing, and cutover to production activities;
  - Execute testing to ensure that the end product continues to conform to the APCO/CSAA ANS 2.101.2-2014 standard; and
  - Coordinate troubleshooting efforts with all appropriate agencies and staff as necessary when problems arise.

Task Deliverables

- Sustaining Coordination Services

Task Assumptions

- The testing and verification of the ASAP Interface will take place on site.

Task Prerequisites

- Installation of External Alarms OnCall Dispatch Interface (reference Standard Interface Product Installation and Configuration task above)
- Installation of CommSys ConnectCIC
- CommSys ConnectCIC ASAP Option purchased
- Connectivity between CommSys ConnectCIC and the State CJIS Message Switch to receive NLETS transactions

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Coordinate with CommSys for the installation of the External Alarms OnCall Dispatch Interface;

- Coordinate with CommSys and “The Monitoring Association (TMA) for the installation of the ConnectCIC Product for APCO ASAP Alarm Product; and
- Coordinate with CommSys and TMA to arrange testing and validation of the interface.

Customer Team Participation and Responsibilities

Customer shall:

- Provide the appropriate team to complete the Sustaining Coordination Services.

Task Acceptance Criteria

This Task is considered complete when the ConnectCIC ASAP Interface has been installed and Sustaining Coordination Services have been performed.

Testing Phase

51. Test Plan and Test Cases Development – OnCall Dispatch

Task Description

During this Task, the Customer will create a test plan ("CAD Test Plan") with Test Cases for OnCall Dispatch. The CAD Test Plan and Test Cases are essential for the Customer to be able to validate and prove the functionality of the Dispatch Subsystem. Every Benchmark Criteria corresponding to OnCall Dispatch should have at least one Test Case; some Benchmark Criteria may have multiple associated Test Cases. The Customer will identify the Benchmark Criteria that correspond to the applicable Test Cases. A clear pass/fail criterion must be defined for each Test Case. The Test Plan and Test Cases will be agency-specific, and work-process driven with clearly documented Pass/Fail criteria. Only the elements of the Test Plan and Test Cases conforming with the Benchmark Criteria shall be used in evaluating and testing the Subsystem. The Test Plan is the set of Test Cases that will serve as the basis of testing the fully configured Subsystem, including interfaces.

The Customer will not need a fully configured Subsystem to create the Test Plan and Test Cases. The Test Case creation should be accomplished using a workflow-based Test Case.

Task Deliverables

- Customer's CAD Test Plan and Test Cases

Task Prerequisites

- OnCall Dispatch Fundamentals for Core Team Task is complete.

Task Assumptions

- N/A

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Consult with the Customer during the Test Plan and Test Cases creation Task to validate the Test Cases correspond to the Benchmark Criteria (applicable to Dispatch).

Customer Team Participation and Responsibilities

Customer shall:

- Create the CAD Test Plan and Test Cases consistent with the Benchmark Criteria; and
- Provide CAD Test Plan and Test Cases to Hexagon.

Task Acceptance Criteria

This Task is complete when the Customer has created the CAD Test Plan and Test Cases and Hexagon has validated the same in accordance with the Benchmark Criteria.

52. Test Plan and Test Cases Development – OnCall Records

Task Description

During this Task, the Customer will create a test plan ("RMS Test Plan") with Test Cases for OnCall Records. The RMS Test Plan and Test Cases are essential for the Customer to be able to validate and prove the functionality of the Records Subsystem. Every Benchmark Criteria corresponding to OnCall Records should have at least one Test Case; some Benchmark Criteria may have multiple associated Test Cases. The Customer will identify the Benchmark Criteria that correspond to the applicable Test Cases. A clear pass/fail criterion must be defined for each Test Case. The Test Plan and Test Cases will be agency-specific, and work-process driven with clearly documented Pass/Fail criteria. Only the elements of the Test Plan and Test Cases conforming with the Benchmark Criteria shall be used in evaluating and testing the System. The Test Plan is the set of Test Cases that will serve as the basis of testing the fully configured Subsystem, including interfaces.

The Customer will not need a fully configured Subsystem to create the Test Plan and Test Cases. The Test Case creation should be accomplished using a workflow-based Test Case.

Task Deliverables

- Customer's RMS Test Plan and Test Cases

Task Prerequisites

- OnCall Records Fundamentals for Core Team Task is complete.

Task Assumptions

- N/A

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Consult with the Customer during the RMS Test Plan and Test Cases creation task to validate the Test Cases correspond to the Benchmark Criteria.

Customer Team Participation and Responsibilities

Customer shall:

- Create the RMS Test Plan and Test Cases consistent with the Benchmark Criteria; and
- Provide RMS Test Plan and Test Cases to Hexagon.

Task Acceptance Criteria

This Task is complete when the Customer has created the RMS Test Plan and Test Cases and Hexagon has validated the same in accordance with the Benchmark Criteria.

53. Customer Functional Testing – OnCall Dispatch

Task Description

The Customer, with support from Hexagon, will test OnCall Dispatch's conformance with the Benchmark Criteria. The Customer will conduct Functional Testing over the course of ten (10) Business Days ("Dispatch Testing Period"). During the Dispatch Testing Period, the Customer shall execute the CAD Test Plan and corresponding Test Cases. Except as expressly provided and the Customer's subjective assessment of the performance (ability for the System to timely to react to Customer inputs) of the Subsystem with 150% load, no other testing or evaluation pertaining to OnCall Dispatch is contemplated in this Project. Customer will document and track the results of each Test Case as either pass or fail and may request Hexagon consultation as necessary during its testing Activity up to twenty-four (24) Business Hours.

Within five (5) Business Days of the end of the CAD Testing Period ("CAD Reporting Period"), the Customer shall file any Blocker Defects and Permissive Defects encountered during Functional Testing – Dispatch through Hexagon's Customer Resource Management (CRM) system. For any Blocker Defect identified, the Customer shall provide, at minimum, the following information: a description of the Defect and the steps used to reproduce it, the functionality tested when the Blocker Defect was encountered, the manner in which the functionality was tested, and the outcome when the functionality was tested. If the Blocker Defects are not filed within the CAD Reporting Period, it is presumed Functional Testing was completed without any Blocker Defect, and this Task is complete. Only Blocker Defects reported by the conclusion of the Reporting Period will be resolved as part of this Task. The existence of Permissive Defect(s) shall not preclude or be a condition of completion of any subsequent Tasks or implementation of a new Release.

To the extent requested, Customer agrees to promptly respond to requests for additional information regarding the Blocker Defect requested by Hexagon. Upon diagnosing the Blocker Defect and validating the Defect encountered meets the attributes of a Blocker Defect, Hexagon resources shall proceed to resolve the Blocker Defect accordingly. If the investigation determines the reported Blocker Defect did not meet the attributes of a Blocker Defect then the reported Defect will be reclassified in accordance with the levels provided in the Master Terms Glossary. Alternatively, if the investigation shows the reported Blocker Defect was caused by Customer hardware, Network Infrastructure, or Third-Party Software not provided by Hexagon, or non-conformance with Attachments E-1 and F, then Hexagon will provide such information to the Customer for the Customer to resolve and the Blocker Defect will be closed and regarded as complete.

As part of its resolution efforts, Hexagon may at its discretion provide a procedural or programmatic work around, a configuration change, or provide an Update. Once the Blocker Defect(s) is addressed, Hexagon will report to Customer the Blocker Defect has been addressed and the Customer will have five (5) Business Days to execute its Test Plan ("CAD Resolution Testing Period") to validate the fix provided by Hexagon has resolved the Blocker Defect.

After the Functional Testing, Hexagon will enforce a Code Freeze. No configurations or modifications will be allowed to the Subsystem by Hexagon or Customer, except those required to resolve any Blocker Defect. Upon addressing Blocker Defects, the Subsystem is a "Production Ready System." A Production Ready System signifies completion of all configuration and joint testing tasks. At this point, Hexagon will enforce a Subsystem-wide Code Freeze. Any System/Subsystem modifications will be handled via Change Order.

Task Deliverables

- OnCall Dispatch Functional Testing
- System Code Freeze

Task Prerequisites

- Customer and Hexagon mutually confirm that OnCall Dispatch and Mobile Unit are ready for testing.
- Test Plan and Test Cases Development – OnCall Dispatch Task is complete.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Verify all applicable software, systems and ancillary systems, including the redundancy of Production system (if applicable), are ready for Functional Testing;
- Provide support during Functional Testing;
- Review Defects filed by the Customer; and
- Resolve Blocker Defects filed by the Customer.

Customer Team Participation and Responsibilities

Customer shall:

- Verify all applicable software, systems and ancillary systems, including the redundancy of Production system (if applicable), are ready for Functional Testing;
- Execute the CAD Test Plan; and
- Track and document results from executed Test Cases and file any Blocker Defects in the CRM system by the end of the CAD Reporting Period.

Task Acceptance Criteria

This Task is complete upon expiration of the CAD Testing Period and resolution of all Blocker Defects reported by the end of the CAD Reporting Period.

54. Customer Functional Testing – OnCall Records

Task Description

The Customer, with support from Hexagon, will test OnCall Records Subsystem's conformance with the Benchmark Criteria. The Customer will conduct Functional Testing over the course of ten (10) consecutive Business Days ("Records Testing Period"). During the Records Testing Period, the Customer shall execute the RMS Test Plan and corresponding Test Cases. Except as expressly provided, no other testing or evaluation for OnCall Records is contemplated in this Project. Hexagon and the Customer will jointly document and track the results of each Test Case as either pass or fail.

Within five (5) Business Days of the end of the RMS Testing Period ("RMS Reporting Period"), the Customer shall file any Blocker Defects and Permissive Defects encountered during Functional Testing – Records through Hexagon's Customer Resource Management (CRM) system. For any Blocker Defect identified, the Customer shall provide, at minimum, the following information: a description of the Defect and the steps used to reproduce it, the functionality tested when the Blocker Defect was encountered, the manner in which the functionality was tested, and the outcome when the functionality was tested. If the Blocker Defects are not filed within the RMS Reporting Period, it is presumed Functional Testing was completed without any Blocker Defect, and this Task is complete. Only Blocker Defects reported by the conclusion of the Reporting Period will be resolved as part of this Task. The existence of Permissive Defect(s) shall not preclude or be a condition of completion of any subsequent Tasks or implementation of a new Release.

To the extent requested, Customer agrees to promptly respond to requests for additional information regarding the Blocker Defect requested by Hexagon. Upon diagnosing the Blocker Defect and validating the Defect encountered meets the attributes of a Blocker Defect, Hexagon resources shall proceed to resolve the Blocker Defect accordingly. If the investigation determines the reported Blocker Defect did not meet the attributes of a Blocker Defect then the reported Defect will be reclassified in accordance with the levels provided in the Master Terms Glossary. Alternatively, if the investigation shows the reported Blocker Defect was caused by Customer hardware, Network Infrastructure, or Third-Party Software not provided by Hexagon, or non-conformance with Attachments E and F, then Hexagon will provide such information to the Customer for the Customer to resolve, and the Blocker Defect will be closed and regarded as complete.

As part of its resolution efforts, Hexagon may at its discretion provide a procedural or programmatic work around, a configuration change, or provide an Update. Once the Blocker Defect(s) is addressed, Hexagon will report to Customer the Blocker Defect has been addressed and the Customer will have five (5) Business Days to execute its Test Plan ("RMS Resolution Testing Period") to validate the fix provided by Hexagon has resolved the Blocker Defect.

Task Deliverables

- OnCall Records Functional Testing
- System Code Freeze

Task Prerequisites

- Customer and Hexagon mutually confirm that OnCall Records is ready for testing.
- Test Plan and Test Cases Development – OnCall Records Task is complete.
- Custom Interface Product Installation and Configuration Task is complete.
- The Customer has installed and configured at least one (1) workstation per tester.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Verify OnCall Records is ready for Functional Testing.
- Provide support during Functional Testing.
- Review Defects identified in the Blocker Report by the Customer; and
- Resolve Blocker Defects identified in the Blocker Report.

Customer Team Participation and Responsibilities

Customer shall:

- Verify OnCall Records is ready for Functional Testing.
- Execute the RMS Test Plan;
- Track and document results from executed Test Cases and provide Hexagon a Blocker Report; and
- If applicable or desired, re-execute Test Cases during the Resolution Testing Period.

Task Acceptance Criteria

This Task is complete upon expiration of the RMS Testing Period and resolution of all Blocker Defects reported by the end of the RMS Reporting Period.

Training Phase

55. Hexagon-Led Training

Task Description

During the Training phase, Hexagon resources will conduct Administrative and Train-the-Trainer sessions for Customer-designated personnel.

The following formal training classes are included in the Project (“Hexagon Training Classes”):

- HxGN OnCall Dispatch System Administrator Training – Qty: 1
- HxGN OnCall Dispatch Train-the-Trainer – Qty: 1
- HxGN OnCall Dispatch Train-the-User – Qty: 4
- HxGN OnCall Dispatch | Mobile Unit Train-the-Trainer – Qty: 2
- HxGN OnCall Dispatch | Mobile Responder Train-the-Trainer
- HxGN OnCall Records Train-the-Trainer – Qty: 1
- HxGN OnCall Records NIBRS Report Generation Training (Qty: 1)
- [redacted] Integration Developer Training – Qty: 1

It is recommended that Customer develop its own training program, including, but not limited to: creating a training plan suitable for its needs, identifying a training cadre for each Subsystem, and leveraging the Hexagon training materials and Documentation to ensure its Users have acquired the necessary knowledge and are in a position to use OnCall Dispatch and OnCall Records upon Cutover. The Customer is solely responsible for training its Users. The Customer shall complete its User Training no later than sixty (60) calendar days after Hexagon has completed the Hexagon Training Classes (“End User Training Period”).

Task Deliverables

- Training course agendas
- Applicable COTS Documentation, in electronic format; for the Hexagon Training Classes

Task Prerequisites

- Customer has identified and secured an appropriate training room and set up with the workstations, at least one (1) LCD projector, display screen or other appropriate surface to display a projected image, and white-board space or other ability to take notes and record questions.
- The Customer has installed and configured at least one (1) workstation per student attending the session.
- Customer Functional Testing Tasks for each Subsystem are complete.

Task Assumptions

- The Customer will complete end user training within the End User Training Period.
- Both end-user training and train-the trainer training will be provided as specifically identified herein. Training will take place during normal Business Hours, which is typically from 8:00 am - 5:00 pm.

- Training documentation provided by Hexagon with this SOW will be standard COTS Documentation and help files and will not be customized to the Customer's site-specific configuration. All Documentation will be provided in electronic format. Should printed copies be required, the Customer is responsible for providing them.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Conduct Hexagon Training Classes.

Customer Team Participation and Responsibilities

Customer shall:

- Provide appropriate facilities and install/configure workstations as indicated in the Task Assumptions;
- Provide a Project Workstation for each attendee of the Hexagon Training Classes;
- Ensure appropriate personnel participate in the Hexagon Training Courses; and
- Complete end user training within the End User Training Period.

Task Acceptance Criteria

This Task is complete once Hexagon has delivered the Hexagon Training Classes to the Customer.

56. Test and Training Environment Creation

Task Description

Following completion of all testing Tasks, Hexagon will create the Test and Training Environments using a snapshot of the Production Ready System. As part of this Task, Hexagon will test the Test and Training Environments to verify the Production Ready System has been properly loaded. For clarification, this testing is not intended to repeat or overlap with Customer Functional Testing Tasks.

Task Deliverables

- Test and Training Environment installed

Task Prerequisites

- Test and Training [redacted] is available.
- The System is a Production Ready System.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Install and test the Hexagon System in the Test and Training Environments.

Customer Team Participation and Responsibilities

Customer shall:

- Provide IT support, as required; and
- Provide hardware, database software, operating system software, network, and physical site necessary for creation of Test Environment.

Task Acceptance Criteria

This Task is complete when the System has been installed and tested in the Test and Training Environments.

Cutover Phase

57. Cutover Plan

Task Description

Hexagon and the Customer will jointly develop a Cutover Plan. The Cutover Plan will detail the steps necessary to cutover the Subsystems. The Cutover Plan will assign tasks and responsibilities to both Hexagon and Customer personnel in the month prior to Cutover. The Cutover Plan covers topics including Customer staffing, movement of equipment into final locations, final database cleanout of test events, procedures to report issues, and planned sequence of events for the Cutover day.

Hexagon will provide the initial draft of the Cutover Plan to the Customer for review. The Customer will review the draft and provide feedback to Hexagon within ten (10) Business Days, which will incorporate appropriate feedback into a final Cutover Plan.

Task Deliverables

- Cutover Plan

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Create a draft Cutover Plan (i.e., prepare a checklist of responsibilities and tasks to be completed during the Cutover Task prior to Cutover);
- Work with Customer personnel to refine the Cutover Plan; and
- Review and approve the final Cutover Plan.

Customer Team Participation and Responsibilities

Customer shall:

- Review and comment on the draft Cutover Plan within ten (10) Business Days of receipt;
- Work with Hexagon personnel to refine the Cutover Plan; and
- Review and approve the final Cutover Plan.

Task Acceptance Criteria

This Task is complete when the Customer has reviewed and approved the final Cutover Plan.

58. System Readiness Review

Task Description

During this Task Hexagon technical resources, the Hexagon Project Manager, and the Customer team will meet and determine if the OnCall Subsystems are ready for Cutover.

In addition, the System Readiness Review verifies that the following has occurred:

- A document titled, “Cutover Plan” has been developed and approved by both Hexagon and the Customer;
- Establishment and approval of a schedule for Cutover Activities; and
- Identification and scheduling of Hexagon and Customer resources required for Cutover Activities.

Task Deliverables

- Readiness Review meeting minutes
- Discussion notes on the results from Hexagon’s final review of the system

Task Prerequisites

- Cutover Plan Task is complete.

Task Assumptions

- The Customer certifies it has trained all personnel who will be utilizing the system.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Conduct a conference call to discuss if the system is ready to perform Cutover;
- Provide system Cutover notification to appropriate internal and external interface stakeholders supplying systems integral to Cutover operations;
- Review and provide timely feedback/approval of Cutover Plan; and
- Work with Customer to determine suitable Cutover schedule.

Customer Team Participation and Responsibilities

Customer shall:

- Participate in the conference call;
- Notify internal and external interface stakeholders about pending Cutover;
- Review and provide timely feedback/approval of Cutover Plan; and
- Work with Hexagon to determine suitable Cutover schedule.

Task Acceptance Criteria

This Task is complete when the Readiness Review has been conducted.

59. OnCall Dispatch Final Data Conversion

Task Description

Hexagon will perform a final data conversion of legacy data in the three weeks following cutover to production use of OnCall Dispatch.

Task Deliverables

- Final OnCall Dispatch Data Conversion

Task Prerequisites

- OnCall Dispatch Data Conversion Auditing Task is complete.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Conduct the final OnCall Dispatch data conversion.

Customer Team Participation and Responsibilities

Customer shall:

- Ensure SMEs who understand the structure and use of legacy data are available to work with the Hexagon CAD Data Conversion Implementer for the duration of this task.

Task Acceptance Criteria

This Task is considered complete when Hexagon has conducted the final OnCall Dispatch data conversion.

60. Cutover to Production Use

Task Description

Cutover reflects the culmination of all the Tasks in this SOW. It reflects the point at which the Customer first uses the System in a live environment for its intended purpose.

The Parties shall execute the Cutover Plan, as practical, as part of Cutover. Beginning on Monday of the week of Cutover, Hexagon resources and the Project Manager will support the Customer's Activities leading to Cutover, during Cutover, and post-Cutover. The Hexagon team shall be on site throughout the entire week of Cutover, Monday through Friday On the day of Cutover and the three (3) days immediately following Cutover, Hexagon shall have a CAD and RMS implementer at the Customer Site on a twenty-four (24) hour cycle. The Project Manager will be on site during the week of Cutover during business hours (except on the actual day of Cutover where an alternate schedule will be in place). Upon Cutover, the Customer's System Administrator will assume primary responsibility of the management and administration of the System, and the Hexagon resources will provide support as needed by the Customer System Administrator. At times where the Hexagon resources are not otherwise available after the Project is complete, the Customer shall contact Hexagon's HelpDesk in accordance with the Maintenance Terms within the Agreement.

Cutover also marks the commencement of the Warranty Period for the Project Software as described in Attachment K. .

Task Deliverables

- Cutover of Dispatch and Records Subsystems (simultaneously)

Task Prerequisites

- All prior Tasks are complete.
- The End User Training Period is complete.

Task Assumptions

- The Parties have agreed Cutover can proceed.
- Cutover will take place on the day and time specified in the Cutover Plan.
- Both Subsystems will cutover on the same day.
- Hexagon will provide resources on site.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Hexagon shall provide technical resource(s) to support Cutover during the week of Cutover.

Customer Team Participation and Responsibilities

Customer shall:

- Ensure availability of trained Users;
- Ensure availability of Core Team during Cutover Activities;

- Assume System Administration and management for the System upon Cutover;
- Ensure availability of all third-party vendors impacted by the Cutover;
- Ensure availability of all IT disciplines necessary to immediately address issues as necessary; and
- Ensure availability of member(s) of the training cadre during all shifts.

Task Acceptance Criteria

This Task is complete upon Cutover of the Subsystems.

61. Post-Cutover Support

Task Description

During this Task, Hexagon resources will provide Post-Cutover support to Customer. The “Post-Cutover Support Period” is the two (2) Business weeks beginning the Monday following Cutover. It is designed to provide the Customer with dedicated, quickly accessible support for questions and Defects encountered following the Cutover to Production use of the new System. During the first week of Post Cutover Support Period, the Hexagon resources will work onsite. Hexagon will perform its obligations during second week of the Post Cutover Support Period remotely.

During this Task, Hexagon resources will be assigned Defects that are filed by the Customer against the new System. Hexagon resources will work to identify and address the Defects reported, understanding the Defects will be triaged based upon their severity during the Post Cutover Support Period. Defects remaining after the Post Cutover Support Period will be addressed by the Help Desk. Defects reported outside of Business Hours will be addressed in accordance with the maintenance provisions of the Agreement.

The Post-Cutover Support Period is not a configuration period. Requests for new configurations that are not related to addressing a Defect will not be supported during this time frame. This is done to ensure the stability of the System delivered and that focus remains on Defects and to minimize the introduction of new opportunities for errors or problems.

Task Deliverables

- Task Completion Form confirming that Post-Cutover Support has been provided in accordance with SOW Post-Cutover Support task description

Task Prerequisites

- System Cutover to Production Use Task is complete.

Task Assumptions

- Post-Cutover Support is provided Monday-Friday during normal Business Hours. Standard after-hours emergency support procedures, defined in the Cutover Plan, remain the same for the duration of this Task.
- Defects will be reported via Hexagon’s designated CRM tool.
- The Customer System Administrator remains the primary point of contact and initial troubleshooting point of contact for all issues during this Task.
- The Customer System Administrator maintains responsibility for core system administration tasks.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide ten (10) Business Days of Post-Cutover support in accordance with this SOW; and
- Address Defects within the Post Cutover Support Period.

Customer Team Participation and Responsibilities

Customer shall:

- Ensure Defects are recorded in Hexagon’s CRM tool in a timely manner and in accordance to the mutually agreed upon Project Schedule.

Task Acceptance Criteria

This Task is complete when the Post-Cutover Support Period has expired.

62. OnCall Records NIBRS Certification

Task Description

This Task defines the services required for NIBRS Validation and Reporting Qualification via OnCall Records.

Task Prerequisites

- Post-Cutover Support Task is complete.

Task Assumptions

- NIBRS validation will utilize production data.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Assist Customer with the NIBRS certification process; and
- After certification is achieved, install NIBRS in the Production Environment.

Customer Team Participation and Responsibilities

Customer shall:

- Ensure System Administrator is available to support all tasks.

Task Acceptance Criteria

This Task is complete when NIBRS certification has been achieved.

62. OnCall Dispatch Subsystem 30-Calendar Day Reliability Test

Task Description

The Reliability Period Task is designed to demonstrate the stability of the OnCall Dispatch Subsystem following Cutover ("Dispatch Reliability Period"). During the Reliability Period, the OnCall Dispatch Subsystem shall operate without a Blocker Defect for a total of thirty (30) calendar days. Once the Blocker Defect is resolved (either through configuration, reasonable work around, or a programmatic code change), the Customer shall have two (2) business days to test the resolution. Once resolved or the testing period has expired, the Dispatch Reliability Period shall resume from the prescribed point in time. The first fifteen (15) days of the Reliability Period is regarded as Phase 1 and the second fifteen days (days 16-30) are regarded as Phase 2 of the Reliability Period. Once the System has operated for fifteen (15) consecutive days without a valid Blocker Defect, then Phase 1 of the Reliability Period is complete and Phase 2 of the Reliability Period shall commence and conclude once it has operated from Day 16 to Day 30 without a valid Blocker Defect. If a valid Blocker Defect is logged during Phase 1, then once the Blocker Defect is resolved, the Reliability Period will resume at the first day of Phase 1 of the Reliability Period (i.e. day 1). If a valid Blocker Defect is logged during Phase 2, then once the Blocker Defect is resolved, the Reliability Period will resume at the first day of Phase 2 of the Reliability Period (i.e. day 16).

Requests for new configurations not related to addressing a Blocker Defect cannot be supported during this time frame. Similarly, the Customer shall refrain from making any configuration changes until the Dispatch Reliability Period is complete.

Task Deliverables

- Customer support for Blocker Defects

Task Prerequisites

- Cutover to Production Use Task is complete.

Task Assumptions

- Support is provided Monday through Friday during normal business hours. Standard after-hours emergency support procedures remain the same for the duration of this Task.
- This Task is only for the OnCall Dispatch Subsystem.
- Blocker Defects will be reported via the Help Desk Portal.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- The designated Hexagon CAD implementer will coordinate addressing post-live Blocker Defects with the Customer; and
- Resolve valid Blocker Defects.

Customer Team Participation and Responsibilities

Customer shall:

- Use and monitor the Hexagon OnCall Dispatch Subsystem in a production environment;
- Maintain a log of problems found;
- Contact Hexagon personnel in a timely manner in the event of system problems or failures; and
- Begin system monitoring in support of the Extended Warranty period.

Task Acceptance Criteria

This Task is complete after the OnCall Dispatch Subsystem completes the Dispatch Reliability Period.

63. HxGN OnCall Dispatch | Smart Advisor Follow-up Workshop 1

Task Description

- Within thirty (30) days following Cutover for OnCall Dispatch, Hexagon will conduct a one (1) Day workshop with Customer to provide guidance to optimize Customer's specific Smart Advisor workflows ("Smart Advisor Follow-up Workshop 1").

Task Deliverables

- Smart Advisor Follow-up Workshop 1

Task Prerequisites

- Customer has Cutover OnCall Dispatch and obtained historical data

Task Assumptions

- The Smart Advisor Follow-up Workshop 1 shall last no more than one (1) Business Day

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide guidance to Customer on use of Smart Advisor and Smart Advisor agent configurations

Customer Participation and Responsibilities

Customer shall:

- Provide desired use cases for Smart Advisor at least ten (10) business days prior to the start of the workshop.
- Participate in workshop and
- Go through their experiences and current outputs from Smart Advisor.

Task Acceptance Criteria

This Task is complete upon the earlier of: (i) completion of Smart Advisor Follow-up Workshop 1 or (ii) thirty (30) calendar days following Cutover for OnCall Dispatch.

64. HxGN OnCall Dispatch | Smart Advisor Follow-up Workshop 2

Task Description

Following Smart Advisor Follow-up Workshop 1 and no later than sixty (60) calendar days after Cutover for Dispatch, Hexagon will conduct a second one (1)-day workshop with Customer about optimization of Customer's specific Smart Advisor workflows ("Smart Advisor Follow-up Workshop 2"). If Smart Advisor Follow-up Workshop 1 was not performed and is otherwise accepted in accordance with the Task Acceptance Criteria in that Task, then this Task will be omitted from the scope with neither Party having any obligation under this Task.

Task Deliverables

- Smart Advisor Follow-up Workshop 2

Task Prerequisites

- Customer has used Smart Advisor for sixty (60) days in a production environment.
- Smart Advisor Follow-up Workshop 1

Task Assumptions

- The Smart Advisor Follow-up Workshop 2 shall last no more than one (1) Business Day.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Provide guidance to customer on best use of Smart Advisor and Smart Advisor agent configurations

Customer Participation and Responsibilities

Customer shall:

- Participate in workshop, bringing example use cases; and
- Go through their experiences and current outputs from Smart Advisor.

Task Acceptance Criteria

Provided Smart Advisor Follow-up Workshop 1 was performed, this Task is complete upon the earlier of: (I) conclusion of the Smart Advisor Follow-up Workshop 2 or (ii) sixty (60) days after Cutover for OnCall Dispatch.

Attachment A – Pricing Summary

OnCall Dispatch and Oncall Records (On-Premise)	Total
Software:	
OnCall Dispatch Software	$2,247,115
OnCall Records Software	$654,748
Services:	
OnCall Dispatch Project Implementation	$1,250,280
OnCall Records Project Implementation	$965,476
Mobile Responder Implementation	$19,916
OnCall Dispatch Training Environment Implementation	$8,845
Additional support for 60-day Customer End User Training (CAD/RMS)	$31,758
Additional services for expanded Data Conversions (CAD/RMS)	$40,567
OnCall Dispatch Train-the-User (48 Users)	$158,963
OnCall Mobile Unit Training for EMS	$33,429
Smart Advisor Software and Services	$46,961
Custom Interfaces:	
OnCall Dispatch Custom Interfaces	$90,416
OnCall Records Custom Interfaces	$258,628
Other:	
Performance Bond	$116,744
Escrow	$614
Base System Total Software and Services	$5,924,460
Initial Recurring Maintenance/Extended Warranty - Year 1	$773,847
System Total including First Year Maintenance	**$6,698,307**
Additional Discount (expires 12/31/24)	($450,000)
OnCall Offered Price	**$6,248,307**
Annual Recurring Fees	
Annual Recurring Maintenance Fee – Year 2	$804,801
Annual Recurring Maintenance Fee – Year 3	$836,993
Annual Recurring Maintenance Fee – Year 4	$870,473
Annual Recurring Maintenance Fee – Year 5	$905,292
Optional OnCall Recurring Years 6-10	

Annual Recurring Maintenance Fee – Year 6	$941,503
Annual Recurring Maintenance Fee – Year 7	$979,163
Annual Recurring Maintenance Fee – Year 8	$1,018,330
Annual Recurring Maintenance Fee – Year 9	$1,059,063
Annual Recurring Maintenance Fee – Year 10	$1,101,426

Pricing Assumptions

- This offer is valid through December 31, 2024. The discount may be adjusted depending on changes that are made to the base offered solution.
- This price is assuming a combined project (CAD and LERMS). If the Customer chooses to complete the projects separately, Hexagon reserves the right to reprice system integration services costs.
- The pricing provided assumes production, test, and disaster recovery (backup) environments. A training environment for OnCall Dispatch has also been included in the offered price.
- Project Implementation Services included in the price shown are inclusive of project management, implementation, TTT training services, and related travel.
- An RMS data conversion from the legacy OneSolution has been provided. This assumes conversion of up to [redacted] If additional conversion services are needed, Hexagon can price them at the time of the request.
- The Dynamo Curriculum E-Learning licenses included in this pricing for twelve (24) named users for implementation team training are for a 12-month subscription term beginning when the Dynamo licenses are issued.
- Pricing for base software licensing is based on the information provided by the Customer and the Hexagon concurrent licensing model. Please see the included Bill of Materials in SOW Attachment A for license counts included in this proposal. After further discussions with the Customer, this pricing and the client counts may be adjusted.
- Third party software and services are included in the base system total cost; some of these third parties start their software maintenance at cutover and others upon shipment. All have been included in the pricing appropriately based on an assumed 26-month project timeline. If for any reason this timeline is exceeded, there may be additional costs which the Customer would be required to pay for third parties.
- Software Maintenance & Support - Year 2 represents the 12-month maintenance period which begins at the first anniversary of Subsystem Cutover to live operations. Year 2 Maintenance can be purchased at the prices set forth in the table above subject to the composition of Software and quantities remaining the same. Any adjustments to the composition of the System will have a corresponding effect on future maintenance pricing. Year 2 Maintenance would be subject to a separate agreement.
- Rights to receive Software Updates are included in annual maintenance costs. Hexagon Services to assist with implementing the Update can be priced at the time of the request under a separate agreement.
- Sales taxes are not included in this quote. Final sales tax billed will reflect the applicable tax rates at time of sale as required by law.

Bill of Materials

Description	Quantity
Hexagon OnCall Software	
CAD Software	
HxGN OnCall Dispatch - Backup NL	1
[redacted]Integration Runtime Engine NL	1
[redacted]Integration Developer Engine NL	1
HxGN OnCall Dispatch - RestAPI NL	2
HxGN OnCall Dispatch - RestAPI NL - Training	1
HxGN OnCall Dispatch - Viewer CC	90
HxGN OnCall Dispatch - Advantage CC	15
HxGN OnCall Dispatch - Advantage CC - Training License	9
HxGN OnCall Dispatch - Advanced Mapping	15
HxGN OnCall Dispatch - Resource Management	15
HxGN OnCall Dispatch - Resource Management - TRN License	9
HxGN OnCall Dispatch - [redacted] Interface	15
HxGN OnCall Dispatch - [redacted] Interface - Training	9
HxGN OnCall Dispatch - [redacted]Map Control	15
HxGN OnCall Dispatch - Customer Rules Engine - Advantage	15
HxGN OnCall Dispatch - Customer Rules Engine - Editor	1
HxGN OnCall Dispatch - Customer Rules Engine - Server	10
HxGN OnCall Dispatch - Dashboard CC	25
HxGN OnCall Analytics - Dispatch Advantage NL 4 Core	1
HxGN OnCall Analytics - Dispatch Advantage NL Add 2 Core	2

Description	Quantity
Mobile Software	
HxGN OnCall Dispatch - Mobile Unit	297
HxGN OnCall Mobile Server	5
HxGN OnCall Dispatch - Mobile Responder Client CC	125
Smart Advisor Software	
HxGN OnCall Dispatch - Smart Advisor	15
HxGN OnCall Dispatch - Smart Advisor Mobile	297
LERMS Software	
[redacted] - Integration Runtime Engine NL - Additional License	1
HxGN OnCall Records - Concurrent User License	139
HxGN OnCall Analytics - Records Essentials NL 4 Core	1
HxGN OnCall Analytics - Records Essentials NL Add 2 Core	2
HxGN OnCall Records - Citizen Reporting	18
Interfaces	
CAD Interfaces	
HxGN OnCall Dispatch - Informer	1
HxGN OnCall Dispatch - Tracker CC	500
HxGN OnCall Dispatch - Call-Taker Interface	2
HxGN OnCall Dispatch - Notifications	1
HxGN OnCall Dispatch - Fire Link Interface	2
HxGN OnCall Dispatch - CAD Link Interface	1
HxGN OnCall Dispatch - [redacted] Interface	1
HxGN OnCall Dispatch - PTT	1
Fire Station Alerting OnCall Dispatch Interface	1

Description	Quantity
Dispatch Alerts OnCall Interface	2
External Alarms OnCall Dispatch Interface	1
PLT Radio OnCall Dispatch Interface	1
CAD to CAD OnCall Dispatch Interface	1
[redacted]OnCall Call-Taker Interface	1
CAD Interface to [redacted](Address Query)	1
CAD Interface for [redacted](Address Query)	1
CAD Interface to [redacted](Address Query)	1
CAD Interface for [redacted](Intrado)	1
CAD Interface to [redacted]	1
Consulting Services for [redacted]	1
LERMS Interfaces	
HxGN OnCall Records-NIBRS Report & Validate -TX	1
RMS Interface to NCIC	1
RMS Interface for TDEX	1
RMS Interface to [redacted]	1
RMS interface for [redacted]	1
RMS interface for Cris	1
RMS Interface for [redacted]	1

Description	Quantity
HxGN Connect	
HxGN Connect Live Share	5
HxGN Connect Tenant Access	1

Description	Quantity
HxGN Connect Live Share - Smart Advisor	5
HxGN Connect Smart Advisor - Incident Agents	1
HxGN Connect Interface - Incident API	1
HxGN Connect Interface - Unit API	1
HxGN Connect Gateway - Subscription	1
HxGN Connect Interface - OnCall Dispatch - Subscription	1

Attachment B – Payment Schedule

The total value of the Order is $6,248,307, which is the basis for the payment milestones.

Milestone Payment Schedule		
MS (#)	**Milestone Deliverable**	**MS (%)**
1	Upon Completion of Task #1: Project Kickoff Meeting	10.00%
2	Upon Completion of Task #13: [redacted] and OnCall Software Staging	15.00%
3	Upon Completion of Task #19: OnCall Dispatch System Build #2	10.00%
4	Upon Completion of Task #23: OnCall Dispatch Configuration Consulting #1	10.00%
5	Upon Completion of Task #36: OnCall Records System Configuration Workshop 2	10.00%
6	Upon Completion of Task #25: OnCall Dispatch Configuration Consulting #3	10.00%
7	Upon Completion of Task #53: Customer Functional Testing - OnCall Dispatch	10.00%
8	Upon Completion of Task 55: Hexagon Led Training	5.00%
9	Upon Completion of Task #60: Cutover to Production Use	10.00%
10	Upon Completion of Task #62: CAD Reliability Period	10.00%
	Total	**100.00%**

Attachment C – Initial Project Schedule.

Task Name	Duration	Business Days Since Start
Williamson County, TX Project Plan	**636.5 days**	**0 days**
Planning Phase	**636.5 days**	**0 days**
Project Kickoff Meeting	**4.5 days**	**20 days**
COTS Interface Questionnaire Completion	**5.5 days**	**28.25 days**
OnCall Dispatch Launch	**6.5 days**	**29.5 days**
OnCall Dispatch GIS Requirements Review	**1.13 days**	**29.5 days**
OnCall Records Business Process Analysis (BPA) Workshop	**7.5 days**	**29.5 days**
Custom Interface Requirements Gathering	**34 days**	**24.5 days**
OnCall Records Custom Interface Requirements Gathering (ICDs)	**34 days**	**24.5 days**
RMS Interface to NCIC	**15.13 days**	**24.5 days**
Customer reviews ICD	10 days	26.13 days
Customer approves ICD	3 days	36.63 days
RMS Interface for TDEX	**22.13 days**	**26.13 days**
Customer reviews ICD	10 days	34.25 days
Customer approves ICD	3 days	45.25 days
RMS Interface to [redacted]	**15.13 days**	**34.25 days**
Customer reviews ICD	10 days	35.88 days
Customer approves ICD	3 days	46.38 days
RMS interface for Cris	**16.13 days**	**35.88 days**
Customer reviews ICD	10 days	38.25 days
Customer approves ICD	3 days	49 days
RMS interface for [redacted]	**18.13 days**	**38.25 days**
Customer reviews ICD	10 days	42.38 days
Customer approves ICD	3 days	53.38 days
RMS Interface for [redacted]	**16.13 days**	**42.38 days**
Customer reviews ICD	10 days	44.5 days
Customer approves ICD	3 days	55.5 days
OnCall Dispatch Custom Interface Requirements Gathering (ICDs)	**19.88 days**	**24.5 days**

CAD Interface to [redacted] (Address Query)	**14.63 days**	**24.5 days**
Customer reviews ICD	10 days	25.63 days
Customer approves ICD	3 days	36.13 days
CAD Interface for [redacted] (Address Query)	**14.63 days**	**25.63 days**
Customer reviews ICD	10 days	26.75 days
Customer approves ICD	3 days	37.25 days
CAD Interface to [redacted] (Address Query)	**14.63 days**	**26.75 days**
Customer reviews ICD	10 days	27.88 days
Customer approves ICD	3 days	38.38 days
CAD Interface for Text to 911 (Intrado)	**16.38 days**	**27.88 days**
Customer reviews ICD	10 days	30.25 days
Customer approves ICD	3 days	41.25 days
CAD Interface to [redacted]	**14.13 days**	**30.25 days**
Customer reviews ICD	10 days	31.13 days
Customer approves ICD	3 days	41.38 days
Custom Interface Development	**68.38 days**	**0 days**
OnCall Records Custom Interface Development	**68.38 days**	**0 days**
RMS Interface to NCIC	**10 days**	**39.63 days**
RMS Interface for TDEX	**2 days**	**48.25 days**
RMS Interface to [redacted]	**5 days**	**49.38 days**
Anti Bias Reporting (TX)	**5 days**	**52 days**
RMS interface for Cris	**12 days**	**56.38 days**
RMS interface for [redacted]	**8.5 days**	**58.5 days**
RMS Interface for [redacted]	**5 days**	**0 days**
OnCall Dispatch Custom Interface Development	**8.13 days**	**39.13 days**
CAD Interface to [redacted] (Address Query)	**2.5 days**	**39.13 days**
CAD Interface for [redacted] (Address Query)	**2.5 days**	**40.25 days**
CAD Interface to [redacted] (Address Query)	**2.5 days**	**41.38 days**
CAD Interface for Text to 911	**3 days**	**44.25 days**
CAD Interface to [redacted]	**2.5 days**	**44.38 days**
OnCall Dispatch Data Conversion Analysis and Mapping	**14 days**	**24 days**
OnCall Dispatch Data Conversion Scripting	**64 days**	**43.27 days**

OnCall Dispatch Data Conversion Audit	**10 days**	**107.27 days**
OnCall Records Data Conversion	**599.5 days**	**37 days**
Staging Phase	**100.63 days**	**20 days**
Physical Infrastructure Installation	**1 day**	**20.25 days**
[redacted]**Server and OnCall Software Staging**	**22.02 days**	**21.25 days**
OnCall Dispatch GIS Consulting	**21.13 days**	**43.27 days**
OnCall Records State NIBRS Validation Installation	**3 days**	**43.27 days**
OnCall Records Address Server Mapping Configuration	**7.5 days**	**44.27 days**
OnCall Dispatch System Build 1	**16.6 days**	**59.4 days**
OnCall Dispatch System Build 1	3 days	63 days
Customer Build Out of Remaining Data	10 days	66 days
OnCall Dispatch Deployment and Response Planning Workshop	**15 days**	**81 days**
OnCall Dispatch Deployment and Response Planning Workshop	3 days	83 days
Customer Build Out of Remaining Data	10 days	86 days
OnCall Dispatch System Build 2	**19 days**	**101 days**
OnCall Dispatch System Build 2	3 days	107 days
Customer Build Out of Remaining Data	10 days	110 days
Configuration Phase	**626 days**	**0 days**
OnCall Dispatch Fundamentals for Core Team	**6 days**	**125 days**
COTS Interface Product Installation and Configuration	**8.25 days**	**120.63 days**
OnCall Dispatch | [redacted]	**3.25 days**	**125.63 days**
OnCall Dispatch | [redacted]**Installation**	**1 day**	**125.63 days**
CommSys ConnectCIC Installation	**5.25 days**	**128.88 days**
OnCall Dispatch Configuration Consulting 1	**18 days**	**136 days**
OnCall Dispatch Configuration 1 Workshop	3 days	141 days
Customer configures OnCall Dispatch	7 days	147 days
OnCall Dispatch Configuration Consulting 2	**15 days**	**159 days**
OnCall Dispatch Configuration 2 Workshop	3 days	161 days
Customer configures OnCall Dispatch	7 days	167 days
OnCall Dispatch Configuration Consulting 3	**18.25 days**	**179 days**
OnCall Dispatch Configuration 3 Workshop	3 days	184.25 days

Customer configures OnCall Dispatch	7 days	190.25 days
OnCall Dispatch Customer Rules Engine Configuration Workshop	**15.75 days**	**202.25 days**
CRE Configuration Workshop	3 days	205 days
Customer configures CRE	10 days	208 days
Hexagon - Automated Case Number Assignment CRE Workflow	0.5 days	208 days
OnCall Dispatch | Mobile Unit Configuration Consulting Session - Law/Fire	**15 days**	**223 days**
OnCall Dispatch | Mobile Unit Law/Fire Configuration Session	3 days	225 days
Customer configures OnCall Dispatch | Mobile Unit	10 days	228 days
OnCall Dispatch | Mobile Unit Configuration Consulting Session - EMS	**17 days**	**234 days**
OnCall Dispatch | Mobile Unit EMS Configuration Session	3 days	238 days
Customer configures OnCall Dispatch | Mobile Unit	10 days	241 days
OnCall Dispatch | Mobile Responder Configuration - Law	**2 days**	**228 days**
OnCall Dispatch | Mobile Responder Law Configuration	1 day	228 days
OnCall Dispatch | Mobile Responder Configuration - Fire	**2 days**	**241 days**
OnCall Dispatch | Mobile Responder Fire Configuration	1 day	241 days
Smart Advisor Configuration Workshop	**2 days**	**251 days**
Smart Advisor Workshop	1 day	252 days
OnCall Records Fundamentals for Core Team	**6 days**	**120 days**
OnCall Records Fundamentals for Core Team	4 days	122 days
OnCall Records System Configuration Workshop 1	**14 days**	**136 days**
OnCall Records Configuration Workshop 1	4 days	141 days
Customer configures OnCall Records	5 days	145 days
OnCall Records System Configuration Workshop 1 Follow-up Session	**10 days**	**145 days**
OnCall Records COTS Reports Review	**3 days**	**150 days**
OnCall Records System Configuration Workshop 2	**15 days**	**165 days**
OnCall Records Configuration Workshop 2	4 days	171 days
Customer configures OnCall Records	5 days	175 days
OnCall Records System Configuration Workshop 2 Follow-up Session	**10 days**	**175 days**

OnCall Records System Configuration Workshop 3	**14 days**	**195 days**
OnCall Records Configuration Workshop 3	4 days	200 days
Customer configures OnCall Records	5 days	204 days
OnCall Records System Configuration Workshop 3 Follow-up Session	**10 days**	**209 days**
OnCall Citizen Reporting System Configuration Workshop	**15 days**	**214 days**
OnCall Citizen Reporting System Configuration Workshop Follow-up Session	**5 days**	**234 days**
OnCall Records State NIBRS Reporting Installation	**2 days**	**46.27 days**
Additional Agencies Cloning	**15 days**	**444.75 days**
OnCall Dispatch Archive Database Staging	**0.25 days**	**43.27 days**
OnCall Analytics - Dispatch Configuration	**7 days**	**197.25 days**
OnCall Analytics - Records Configuration	**421.88 days**	**197.25 days**
OnCall Analytics|Admin and User Training - CAD	**13.75 days**	**204.25 days**
HxGN OnCall Analytics - Admin and User Training	3 days	210 days
OnCall Analytics|Admin and User Training - Records	**13.88 days**	**612.13 days**
HxGN OnCall Analytics - Admin and User Training	3 days	618 days
Custom Interface Product Installation and Configuration	**26 days**	**154 days**
OnCall Records Custom Interfaces	**25 days**	**155 days**
RMS Interface to NCIC	**5 days**	**155 days**
RMS Interface for TDEX	**2 days**	**160 days**
RMS Interface to [redacted]	**2 days**	**162 days**
Anti Bias Reporting (TX)	**10 days**	**164 days**
RMS interface for Cris	**2 days**	**174 days**
RMS interface for [redacted]	**3 days**	**176 days**
RMS Interface for [redacted]	**1 day**	**179 days**
OnCall Dispatch Custom Interfaces	**13 days**	**154 days**
CAD Interface to [redacted] (Address Query)	**3 days**	**154 days**
CAD Interface for [redacted] (Address Query)	**3 days**	**157 days**
CAD Interface to [redacted] (Address Query)	**3 days**	**160 days**
CAD Interface for Text to 911 (Intrado)	**3 days**	**163 days**
CAD Interface to [redacted]	**1 day**	**166 days**
Standard Interface Product Installation and Configuration	**10 days**	**197.25 days**

CAD to CAD OnCall Dispatch Interface [redacted]	**10 days**	**197.25 days**
Fire Station Alerting OnCall Dispatch Interface [redacted]	**1 day**	**197.25 days**
Dispatch Alerts OnCall Interface [redacted]	**1 day**	**197.25 days**
Dispatch Alerts OnCall Interface [redacted]	**1 day**	**197.25 days**
External Alarms OnCall Dispatch Interface [redacted]	**3 days**	**197.25 days**
PLT Radio OnCall Dispatch Interface [redacted]	**1 day**	**197.25 days**
[redacted] Call-Taker Interface	**1 day**	**197.25 days**
Consulting Services and Vendor Views	**1 day**	**197.25 days**
Consulting Services for [redacted]	**1 day**	**197.25 days**
Testing Phase	**318.75 days**	**126 days**
Test Plan and Test Cases Development - OnCall Dispatch	**150 days**	**131 days**
Customer Creation of Test Plan and Test Cases	150 days	131 days
Customer Provides Test Plan and Test Cases to Hexagon	0 days	281 days
Test Plan and Test Cases Development - OnCall Records	**150 days**	**126 days**
Customer Creation of Test Plan and Test Cases	150 days	126 days
Customer Provides Test Plan and Test Cases to Hexagon	0 days	276 days
Customer Functional Testing - OnCall Dispatch	**105 days**	**334.75 days**
Customer Functional Testing	10 days	334.75 days
Customer Provides Blocker Error Report	5 days	344.75 days
Customer Executes Test Plan Post Blocker Error Resolution	5 days	434.75 days
Customer Functional Testing - OnCall Records	**100 days**	**344.75 days**
Customer Functional Testing	10 days	344.75 days
Customer Provides Blocker Error Report	5 days	354.75 days
Customer Executes Test Plan Post Blocker Error Resolution	5 days	439.75 days
Training Phase	**105.25 days**	**444.75 days**
Hexagon-Led Training	**62.25 days**	**444.75 days**
HxGN OnCall Dispatch System Administrator Training	**7.25 days**	**444.75 days**
HxGN OnCall Dispatch | Train the Trainer	**13 days**	**452 days**
HxGN OnCall Dispatch | Train the User #1	**13 days**	**452 days**
HxGN OnCall Dispatch | Train the User #2	**10 days**	**465 days**
HxGN OnCall Dispatch | Train the User #3	**10 days**	**475 days**
HxGN OnCall Dispatch | Train the User #4	**13 days**	**485 days**

OnCall Dispatch | Mobile Unit Train-the-Trainer	**9.25 days**	**444.75 days**
OnCall Dispatch | Mobile Unit Train-the-Trainer (EMS)	**9 days**	**454 days**
OnCall Dispatch | Mobile Responder Train-the-Trainer	**2 days**	**459 days**
OnCall Records Train-the-Trainer	**7.25 days**	**444.75 days**
[redacted]Developer Training	**6 days**	**498 days**
OnCall Citizen Reporting Train-the-Trainer (TTT)	**5 days**	**498 days**
State NIBRS Report Generation Training	**3 days**	**504 days**
Customer-Led End User Training (60 calendar days)	**42 days**	**508 days**
Disaster Recovery, Test, and Training Environment Creation	**10.25 days**	**444.75 days**
Cutover Phase	**73.25 days**	**550 days**
Cutover Plan	**11.63 days**	**550 days**
Hexagon Delivers Draft Cutover Plan	0.13 days	551 days
Customer Reviews and Approves Cutover Plan	10 days	551.13 days
System Readiness Review	**1 day**	**561.63 days**
OnCall Dispatch Final Data Conversion	**10 days**	**562.63 days**
Cutover to Production Use	**20.25 days**	**563 days**
Post-Cutover Support	**20 days**	**583.25 days**
Post Cutover Support Week 1 - Onsite	**5 days**	**583.25 days**
Post Cutover Support Week 2 - Onsite	**5 days**	**588.25 days**
30 Day Reliability	**5 days**	**593.25 days**
OnCall Records NIBRS Certification	**40 days**	**583.25 days**

Attachment D – Training Curriculum

HxGN OnCall Dispatch | Advantage System Administrator Training (Qty: 1)

The HxGN OnCall Dispatch | Advantage System Administrator course is a four-day, hands-on training class on how to configure and manage the OnCall system. During this course, the students will learn how to access the OnCall database and use available tools to administer and configure the system.

MAJOR TOPICS

- Understanding the Environment
- Map Legend Management
- UI Editor
- Localized Strings
- Layout Manager
- Notification Configuration
- Custom Fields
- Parameter Management
- Deployment Configuration
- Response Plans Configuration
- Role Management
- Type Codes Management
- Agency Management
- Geographic
- Resources
- Change Management

PREREQUISITES

- Customer Environment fully staged and available
- HxGN OnCall Dispatch | Advantage fully licensed, staged, and available
- Credentials available
- Hexagon user account provisioned with local administrator rights on all appropriate servers and workstations

TRAINING DETAILS

Method	Conducted on site by Hexagon Personnel
Target Audience	Personnel responsible for administering and supporting the system
Duration	Four (4) Business Days
Student Capacity	Six (6), with a maximum of one (1) student per workstation

HxGN OnCall Dispatch | Advantage Train-the-Trainer (Qty: 1)

HxGN OnCall Dispatch | Advantage Train-the-Trainer is a four (4)-day comprehensive course to familiarize communications personnel with the use of OnCall. Students will learn all of the essential functions of OnCall including navigating the application, entering and updating events, performing inquiries, handling units including updates and status changes, and communicating with other users. An introduction to the use of interfaces to such things as NCIC, state crime databases, and mobile units is also presented, if the interfaces are available. Students completing the course should have a good working knowledge of using HxGN OnCall Dispatch | Advantage.

This course also includes three (3) additional days of consulting to guide the Customer in developing its training plan and materials for end users.

MAJOR TOPICS

- Events – Creation, Updates, and Status Changes
- Mapping – Commands, Controls, and Views
- Units – Status Changes and Properties Updates
- Inquiries – Events, Units, and Employees
- Messaging – Send, Receive, and Attachments
- Using training guidelines and techniques for HxGN OnCall Dispatch | Advantage

PREREQUISITES

- Customer Environment fully staged and available
- HxGN OnCall Dispatch | Advantage fully licensed, staged, and available
- Credentials available
- Hexagon user account provisioned with local administrator rights on all appropriate servers and workstations

TRAINING DETAILS

Method	Conducted on site by Hexagon Personnel
Target Audience	Personnel responsible for training call-taking and dispatching staff
Duration	Four (4) Business Days
Student Capacity	Twelve (12), with a maximum of one (1) student per workstation

HxGN OnCall Dispatch | Advantage Train-the-User (Qty: 4)

HxGN OnCall Dispatch | Advantage Train-the-User is a four-day comprehensive course to familiarize communications personnel with the use of OnCall. Students will learn all of the essential functions of OnCall including navigating the application, entering and updating events, performing inquiries, handling units including updates and status changes, and communicating with other users. An introduction to the use of interfaces to such things as NCIC, state crime databases, and mobile units is also presented, if the interfaces are available. Students completing the course should have a good working knowledge of using HxGN OnCall Dispatch | Advantage.

MAJOR TOPICS

- Events – Creation, Updates, and Status Changes
- Mapping – Commands, Controls, and Views
- Units – Status Changes and Properties Updates
- Inquiries – Events, Units, and Employees
- Messaging – Send, Receive, and Attachments

PREREQUISITES

- Customer Environment fully staged and available
- HxGN OnCall Dispatch | Advantage fully licensed, staged, and available
- Credentials available
- Hexagon user account provisioned with local administrator rights on all appropriate servers and workstations

TRAINING DETAILS

Method	Conducted on site by Hexagon Personnel
Target Audience	Call-taking and dispatching end users
Duration	Four (4) Business Days
Student Capacity	Twelve (12), with a maximum of one (1) student per workstation

HxGN OnCall Dispatch | Mobile Unit Train-the-Trainer (Qty: 1)

COURSE OVERVIEW

HxGN OnCall Dispatch | Mobile Unit Train-the-Trainer is a two (2)-day comprehensive course to familiarize trainers with the operation and use of the HxGN OnCall Dispatch | Mobile Unit software. Trainers will learn all of the essential functions of HxGN OnCall Dispatch | Mobile Unit including navigating the application, creating, receiving and updating events, utilizing the map, performing inquiries, handling units including updates and status changes, and communicating with other users. Multiple agency-specific operations are also covered, including Law Enforcement related updates. Trainers completing the course should have a good working knowledge of HxGN OnCall Dispatch | Mobile Unit.

This course also includes four (4) additional days of consulting to guide the Customer in developing its training plan and materials for end users.

MAJOR TOPICS

- Create, receive and update active events
- Update active unit status and properties
- Submitting inquires for events and units
- Submitting and receiving messages
- Create and receive HxGN OnCall Dispatch | Informer queries from HxGN OnCall Dispatch | Mobile Unit
- Using training guidelines and techniques for HxGN OnCall Dispatch | Mobile Unit

PREREQUISITES

- Customer mobile hardware fully staged and available
- HxGN OnCall Dispatch | Advantage and HxGN OnCall Dispatch | Mobile Unit fully licensed, staged, and available
- Credentials available
- Hexagon user account provisioned with local administrator rights on all servers and workstations
- Customer Data collection spreadsheets completed
- HxGN OnCall Dispatch | Advantage and HxGN OnCall Dispatch | Mobile Unit fully staged and available on the trainer's workstation

COURSE DETAILS

Method	Conducted on site by Hexagon Personnel
Target Audience	Personnel responsible for training the field personnel that respond to CAD events (Law)
Duration	Two (2) Business Days
Student Capacity	Twelve (12), with a maximum of one (1) student per workstation

HxGN OnCall Dispatch | Mobile Unit Train-the-Trainer (Fire/EMS) (Qty: 1)

COURSE OVERVIEW

HxGN OnCall Dispatch | Mobile Unit Train-the-Trainer (Fire/EMS) is a one (1)-day comprehensive course to familiarize trainers with the operation and use of the HxGN OnCall Dispatch | Mobile Unit software. Trainers will learn all of the essential functions of HxGN OnCall Dispatch | Mobile Unit including navigating the application, creating, receiving and updating events, utilizing the map, performing inquiries, handling units including updates and status changes, and communicating with other users. Multiple agency-specific operations are also covered, including Fire and EMS related updates. Trainers completing the course should have a good working knowledge of HxGN OnCall Dispatch | Mobile Unit.

This course also includes four (4) additional days of consulting to guide the Customer in developing its training plan and materials for end users.

MAJOR TOPICS

- Create, receive and update active events
- Update active unit status and properties
- Submitting inquires for events and units
- Submitting and receiving messages
- Create and receive HxGN OnCall Dispatch | Informer queries from HxGN OnCall Dispatch | Mobile Unit
- Using training guidelines and techniques for HxGN OnCall Dispatch | Mobile Unit

PREREQUISITES

- Customer mobile hardware fully staged and available
- HxGN OnCall Dispatch | Advantage and HxGN OnCall Dispatch | Mobile Unit fully licensed, staged, and available
- Credentials available
- Hexagon user account provisioned with local administrator rights on all servers and workstations
- Customer Data collection spreadsheets completed
- HxGN OnCall Dispatch | Advantage and HxGN OnCall Dispatch | Mobile Unit fully staged and available on the trainer's workstation

COURSE DETAILS

Method	Conducted on site by Hexagon Personnel
Target Audience	Personnel responsible for training the field personnel that respond to CAD events (Fire/EMS)
Duration	One (1) Business Day
Student Capacity	Twelve (12), with a maximum of one (1) student per workstation

HxGN OnCall Dispatch | Mobile Responder Train-the-Trainer (Qty: 1)

Mobile Responder training is a Train-the-Trainer course designed to train Agency trainers in the use of the Mobile Responder product.

MAJOR TOPICS

- Using Mobile Responder on Smartphone or tablet
- Changing unit status
- Submitting inquiries
- Sending and receiving messages
- Updating unit properties
- Updating events
- Informer queries

PREREQUISITES

- Responsibility for mobile computing operations
- Assignment of at least one person who has been through OnCall Dispatch training to perform necessary dispatching and other CAD functions
- Availability of customer specific Mobile Responder configuration
- Availability of test or training Mobile Responder smartphone or tablet for use in class

TRAINING DETAILS

Method	Conducted on site by Hexagon Personnel
Target Audience	Designed for Mobile Responder Trainers
Duration	One (1) day, but can be changed depending on customer needs
Student Capacity	12

HxGN OnCall Records Train-the-Trainer (Qty: 1)

This course provides training for the agency-designated trainers. All modules will be reviewed and related to each department in the agency such as Records, Patrol, Investigations, Evidence, and other departments. The users review the modules, searching capabilities, reporting, and other features in OnCall Records.

MAJOR TOPICS

- Navigating in OnCall Records
- Understanding the OnCall Records tabs: Hone, Reports, Search, Master Indices, Investigations, Court, Jail Management, Traffic, Evidence Management, Department, and Other Info
- Understanding the Master Indices (Master Name, Master Vehicle, Master Location)
- Reviewing the OnCall Records Modules
- Understanding the Master Indices (Master Name, Master Vehicle, Master Location
- Linking data
- Configuring alerts
- Exporting search results
- Setting alerts
- Understanding workflow
- Combining Master Index records
- Using canned and Report Server reports
- Using the Record Properties menu
- Using the Records Linked menu

PREREQUISITES

- Introduction to Windows course or equivalent knowledge and familiarity with the Windows user interface
- Understanding of basic Public Safety terminology
- Knowledge of agency business processes
- Agency modules to be used have been identified
- OnCall Records configuration complete
- OnCall Records Acceptance Testing complete

TRAINING DETAILS

Method	Conducted on site by Hexagon Personnel
Target Audience	Agency trainers or end users
Duration	Four (4) Business Days
Student Capacity	Twelve (12), with a maximum of one (1) student per workstation

HxGN OnCall Records NIBRS Report Generation Training (Qty: 1)

This course provides training for key personnel on the utilization of Hexagon NIBRS Reporting client.

MAJOR TOPICS

- Understanding the Statute table for NIBRS reporting
- Understanding the mastcode table for NIBRS Data Elements
- Navigating the Incident and Arrest/Juvenile Contact modules to identify NIBRS Data Elements for entry
- Review of Federal Data Elements
- Clearing NIBRS Validation errors
- Navigating the NIBRS Thin Client
- Generating monthly NIBRS reports
- Submitting monthly NIBRS reports
- Complex scenarios
- Understanding workflow

PREREQUISITES

- NIBRS Reporting Installation Task complete
- OnCall Records configuration complete
- OnCall Records Customer Functional Testing complete

TRAINING DETAILS

Method	Conducted remotely by Hexagon Personnel
Target Audience	Agency end users
Duration	Two (2) Business Days
Student Capacity	Twelve (12), with a maximum of one (1) student per workstation

[redacted] Training (Qty: 1)

This [redacted] training course is designed for customers who have purchased an [redacted] license who have an interest in configuring their own [redacted] The Training class will be comprised of general [redacted] training and API specific training. Students will receive both classroom training and hands-on experience enabling them to build and manage interfaces using [redacted] and the CAD/RMS API.

Upon successful completion, trainees will be able to take the core concepts/fundamentals and be able to configure simple-to-moderate interfaces in [redacted] With the foundational knowledge provided, trainees will be able to continue to use [redacted] and build more complex interfaces over time, as that is the primary way to become a truly proficient user.

Please note the stated prerequisites and student capacity, as strict adherence is essential to the successful completion of this course.

MAJOR TOPICS

General [redacted] Knowledge

- Developing and deploying [redacted] Systems
- Understanding the Data Structures
- Business Rules Implementation
- Linking Systems together via Publish/Subscribe and Receive/Inject
- Generating / Consuming XML
- Advanced Knowledge Topics (topics will be customized to address customer interface needs)

API Knowledge

- Understanding the specific API functionality available
- Using [redacted] to communicate to the API
- Subscribing to Topics
- Subscribing to logs

PREREQUISITES

Trainees will need a laptop or computer with the [redacted] installed. In addition, strong adherence to the following prerequisites is mandatory:

- Responsibility for the administration, support, and maintenance of [redacted] and the systems/interfaces built within the application.
- Technical understanding of databases, [redacted], and network communications.
- Working knowledge of [redacted] This includes major networking components, including clients, servers, local area networks, network ports, and protocols.

TRAINING DETAILS

Method	Conducted on site by Hexagon Personnel
Target Audience	[redacted] User/Implementer
Duration	Four (4) days
Student Capacity	4-8, with a maximum of 1 student per workstation

Attachment E-1 – OnCall Dispatch Specifications

[following this page]

HxGN OnCall® Dispatch Suite

System Specifications

Release date: November 2024
Release version: 10.00.2409
Release type: On-premises and cloud
Released by: Hexagon Global Technology Center
Release method: Hexagon Global Software Delivery Process

Copyright

Terms of Use

By installing, copying, downloading, accessing, viewing, or otherwise using the Subject Product, you agree to be bound by the terms of the EULA found *here* (*https://legaldocs.hexagon.com/sig/Licenses/EULA_SA_SIG-Eng_062023.pdf*).

Disclaimers

Hexagon and its suppliers believe the information in this publication is accurate as of its publication date. Hexagon is not responsible for any error that may appear in this document. The information and the software discussed in this document are subject to change without notice.

Language Translation Disclaimer: The official version of the documentation is in English. Any translation of this document into a language other than English is not an official version and has been provided for convenience only. Some portions of a translation may have been created using machine translation. Any translation is provided "as is.” Any discrepancies or differences occurring in a translation versus the official English version are not binding and have no legal effect for compliance or enforcement purposes. Hexagon disclaims any and all warranties, whether express or implied, as to the accuracy of any translation.

Reasonable efforts have been made to provide an accurate translation; however, no translation, whether automated or provided by human translators is perfect. If any questions arise related to the accuracy of the information contained in a translated version of documentation, please refer to its official English version. Additionally, some text, graphics, PDF documents, and/or other accompanying material may not have been translated.

Links to Third-Party Websites

This document may provide links to third-party websites for your convenience and information. Third-party websites will be governed by their own terms and conditions. Hexagon does not endorse companies or products to which it links.

Third-party websites are owned and operated by independent parties over which Hexagon has no control. Hexagon shall not have any liability resulting from your use of the third-party website. Any link you make to or from the third-party website will be at your own risk and any information you share with the third-party website will be subject to the terms of the third-party website, including those relating to confidentiality, data privacy, and security.

Hexagon provides access to Hexagon international data and, therefore, may contain references or cross references to Hexagon products, programs and services that are not announced in your country. These references do not imply that Hexagon intends to announce such products, programs or services in your country.

Trademarks

"Hexagon,” “Hexagon Safety, Infrastructure & Geospatial,” “Intergraph,” the Hexagon logo, and the Intergraph logo are registered trademarks of Hexagon AB or its subsidiaries.

Other brands and product names are trademarks of their respective owners.

Revisions

Hexagon reserves the right to revise these terms at any time. You are responsible for regularly reviewing these terms. Your continued use of this document after the effective date of such changes constitutes your acceptance of and agreement to such changes.

Contact Us

Contact us https://hexagon.com/company/contact-us with any questions regarding these terms.

Contents

Overview of System Specifications

This document provides the specifications for hardware required to support the HxGN OnCall® Dispatch system.

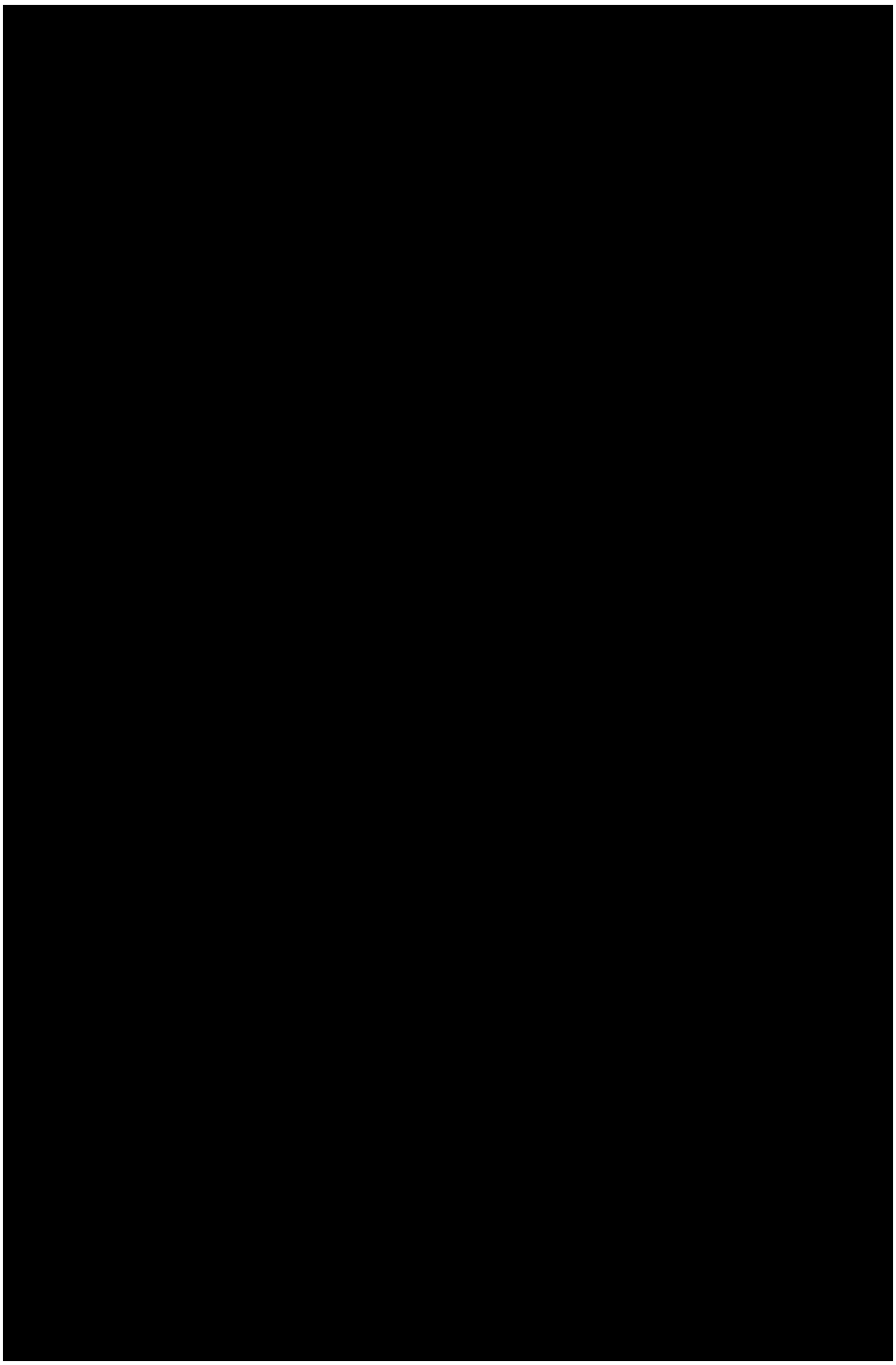
Hexagon's Safety, Infrastructure & Geospatial division has developed the following hardware requirements with the best possible performance and safety in mind. These requirements are intended to provide the required performance during a large incident.

All recommendations, specifications, or directions are based on certain assumptions and theoretical facts, and are not definitive. Prior to final reliance, it is necessary to test all such recommendations, specifications, and directions against actual anticipated use/load, actual configuration/customization, actual interfaces, actual workflows, and other such particulars; and, it is further necessary to make such adjustments as are dictated by appropriate evaluation of test results.

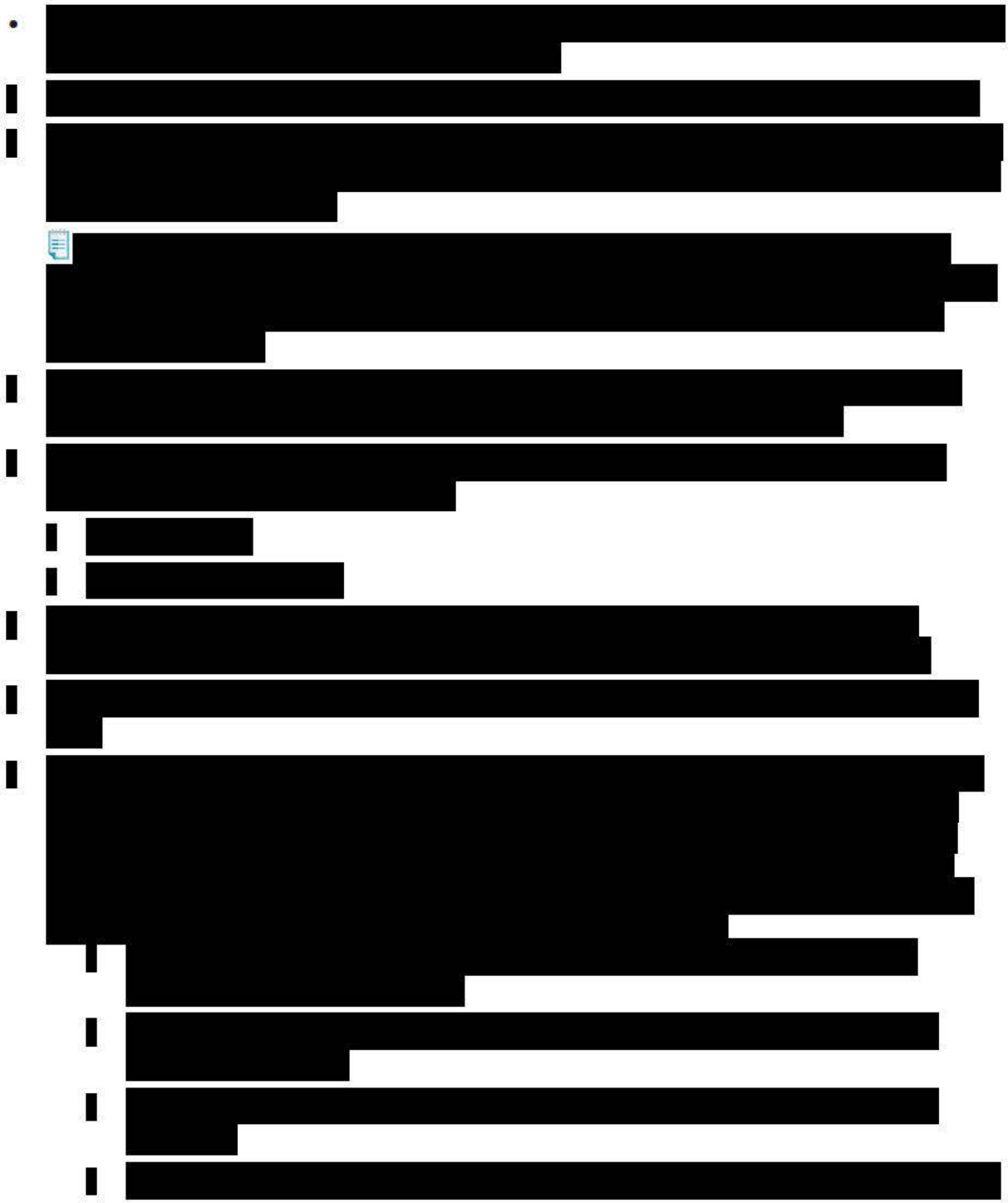
[redacted]

[redacted]

[redacted]



Additional Mobile Server Information



[redacted]

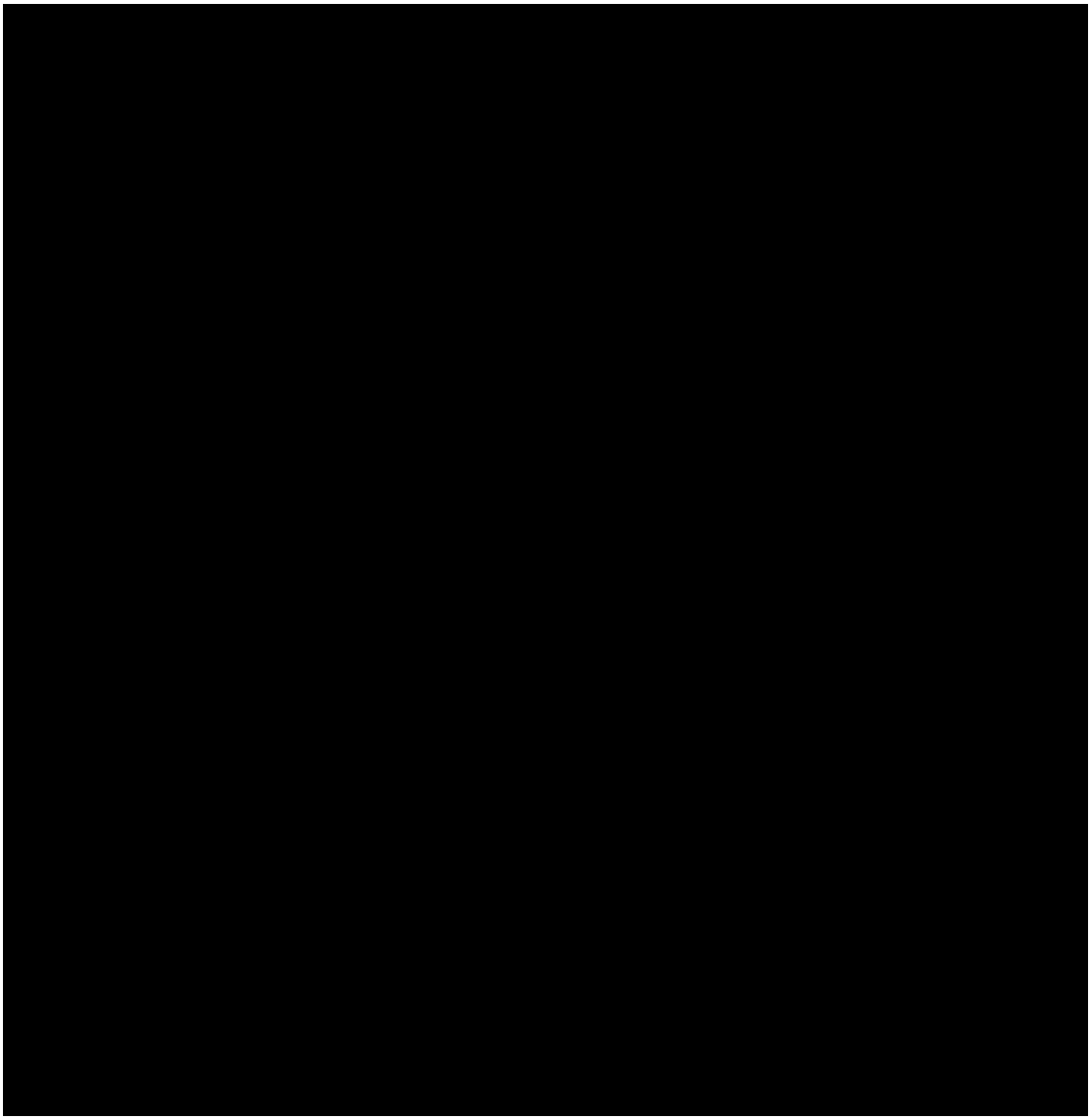
[redacted]

HxGN OnCall Dispatch Client Specifications

The following specifications apply to both browser users and Electron application users.

For information on the browsers that were verified for this release, see the *HxGN OnCall Dispatch Supported Environments*.

HxGN OnCall Dispatch Clients



HxGN OnCall Dispatch | Mobile Unit Clients

HxGN OnCall Dispatch | Mobile Responder Clients

The following are the supported client devices for the Mobile Responder (also known as HxGN OnCall® Mobile) application:

- [redacted]
- [redacted]

Certification has been performed on a limited number of devices due to the diversity in [redacted] Testing has been performed with the platforms and devices listed at the beginning of this section. While other devices are viable, Hexagon recommends testing with a single device before purchasing large quantities.

[redacted]

HxGN OnCall Dispatch | Tracker GPS Specifications

For information on Tracker GPS protocols, see the *HxGN OnCall Dispatch | Tracker GPS Format Guide*.

Video Responder and Security Guardian Specifications

The client specifications match the OnCall Dispatch client specifications outlined in this document. However, for those systems where clients will be heavily relying on video, it is strongly recommended that all clients have [redacted] for optimal performance when dealing with streamed video. For servers, use the appropriate, standard OnCall Dispatch specifications.

Technical Support

[redacted]

Submit a Case Online

[redacted]

[redacted]

Attachment E-2 – OnCall Records Specifications

[following this page]

HxGN OnCall® Records

System Requirements

Release date: 5/13/2022
Release version: 10.0
Release type: On-premises
Released by: Hexagon Global Technology Center
Release method: Hexagon Global Software Delivery Process

Copyright

Terms of Use

By installing, copying, downloading, accessing, viewing, or otherwise using the Subject Product, you agree to be bound by the terms of the EULA found *here* (*https://www.hexagonsafetyinfrastructure.com/-/media/Legal/Hexagon/SI/Licenses/EULA_SA_SIG-Eng_062021.pdf*).

Disclaimers

Hexagon and its suppliers believe the information in this publication is accurate as of its publication date. Hexagon is not responsible for any error that may appear in this document. The information and the software discussed in this document are subject to change without notice.

Language Translation Disclaimer: The official version of the documentation is in English. Any translation of this document into a language other than English is not an official version and has been provided for convenience only. Some portions of a translation may have been created using machine translation. Any translation is provided "as is.” Any discrepancies or differences occurring in a translation versus the official English version are not binding and have no legal effect for compliance or enforcement purposes. Hexagon disclaims any and all warranties, whether express or implied, as to the accuracy of any translation.

Reasonable efforts have been made to provide an accurate translation; however, no translation, whether automated or provided by human translators is perfect. If any questions arise related to the accuracy of the information contained in a translated version of documentation, please refer to its official English version. Additionally, some text, graphics, PDF documents, and/or other accompanying material may not have been translated.

Links to Third Party Websites

This document may provide links to third party websites for your convenience and information. Third party websites will be governed by their own terms and conditions. Hexagon does not endorse companies or products to which it links.

Third party websites are owned and operated by independent parties over which Hexagon has no control. Hexagon shall not have any liability resulting from your use of the third party website. Any link you make to or from the third party website will be at your own risk and any information you share with the third party website will be subject to the terms of the third party website, including those relating to confidentiality, data privacy, and security.

Hexagon provides access to Hexagon international data and, therefore, may contain references or cross references to Hexagon products, programs and services that are not announced in your country. These references do not imply that Hexagon intends to announce such products, programs or services in your country.

Trademarks

"Hexagon,” “Hexagon Safety & Infrastructure,” “Intergraph,” the Hexagon logo, and the Intergraph logo are registered trademarks of Hexagon AB or its subsidiaries.

Other brands and product names are trademarks of their respective owners.

Revisions

Hexagon reserves the right to revise these terms at any time. You are responsible for regularly reviewing these terms. Your continued use of this document after the effective date of such changes constitutes your acceptance of and agreement to such changes.

Contact Us

Contact us (*https://www.hexagonsafetyinfrastructure.com/contact-us*) with any questions regarding these terms.

Contents

Overview

This document describes the system requirements for HxGN OnCall® Records from Hexagon's Safety, Infrastructure & Geospatial division.

System Requirements

Prerequisites

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Database Server

[redacted]

Application Server

Client Workstations

Attachment F – System Configuration Diagram

[following this page]

HEXAGON

Williamson County, TX
OnCall Dispatch & OnCall Records
Hardware & Software Configuration

December 2024

System Overview

Color Legend

Black – Base products
Red – Optioned products
Green – Customer-furnished products

TABLE OF CONTENTS

[redacted]

[redacted]

[redacted]

HEXAGON

Williamson County, TX
OnCall Dispatch & OnCall Records
Hardware & Software Configuration

December 2024

Hardware Specifications

Color Legend

Black – Base products
Red – Optioned products
Green – Customer-furnished products

Production

[redacted]

Disaster Recovery

[redacted]

HEXAGON

Williamson County, TX
OnCall Dispatch & OnCall Records
Hardware & Software Configuration

December 2024

Client Hardware Specifications

Color Legend

Black – Base products
Red – Optioned products
Green – Customer-furnished products

[redacted]

HEXAGON

[redacted]

Williamson County, TX
OnCall Dispatch & OnCall Records
Hardware & Software Configuration

December 2024

OnCall Dispatch Architectural Diagram

Color Legend

Black – Base products
Red – Optioned products
Green – Customer-furnished products

[redacted]

HEXAGON

Williamson County, TX
OnCall Dispatch & OnCall Records
Hardware & Software Configuration

December 2024

OnCall Records Architectural Diagram

Color Legend

Black – Base products
Red – Optioned products
Green – Customer-furnished products

[redacted]

HEXAGON

Williamson County, TX
OnCall Dispatch & OnCall Records
Hardware & Software Configuration

December 2024

OnCall Dispatch Management & Mapping Environments

Color Legend

Black – Base products
Red – Optioned products
Green – Customer-furnished products

Production

OnCall Management Environment

Disaster Recovery

OnCall Management Environment

[redacted]

HEXAGON

Williamson County, TX
OnCall Dispatch & OnCall Records
Hardware & Software Configuration

December 2024

OnCall Dispatch Production Environment

Color Legend

Black – Base products
Red – Optioned products
Green – Customer-furnished products

[redacted]

HEXAGON

Williamson County, TX
OnCall Dispatch & OnCall Records
Hardware & Software Configuration

December 2024

OnCall Dispatch Disaster Recovery Environment

Color Legend

Black – Base products
Red – Optioned products
Green – Customer-furnished products

[redacted]

HEXAGON

Williamson County, TX
OnCall Dispatch & OnCall Records
Hardware & Software Configuration

December 2024

CAD Test & Training Environments

Color Legend

Black – Base products
Red – Optioned products
Green – Customer-furnished products

OnCall Dispatch Test Environment

OnCall Dispatch Training Environment

[redacted]

HEXAGON

Williamson County, TX
OnCall Dispatch & OnCall Records
Hardware & Software Configuration

December 2024

RMS Production Environment

Color Legend

Black – Base products
Red – Optioned products
Green – Customer-furnished products

[redacted]

HEXAGON

Williamson County, TX
OnCall Dispatch & OnCall Records
Hardware & Software Configuration

December 2024

RMS Disaster Recovery Environment

Color Legend

Black – Base products
Red – Optioned products
Green – Customer-furnished products

[redacted]

HEXAGON

Williamson County, TX
OnCall Dispatch & OnCall Records
Hardware & Software Configuration

December 2024

RMS Test Environment

Color Legend

Black – Base products
Red – Optioned products
Green – Customer-furnished products

OnCall Records Test Environment

[redacted]

HEXAGON [redacted]

Williamson County, TX
OnCall Dispatch & OnCall Records
Hardware & Software Configuration

December 2024

Notes

Color Legend

Black – Base products
Red – Optioned products
Green – Customer-furnished products

Client Notes:

1. OnCall Dispatch Advantage can use the Customer's map source via a URL provided by the Customer. However, Hexagon recommends the Customer have a dedicated highly available separate instance of the map for OnCall to access.

General Notes:

1. Hexagon assumes that the Local Area Network (LAN), the wide area network (WAN), Active Directory, and Domain Name System (DNS) infrastructure will be provided and staged by the Customer. Each web client connection consumes roughly [redacted], so the network between the clients and the web server must have sufficient capacity to handle all concurrent clients.
2. All workstations, PCs, laptops, and specified peripheral hardware provided by the Customer are assumed to meet the specifications delineated on this diagram.
3. Hexagon assumes that the Customer will provide WAN communications, including wireless network communications.
4. [redacted].
5. The hardware specifications provided in this diagram do not account for the capacity that may be required for converted data.
6. [redacted]
7. This Configuration Diagram illustrates the proposed hardware and software configuration at the time of submission. During implementation, the Hexagon Implementation Team, or a Hexagon subcontractor, may alter this configuration to reflect the negotiated system or alter the location of software to take advantage of efficiencies determined following submission.
8. Non-production interface licenses are available for proposed interfaces. However, implementation is subject to Customer's ability to provide connection to the applicable system. All third-party external interface connections required for non-production Environments are the responsibility of the Customer and/or third-party vendor(s).
9. The OnCall test environment is sized for functional testing. If the Customer desires to perform load testing in the test environment, then the specifications in this configuration diagram will need to be re-evaluated and adjusted.
10. HxGN OnCall Mobile Server is a no-cost administration tool used to manage the Mobile Responder app.
11. CCU refers to concurrent client user
12. Hexagon assumes that the customer will provide all client access licenses (CALs) to maintain system compliancy with Microsoft policy.
13. [redacted] and associated training courses is included to allow the Customer to be able to create interfaces as they need. [redacted]
14. The Operational Reports component of OnCall Dispatch is normally configured to point to the archive server, [redacted]. For those customers that find this acceptable, the read-only reporting replica is not required. For those that feel the need to have the data pulled directly from live or those that plan to create additional customized operational reports, the read-only replica is recommended to prevent performance impacts from malformed reports.

Attachment G-1 – Exhibit A - CAD/Mobile Functional Specifications Matrix

[following this page]

Item #	Specification
	Global System Features
G-1	Ability for authorized user to perform any system tasks from any authorized workstation.
G-2	Ability to display all times as local time.
G-3	Ability to configure format in which dates are stored.
G-4	Ability to operate in a Windows environment to support concurrent processing.
G-5	Ability to support standard Windows functionality (e.g., shortcuts) throughout all applications in the proposal.
	Ability for system to automatically adjust number sequencing for, but not limited to, the below options:
G-6	Yearly
G-7	Monthly
G-8	Weekly
G-9	Daily
G-10	By Agency
G-11	By Jurisdiction
G-12	Client-defined value
G-13	Ability for system to automatically account for daylight savings time and any required parameter (timestamps, time displays) change to daylight savings.
G-14	Ability to log and display all times in military (24 hour) clock format.
G-15	Ability for all date and timestamps to be system generated.
G-16	Ability to configure all date and timestamps.
G-17	Ability to format all date and timestamps differently by agency.
	Ability to provide the user with feedback as to the success or failure of an action, including, but not limited to:
G-18	Audible alert
G-19	Visual alert
G-20	Other
G-21	Ability to save data to an off-site backup environment.
	Ability to provide seamless integration among system components:
G-22	Within applications (e.g., amongst modules)
G-23	Between applications (e.g., between CAD and agency RMS)
	Geofile and Mapping Requirements

G-24	Ability for CAD and other applications to share the same geofile.
G-25	Ability to import GIS data from an ESRI-based source.
G-26	Ability to export GIS data into an ESRI-based source.
G-27	Ability to read GIS data natively within the application.
G-28	Ability to utilize a regional data hub for source data management.
G-29	Ability to integrate with ESRI ArcGIS REST API for map layers

[redacted]

G-30	Ability to accommodate an unlimited number of map layers.
G-31	Ability to create as many map layers as needed.
G-32	Ability to select multiple map layers for display, limited only by the number of available map layers.
G-33	Ability to turn map layers off and on.
G-34	Ability to alert user that additional information (e.g., layers) is available.
	Ability to associate geofile data with the following:
G-35	Address
G-36	Allowed direction of travel
G-37	Beats
G-38	Census tract
G-39	Cross street
G-40	Entire common place or business name and aliases
G-41	Fire zone box

G-42	Division
G-43	High and low cross streets
G-44	Location type
G-45	Jurisdiction
G-46	Neighborhood
G-47	Reporting district
G-48	Response area
G-49	Sectors
G-50	X/Y coordinates
G-51	Ability to import GIS data from a spatial database into CAD geofile.
G-52	Ability to add geofile layers as needed.
G-53	Ability to force adherence to user-defined addressing standards (e.g., abbreviations, directions, etc.).
	Ability to cross-reference addresses and locations with:
G-54	Entire common place or business name and aliases
G-55	Fire-defined reporting areas
G-56	Law enforcement-defined reporting areas
G-57	Location type
G-58	Other identifiers
G-59	Street aliases

[redacted]

G-60	X/Y coordinates
G-61	X/Y/Z coordinates
G-62	Zip codes
G-63	Ability to validate all location entries against a master geofile either from a geofile mask or from the command line.
G-64	Ability to change reporting boundaries (e.g., areas, beats, districts, etc.).
	Ability to support agency-defined location entries including, but not limited to:
G-65	Airport, including ramps, runways, terminal names and numbers
G-66	Apartment building name
G-67	Apartment number (e.g., ½, #5, 2D, D2)
G-68	Bike paths
G-69	Block range
G-70	Business name
G-71	Census tract
G-72	City
G-73	Civic associations (e.g., COPS areas, neighborhoods, community names)
G-74	Common place name
G-75	County
G-76	District
G-77	Exact address (including fractional addresses, alphanumeric)
G-78	Intersections

[redacted]

G-79	Law enforcement district/sector or fire station
G-80	Limited access roadways and highways
G-81	Mile markers
G-82	Public Transporttion System
G-83	Rail System
G-84	On ramps, off ramps, exit numbers (including directionals)
G-85	Partial/misspelled street names
G-86	Prefix
G-87	Reporting area
G-88	Street abbreviation
G-89	Street alias
G-90	Street name
G-91	Street type
G-92	Suffix
G-93	Trail markers
G-94	Water markings (piers, buoys, nautical navigation, landmarks)
G-95	X/Y coordinates
G-96	X/Y/Z coordinates
G-97	Zip code / Keymap
G-98	Zones

G-99	Ability for a single layer to contain overlapping polygons.
G-100	Ability to summarize geofile entries for printing.
G-101	Ability to test new geofile updates "offline" for accuracy and errors, prior to updating the "live" geofile.
G-102	Ability to flag errors in mapping layers so as to provide data to system administrator for future corrections (e.g., user inserts a flag to indicate a missing block)
G-103	Ability to update the system with a new geofile without system downtime or degradation.
G-104	Ability for geofile updates to be recognized without requiring logging off and logging back on to the system.
G-105	Ability to include overlays and overhead photography in mapping application.
G-106	Ability to attach files to addresses (e.g., apartment maps, photos, aerial images).
G-107	Ability to attach premise information (e.g., hazards) to addresses.
G-108	Ability to connect natively to external data map/web services (e.g., Street View, Google Maps/Earth, ArcGIS map services).
G-109	Ability to click on a location on a map and pull up any supplemental information (e.g. fire pre-plan, hazards, incident history) associated with that location.
G-110	Ability to display flags on locations containing additional information (e.g. fire pre-plans, hazards, incident history).
G-111	Ability to limit the ability to attach files to addresses based on user ID.

G-112	Ability to support a map layer for aerial spatial images.
	Address Validation
G-113	Ability to geoverify location of all entered addresses.
G-114	Ability to override geoverified location.
G-115	Ability to create a report of all overridden geoverified locations.
G-116	Ability to enter addresses outside of clients jurisdiction.
G-117	Ability to support geofile entry of a specific address within a block range.
	System Administration
	Major Functions and Features
G-118	Ability to manage all configuration files, passwords, security tables and interfaces.
G-119	Ability for system administrator to define function keys.
G-120	Ability to assign users to multiple security groups.
G-121	Ability to configure users' windows depending on the user's job function and security level.
G-122	Ability to configure the location of automatically displayed message and dialog boxes, including error messages.
G-123	Automatically displayed message and dialog boxes, including error messages, are consistent throughout the application.
G-124	Ability to monitor network and system performance, notifying agency-defined devices or user account when specific triggers are met.
G-125	Ability to seal and archive records and store sealed records in an archival database.
G-126	Ability to configure the display attributes of automatically displayed message and dialog boxes, including error messages.
	Common editing actions allowed with all fields and data:
G-127	Cut
G-128	Copy
G-129	Paste
G-130	Cut, Copy, Paste between forms
G-131	Insert
G-132	Delete
G-133	Sort
G-134	Print screen
G-135	Tab through form fields
G-136	Back-tab through form fields

G-138	Resize windows
G-139	Find
G-140	Replace
G-141	Ability to use the numeric keypad for number entry
G-142	Ability to use an external numeric keypad for number entry
G-143	Point and click
G-144	Drag and drop
G-145	Drop-down lists
G-146	Vertical scroll bar, when the vertical data displayed is larger than the defined area.
G-147	Ability to configure word wrap, when the horizontal data displayed is larger than the defined area.
G-148	Ability to configure word wrap to break between words, not within words.
G-149	Ability to configure a horizontal scroll bar, when the horizontal data displayed is larger than the defined area.
G-150	Ability to configure a standard spell check on definable narrative fields.
G-151	Ability to remotely log out a workstation (mobile or desktop).
G-152	Ability to remotely lock a workstation (mobile or desktop), requiring a password to unlock.
	Code Tables
G-153	Ability to define codes for drop down menus (e.g., BRO for brown, BLU for blue, etc.).
G-154	Obsolete code table values are not displayed on drop down lists for data entry.
G-155	Ability to maintain the system, including code tables, securely via remote workstations.
G-156	Ability to maintain the system, including code tables, securely via web-based remote workstations.
	Ability to import and export data tables to and from a standard format, but not limited to:
G-157	Spreadsheet
G-158	comma-separated value text file
G-159	[redacted]
G-160	Ability to define codes without character length limitations.
G-161	Ability to define codes using alphanumeric characters.
G-162	Ability to make changes and additions to the code tables without modification to or recompilation of the application software.
G-163	Ability to make changes and additions to the code tables without requiring a workstation restart.

G-164	tables without requiring users to log off and back on.
G-165	Ability to modify code tables without advanced database knowledge.
G-166	Ability to designate code table values as obsolete and unavailable for current use, preventing further entry of that value, yet retain the value in the table for inquiries on historical data.
G-167	Ability to create a new code and merge/link historical records to a new code.
G-168	Ability to store the date a code table value becomes obsolete.
G-169	Ability to store the date a code table value becomes effective.
G-170	Obsolete code table values are not displayed on drop down lists f
G-171	Ability to retain deleted table information with the capability to perform an archive and final purge.
G-172	Ability to share code tables among application components.
G-173	Ability to notify users of code table updates upon logging onto the system after the update is made.
G-174	Ability to notify users of geofile updates upon logging onto the system after the update is made.
	Security Administration
G-175	Ability to create multiple security groups defining who has various levels of audit trail access permissions.
G-176	Ability to restrict access to administrative functions and access by security level (e.g., buttons, windows, etc.).
G-177	Ability to define what information will display on screen by security level (e.g., buttons, windows, etc.)
G-178	Ability to provide role-based security per facilities for authorization functions.
G-179	Ability to list who has access to what modules, functions, and databases.
	Ability to restrict user access or group access to files and data fields for specified transactions:
G-180	Add/create
G-181	Attach to email or send via other electronic method
G-182	Delete
G-183	Inquiry
G-184	Modify
G-185	Print
G-186	View
G-187	Ability to separately secure add, modify, delete, and inquiry functions.
G-188	Ability of system administrator to change user IDs.

	ser profiles based on:
G-189	Agency
G-190	Security group
G-191	User ID
G-192	User name
G-193	Any combination of the above
G-194	Ability to restrict access based on both user and workstation (desktop or mobile).
G-195	Ability to access administrative functions from any workstation, with appropriate security access.
G-196	Ability to prevent users from creating ad hoc reports on fields to which they do not have proper security permissions.
	Documentation and Online Help Requirements
	System Documentation
	Ability to provide a System Administrator's Guide containing:
G-197	All documentation detailing system functions, screen layouts, file structures, linking map, data structure, data dictionary/schema and application program design
G-198	All documentation required to perform all system management functions
G-199	Performance monitoring and troubleshooting
	Ability to provide the System Administrator's Guide:
G-200	In an electronic format
G-201	In printed form
	Ability to provide updates to the System Administrator's Guide as they are developed:
G-202	In an electronic format
G-203	In printed form
	Ability to provide a System User's Guide containing all documentation required by systems users:
G-204	In an electronic format
G-205	In printed form
G-206	"Quick reference" user guide
G-207	Cheat sheets
G-208	FAQ's
	Ability to provide updates to the System User's Guide as they are developed:
G-209	In an electronic format
G-210	In printed form

G-211	Ability to access help menu via either the mouse or a keyboard command.
G-212	Ability to print directly from the online help window.
G-213	Ability to provide context-sensitive help in the form of prompts and instructions.
G-214	Ability to provide context-sensitive help only upon a user request.
G-215	Ability to provide help facility for any operation in progress via a function key from any screen or field within any application.
G-216	Ability to provide help facility via function key or icon from any screen or field within any application.
	Ability to maintain online agency-specific documentation and procedures, including:
G-217	Glossary of terms
G-218	Glossary of error codes
G-219	Software help file updates must not override changes made to help files specific to agency-customized documentation.
G-220	Ability to use context sensitive help when finding information about an item on the screen. User should be able to place the cursor on the item and execute no more than one key stroke to obtain help information.
G-221	Ability to include online help documentation that provides step-by-step instructions on how to use the system.
G-222	Ability to provide training modules through help menu.
G-223	Ability to search help files by keywords.
G-224	Ability to edit text in help files to address agency-specific topics.
	Help File Administration
G-225	Ability for help file to automatically update at the time of all version/release updates.
G-226	Ability for system administrator to create/edit error messages.
G-227	Ability to use different fonts, styles, colors and symbols in help files.
G-228	Ability to track user ID and revision dates when online user documentation is revised/changed.
G-229	Ability to provide help files in a Windows help format.
G-230	Ability to bookmark topics.
	Ability for help file to:
G-231	Include or exclude complete phrase searches
G-232	Include or exclude untitled topic searches
G-233	Include or exclude similarity searches

G-235	Utilize context sensitive help providing brief operational definitions for selected items on a screen
G-236	Ability to augment vendor-supplied online help tables with additional information (e.g., add notes to a topic that are viewable along with the vendor-supplied information).
G-237	Ability for updates to help tables to not override additions made by agency.
	Query and Reporting Features
	Data Warehouse (DW) or Reporting (RPT) Server Capability
G-238	The system maintains a separate external database outside the CAD network; secure, but accessible to CAD users and authorized non-CAD external users.
G-239	The system supports writing CAD record data to the DW/RPT server automatically, real-time, as entered in the CAD system.
G-240	The system provides a method to write the final version of the CAD record data to the DW/RPT server on event closure.
G-241	The DW/RPT server stores all data associated with the event record (e.g., event, unit, remarks).
G-242	The system supports DW/RPT server security that allows view-only rights to the data.
G-243	All external CAD data inquiries can be directed to the DW/RPT server instead of the production server.
G-244	The DW/RPT server platform and storage utilize commercial off-the-shelf (COTS) hardware and software.
G-245	The DW/RPT server supports automatic requests for data from external, previously-approved applications.
G-246	The DW/RPT server supports record- and field-based security to restrict viewing of records and fields based on the assigned role, discipline, and jurisdiction at login (e.g., the DW/RPT server security features allow data related to a Law Enforcement jurisdiction to be accessible only to users that login to the DW/RPT server with that role and department clearly defined).
	Query and Report Generating Tool
	Ability to provide a consistent reporting and query tool that can:
G-247	Create interactive query requests
G-248	Access multiple files/tables in a single query (e.g., data for different years, data for all modules).
G-249	Allow the end user to design screen and report formats

G-251	Create reports from any data in the system
G-252	Define temporary fields which may or may not be output
G-253	De-select records/rows in combination with selection of records.
G-254	Generate a map
G-255	Sort selected records/rows by key/index and non-key/non-index fields
	Ability for query/report generating tool to:
G-256	Allow development of user help facilities at the system level
G-257	Run in background mode
G-258	Support all record accesses allowed by the DBMS
G-259	Support the use of third party query tools
G-260	Ability to provide online help for reporting and query tool.
	Ability to present statistics in graphical formats, including, but not limited to the following:
G-261	Pin maps
G-262	Bar graphs
G-263	Pie charts
G-264	Density maps
G-265	Line graphs
G-266	Thematic maps
G-267	Tables with data banners (i.e., pivot tables, cross-tabs)
G-268	Venn diagrams
G-269	ESRI map based
	Ability for query/report generating tool to handle:
G-270	A full suite of statistical operations
G-271	Arithmetic operations, including fractiles and percentiles
G-272	Logic operations
G-273	Prompted queries
G-274	Ability to dynamically reference map layers to provide geospatial analysis.
	Ability to provide a report-formatting facility that accesses:

G-276	Data formats
G-277	Editing rules for a field
G-278	Field headings
G-279	Field sizes
G-280	Formatting rules
G-281	Ability to include subtotals and totals on ad hoc reports.
G-282	Ability to include incorporated statistical functions (e.g., minimum, maximum, range, average, etc.) into ad hoc reports.
	Query Masks
G-283	Ability to use standard screen formats for all inquiries.
G-284	Ability to use predefined data entry forms/screens (masks).
	Query Return Features
G-285	Ability to narrow down searches (search within a search).
G-286	Ability to select any result from a query and drill down for detailed information (e.g., hyperlink).
G-287	Ability to drill down on query results.
G-288	Ability to set default databases for queries.
G-289	Ability to save queries for later use.
G-290	Ability to save queries to a central "query library."
G-291	Ability for all authorized users to access the general library of user-created ad-hoc reports.
G-292	Ability for system to support automatic data suppression for repetitive data.
	Ability to restrict queries that result in large volumes of data by:
G-293	Providing a warning of the numbers of records found
G-294	Providing a warning of the size of records found
G-295	Requesting users to prompt the system to continue the query
G-296	Requesting users to prompt the system to cancel the query
G-297	Ability to find a specific report by querying any populated field associated with that report.
G-298	Ability to clearly indicate when additional information (e.g., more query returns) is available.
G-299	Ability for query returns to indicate the information source.
G-300	Ability to export query results into a standard tools (e.g., Access, Excel, ArcGIS).
G-301	Ability to identify which query results (e.g., columns) to export.
G-302	Ability to print query returns at any time.
G-303	Ability to design a custom form for query output.
G-304	Ability to direct query results to any printer.
G-305	Ability to direct query results to any terminal.

G-306	d as defined by the system administrator (i.e., first 10 records, etc.).
G-307	Ability to view a specified number of records found as defined by the end user (i.e., first 10 records, etc.).
G-308	Ability to sort query results by any criteria (e.g., most recent to oldest, by priority, etc.).
	Ability to restrict user actions by:
G-309	Displaying a single page of data at a time
G-310	Using prompts to continue/refine/alter the query
G-311	Warning of the number of records found
G-312	Ability to export query returns into other features (e.g., messaging, email).
	Ability to restrict agency-defined query returns from dissemination by the following:
G-313	Email
G-314	Messaging
	Global Report Features
G-315	Ability to create standard reports that can be made available to all system users.
G-316	Ability for users to put their own queries/reports in a "dashboard"
G-317	Ability to generate reports from ad hoc query results.
G-318	Ability to route reports to pre-selected individuals or groups.
G-319	Ability to schedule reports to be automatically created.
G-320	Ability to schedule reports to be automatically electronically distributed.
	Ability to automatically generate user-defined date range reports based on a pre-determined schedule:
G-321	Daily
G-322	Weekly
G-323	Monthly
G-324	Annually (calendar)
G-325	Annually (fiscal)

G-326	Based on request
	Ability to produce standard reports containing, at a minimum, the following:
G-327	Agency logo
G-328	Date and time range for the contents of the report
G-329	Date report was printed
G-330	Page number
G-331	Report author
G-332	Report header with department name
G-333	Specified search parameters (e.g., sector, fire zone boxes, unit ID, etc.)
G-334	Ability to save reports for subsequent viewing and/or printing.
G-335	Ability to scratch/delete reports after viewing and/or printing.
G-336	Ability to optionally generate a report in HTML (i.e., for viewing on the intranet or internet).
G-337	Ability to make standard reports available for publishing on the intranet or internet.
	Ability to export data into each of the following formats (please note any limitations):
G-338	ASCII, comma-delimited
G-339	Compatible with MS Office Suite
G-340	DBF
G-341	ESRI-compatible layer
G-342	HTML
G-343	PDF
G-344	Report Generator
G-345	Rich Text Format
G-346	XML
G-347	XTML
	Global Print Features
G-348	Ability to print all code tables and screens by ranges.
G-349	Ability to prevent the printing of selected information.
G-350	Ability to define printing privileges by security group and/or user ID.
	Ability to selectively print system information:
G-351	Print single record
G-352	Print group/all records
G-353	Print all except specific records
	Ability for print report options to include:
G-354	Cancel report print jobs
G-355	Color/black and white

G-356	Docusign Envelope ID: 7DCA6BAC-F7DA-4880-BCC5-3B479EBAC22C , number of pages)
G-357	Queue reports for later printing
G-358	Select printer
G-359	Select workstation
G-360	Specify number of copies
G-361	Specify page ranges and multiple pages
G-362	Specify portrait or landscape mode, where appropriate
G-363	Ability to identify redacted fields within a printed report.
G-364	Ability to view all reports in a print preview mode on screen.
G-365	Ability to cancel a print.
	Ability to require the following prior to allowing a user to print a report:
G-366	Date and time (system generated)
G-367	Name of user printing report
G-368	Reason for printing (drop down list)
G-369	User ID (system generated)
	Global System
	DevSecOps
	During the development process it is verified that:
G-370	A code analysis tool is in use that can detect potentially malicious code, such as time functions, unsafe file operations and network connections.
G-371	The application source code and third party libraries do not contain unauthorized phone home or data collection capabilities. Where such functionality exists, obtain the user's permission for it to operate before collecting any data.
G-372	The application does not ask for unnecessary or excessive permissions to privacy related features or sensors, such as contacts, cameras, microphones, or location.
G-373	The application source code and third party libraries do not contain back doors, such as hard-coded or additional undocumented accounts or keys, code obfuscation, undocumented binary blobs, rootkits, or anti-debugging, insecure debugging features, or otherwise out of date, insecure, or hidden functionality that could be used maliciously if discovered.

[redacted]

G-374	ries do not contain time bombs by searching for date and time related functions.
G-375	The application source code and third party libraries do not contain malicious code, such as salami attacks, logic bypasses, or logic bombs.
G-376	The application source code and third party libraries do not contain Easter eggs or any other potentially unwanted functionality.
G-377	The application has a client or server auto-update feature, updates should be obtained over secure channels and digitally signed. The update code must validate the digital signature of the update before installing or executing the update.
G-378	The application employs integrity protections, such as code signing or subresource integrity. The application must not load or execute code from untrusted sources, such as loading includes, modules, plugins, code, or libraries from untrusted sources or the Internet.
	The solution verifies that:
G-379	The application has protection from subdomain takeovers if the application relies upon DNS entries or DNS subdomains, such as expired domain names, out of date DNS pointers or CNAMEs, expired projects at public source code repos, or transient cloud APIs, serverless functions, or storage buckets (autogen-bucket-id.cloud.example.com) or similar. Protections can include ensuring that DNS names used by applications are regularly checked for expiry or change.
G-380	The application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, or environment variables).
G-381	Frameworks protect against mass parameter assignment attacks, or that the application has countermeasures to protect against unsafe parameter assignment, such as marking fields private or similar.
G-382	All input (HTML form fields, REST requests, URL parameters, HTTP headers, cookies, batch files, RSS feeds, etc) is validated using positive validation (allow lists).

G-383	Structured data is strongly typed and validated against a defined schema including allowed characters, length and pattern (e.g. credit card numbers, e-mail addresses, telephone numbers, or validating that two related fields are reasonable, such as checking that suburb and zip/postcode match).
G-384	URL redirects and forwards only allow destinations which appear on an allow list, or show a warning when redirecting to potentially untrusted content.
G-385	All untrusted HTML input from WYSIWYG editors or similar is properly sanitized with an HTML sanitizer library or framework feature.
G-386	Unstructured data is sanitized to enforce safety measures such as allowed characters and length.
G-387	The application sanitizes user input before passing to mail systems to protect against SMTP or IMAP injection.
G-388	The application avoids the use of eval() or other dynamic code execution features. Where there is no alternative, any user input being included must be sanitized or sandboxed before being executed.
G-389	The application protects against template injection attacks by ensuring that any user input being included is sanitized or sandboxed.
G-390	The application protects against SSRF attacks, by validating or sanitizing untrusted data or HTTP file metadata, such as filenames and URL input fields, and uses allow lists of protocols, domains, paths and ports.
G-391	The application sanitizes, disables, or sandboxes user-supplied Scalable Vector Graphics (SVG) scriptable content, especially as they relate to XSS resulting from inline scripts, and foreignObject.
G-392	Application sanitizes, disables, or sandboxes user-supplied scriptable or expression template language content, such as Markdown, CSS or XSL stylesheets, BBCode, or similar.
G-393	Output encoding is relevant for the interpreter and context required. For example, use encoders specifically for HTML values, HTML attributes, JavaScript, URL parameters, HTTP headers, SMTP, and others as the context requires, especially from untrusted inputs (e.g. names with Unicode or apostrophes, such as ねこ or O'Hara).
G-394	Output encoding preserves the user's chosen character set and locale, such that any Unicode character point is valid and safely handled.

G-395	rst, manual - output escaping protects against reflected, stored, and DOM based XSS.
G-396	Data selection or database queries (e.g. SQL, HQL, ORM, NoSQL) use parameterized queries, ORMs, entity frameworks, or are otherwise protected from database injection attacks.
G-397	Where parameterized or safer mechanisms are not present, context-specific output encoding is used to protect against injection attacks, such as the use of SQL escaping to protect against SQL injection.
G-398	The application protects against JSON injection attacks, JSON eval attacks, and JavaScript expression evaluation.
G-399	The application protects against LDAP injection vulnerabilities, or that specific security controls to prevent LDAP injection have been implemented.
G-400	The application protects against OS command injection and that operating system calls use parameterized OS queries or use contextual command line output encoding.
G-401	The application protects against Local File Inclusion (LFI) or Remote File Inclusion (RFI) attacks.
G-402	The application protects against XPath injection or XML injection attacks.
G-403	The application uses memory-safe string, safer memory copy and pointer arithmetic to detect or prevent stack, buffer, or heap overflows.
G-404	Format strings do not take potentially hostile input, and are constant.
G-405	Sign, range, and input validation techniques are used to prevent integer overflows.
G-406	Serialized objects use integrity checks or are encrypted to prevent hostile object creation or data tampering.
G-407	The application correctly restricts XML parsers to only use the most restrictive configuration possible and to ensure that unsafe features such as resolving external entities are disabled to prevent XML eXternal Entity (XXE) attacks
G-408	Deserialization of untrusted data is avoided or is protected in both custom code and third-party libraries (such as JSON, XML and YAML parsers).
G-409	When parsing JSON in browsers or JavaScript-based backends, JSON.parse is used to parse the JSON document. Do not use eval() to parse JSON.

G-410	All components are up to date, preferably using a dependency checker during build or compile time.
G-411	All unneeded features, documentation, sample applications and configurations are removed.
G-412	If application assets, such as JavaScript libraries, CSS or web fonts, are hosted externally on a Content Delivery Network (CDN) or external provider, Subresource Integrity (SRI) is used to validate the integrity of the asset.
G-413	Third party components come from pre-defined, trusted and continually maintained repositories.
G-414	The attack surface is reduced by sandboxing or encapsulating third party libraries to expose only the required behaviour into the application.
G-415	Build and deployment processes are performed securely and repeatedly, such as CI / CD automation, automated configuration management, and automated deployment scripts.
	Security
G-416	Ability to comply with applicable Criminal Justice Information Services Division (CJIS) requirements, described in the most recent version of the Criminal Justice Information Services Security Policy provided by the U.S. Department of Justice.
G-417	Ability to comply with the Health Insurance Portability and Accountability Act (HIPAA), restricting information from view or access when appropriate.
G-418	Ability to encrypt data transmissions.
G-419	The system does NOT include hidden or "backdoor" accounts.
G-420	The system does NOT contain default accounts.
G-421	The information system automatically audits the creation, modification, enabling, disabling, and removal of accounts.
G-422	Users are required to log out when the organization-defined time period of inactivity is reached or in accordance with organization-defined description of when to log out.
G-423	If shared group accounts are permitted, the information system terminates shared/group account credentials when members leave the group.

G-424	The system employs the principle of least privilege, allowing only authorized access for users(and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
	The information system:
G-425	Audits the execution of privileged functions.
G-426	Prevents non-privileged users from executing privileged functions including: disabling implemented security safeguards/countermeasures, circumventing security safeguards/countermeasures, and altering implement security safeguards/countermeasures.
G-427	Limits the number of concurrent sessions to a configurable number of sessions for privileged access and & number of sessions for non-privileged access.
G-428	Automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect occurs.
G-429	Monitors and controls remote access methods.
G-430	Implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
G-431	Routes all remote accesses through the organization-defined number of managed network access control points.
G-432	Protects wireless access to the system using encryption and authentication of users or devices.
G-433	Is capable of auditing successful and unsuccessful logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. (For web applications: The organization determines that the application is capable of auditing all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.)
G-434	Generates audit records containing information that establishes the type of event that occurred, when and where the event occurred, the source of the event, outcome of the event, and the identity of any individuals or subjects associated with the event.

G-435	connection, transaction, or activity duration, and for client-server transactions, the number of bytes received and bytes sent with additional informational messages to diagnose or identify the event and characteristics that describe or identify the object or resource being acted upon.
G-436	Alerts the organization-defined personnel or roles in the event of an audit processing failure.
G-437	Provides an audit reduction and report generation capability that supports on-demand audit review, analysis, reporting requirements, and after-the-fact investigations of security incidents.
G-438	Provides an audit reduction and report generation capability that does not alter the original content or time ordering of audit records.
G-439	Provides the capability to process audit records for events of interest within audit records.
G-440	Uses internal system clocks to generate time stamps for audit records.
G-441	Records time stamps for audit records that meet the organization's defined granularity of time measurement and can be mapped to Coordinated Universal Time(UTC) or Greenwich Mean Time(GMT).
G-442	Compares the internal information system clocks with the organization-defined authoritative time source at least hourly.
G-443	Synchronizes the internal information system clocks to the authoritative time source when the time difference is greater than one(1) hour.
G-444	Protects audit information and tools from unauthorized access, modification, and deletion.
G-445	Allows the organization-defined personnel or roles to select which auditable events are to be audited by specific components of the system.
G-446	Prevents the installation of organization-defined software and firmware components without verification that such components have been digitally signed using a certificate that is recognized and approved by the organization.
G-447	Enforces access restrictions for change and support auditing of the enforcement actions.
G-448	Uniquely identifies and authenticates organizational users(or processes acting on behalf of organizational users).

G-449	ɔrk access to privileged accounts(i.e. administrator and management accounts).
G-450	Implements multifactor authentication for network access to non-privileged accounts.
G-451	Implement multifactor authentication for local access to privileged accounts.
G-452	Replays-resistant authentication mechanisms for network access to privileged accounts.
G-453	Implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets modern authentication protocol requirements.
G-454	Identifies and authenticates organization-defined devices before establishing a local, remote, or network connection.
G-455	Enforces a minimum password complexity of case sensitive, minimum of twelve(12) characters, and at least one upper-case, letter, lower-case letter, number, and special character for password based authentication. (This control may be considered compliant if password policies are compliant with NIST SP 800-63B Memorized Secret(Section 5.1.1) Guidance)
G-456	Stores and transmits only encrypted representations of passwords.
G-457	For PKI-based authentication, validates certifications by verifying a certification path to an accepted trust anchor and checking certificate status information when constructing and verifying the certification path.
G-458	For PKI-based authentication, enforces authorized access to the corresponding private key.
G-459	For PKI-based authentication, maps the authenticated identity to the account of the individual or group.
G-460	For PKI-based authentication, implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.
G-461	Obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
G-462	Implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

G-463	izational users(or processes acting on behalf of non-organizational users)
G-464	Separates user functionality (including user interface services) from information system management functionality.
G-465	Prevents unauthorized and unintended information transfer via shared system resources.
G-466	Describe the information system's ability to protect against or limit the effects of denial of service attacks.
G-467	Protects the availability of resources by allocating resources on the basis of priority, quota, and/or organization-defined safeguards.
G-468	Does the information system monitor and control communications at the system's external boundary and key internal boundaries within the system?
G-469	Implements subnetworks for publicly accessible system components that are physically and/or logically separated from internal organizational networks.
G-470	Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
G-471	Denies network traffic by default and only allow network communications traffic by exception at managed interfaces.
G-472	Prevents split tunneling for remote devices.
G-473	Routes organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers at managed interfaces.
G-474	Fails securely in the event of an operational failure of a boundary protection device.
G-475	Protects confidentiality and integrity of transmitted information.
G-476	Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission, unless otherwise protected by a hardened or alarmed carrier Protective Distribution System (PDS).

[redacted]

G-477	Terminates the network connection associated with a communication session at the end of the session or after no longer than 30 minutes for RAS-based sessions and no longer than 60 minutes for non-interactive user sessions of inactivity.
G-478	Implements FIPS-validated or NSA-approved cryptography.
G-479	Provides additional data origin and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.
G-480	Provides the means to indicate the security status of child zones and enable verification of a chain of trust among parent and child domains(if the child supports secure resolution services), when operating as part of a distributed, hierarchical namespace.
G-481	Requests data origin authentication and perform data integrity verification on the name/address resolution responses the system receives from authoritative sources.
G-482	Protects the authenticity of communications sessions.
G-483	Protects the confidentiality and integrity of customer data at rest.
G-484	Employs cryptographic mechanisms to prevent unauthorized disclosure and modification of customer data.
G-485	Verifies the correct operation of security functions and performs this verification at least monthly and upon system startup and/or restart.
G-486	Notifies system administrators and security personnel of failed security verification tests and discovered anomalies in security functions.
G-487	When anomalies are discovered during security function verification, shuts the information system down, restarts the information system, and/or performs other alternative action(s).
G-488	Performs an integrity check of organization-defined software, firmware, and information at least monthly and upon startup and/or security-relevant events.
G-489	Checks the validity of organization-defined information inputs.
G-490	Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.
G-491	Reveals error messages only to authorized organization personnel or roles.

G-492	ıards to protect its memory from unauthorized code execution.
G-493	The information systems that collectively provide name/address resolution service for the organization are fault-tolerant.
G-494	Internal/external role separation is implemented for the information systems that collectively provide name/address resolution service for the organization.
	Ability to provide security at the following levels:
G-495	Application
G-496	Database
G-497	Field
G-498	Record
G-499	Screen/Transaction
G-500	System
	Ability to provide security controls by:
G-501	Agency
G-502	Function
G-503	User ID
G-504	Terminal ID
	Ability to view, add, maintain, modify and delete user profiles based on:
G-505	User ID
G-506	User name
G-507	Title/Role (e.g., Chief)
G-508	Rank
G-509	Location
G-510	Security group
G-511	Agency
G-512	Ability to create temporary security profiles.
G-513	Ability to combine, alter and model security roles for specific groups.
G-514	Ability to tie security to personnel module for automated security provisioning driven by work assignment.
G-515	Ability to lock out a user who is deemed a security risk while that user is on-line (e.g., logged into the system).
G-516	Ability to define what information will display on screen for a given security level.
G-517	Ability to prevent users from creating ad hoc reports on fields to which they do not have proper security permissions.
G-518	Ability to integrate with Microsoft Active Directory network management functionality (i.e. LDAP)
G-519	Ability to link security profiles to Active Directory user groups.

G-520	ıe event Active Directory becomes unavailable.
G-521	Ability to allow tiered access to information based on login ID and other authentication practices.
G-522	Ability to support alternate authentication technologies (i.e., ID card, security token, biometrics, etc.).
G-523	Ability to assign security access by physical device (e.g., PCs, terminals, etc.).
G-524	Ability to mask or encrypt a data element as confidential information for security purposes.
G-525	Ability to flag a data element as confidential information for security purposes.
	System Design Attributes
G-526	The proposed system supports and is compatible with standard anti-virus software without conflict or performance degradation.
G-527	The proposed system supports [redacted].
G-528	The proposed system supports [redacted].
G-529	The proposed system supports [redacted].
G-530	The proposed database operating environment uses standard, industry-accepted database management software.
G-531	As a multi-node CAD system, the system will interface with multiple email gateways for notifications.
G-532	The system availability is 99.999% uptime.
G-533	The system has the capability to allow users to continue to create, view, and modify event data if the workstation connection to the CAD server is lost (offline) for any reason.
G-534	Static table data can be migrated from the current CAD to the Proposer's CAD system (historic data migration)

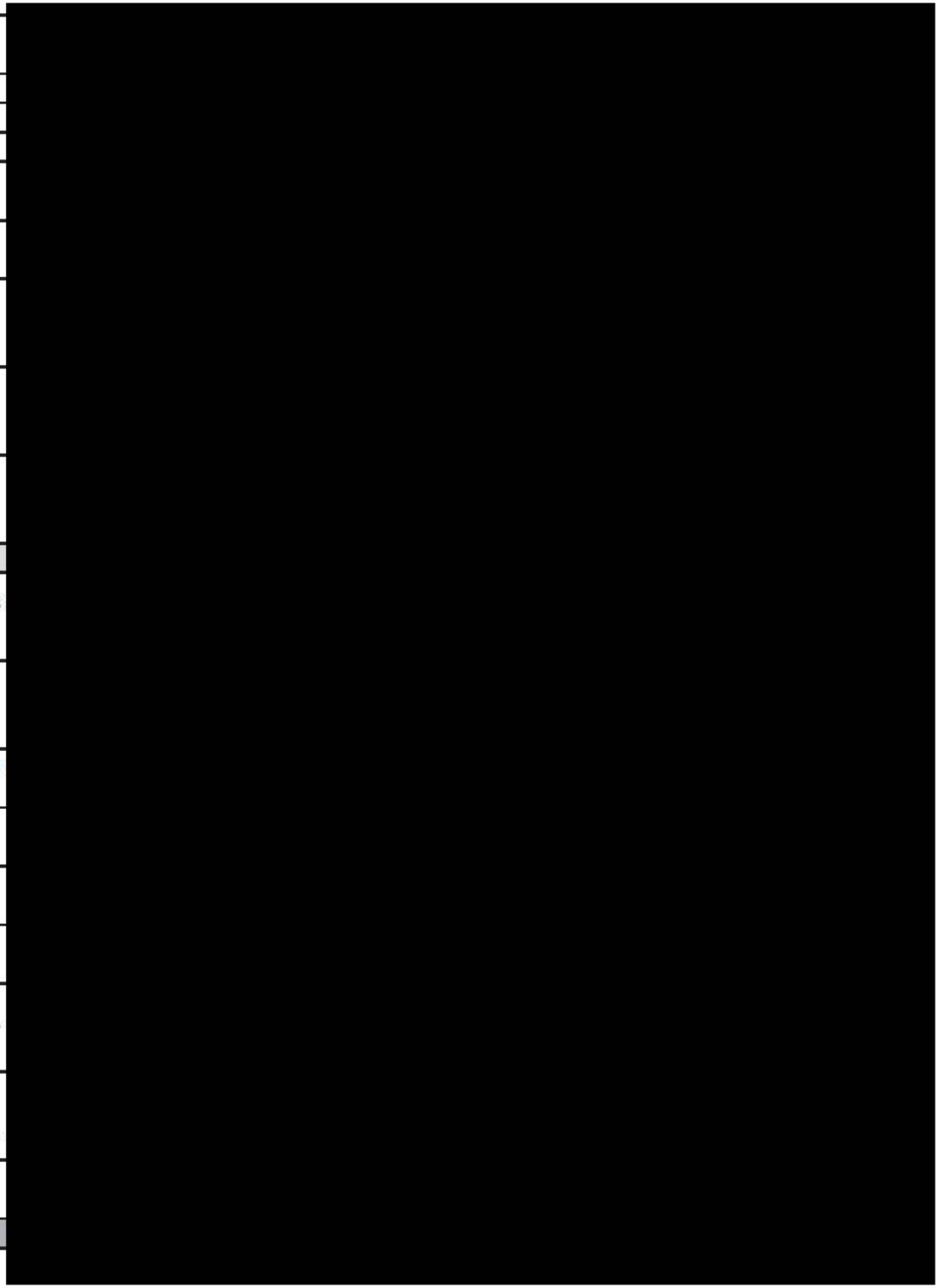
[redacted]

G-535	s CAD application and module updates (new versions) are developed and certified to work with installed/current operating system updates/versions.
G-536	The system network protocol is Transmission Control Protocol (TCP)/Internet Protocol (IP) compliant.
	System Backups
G-537	The system provides a means to perform regular (e.g., daily, weekly) backups, have a robust redundancy plan for the backups and support on-demand access, deployment and management of the backup data.
G-538	Performing the backup procedure does not degrade system performance.
G-539	The system has the capability to roll-back to the date of the last backup.
G-540	The system has the capability of point-in-time recovery.
G-541	When a failure occurs, the system creates an error log that provides sufficient documentation for the agency to establish the cause of the failure.
G-542	Once a failed server has been restored to operational capability, it automatically reconnects with the CAD network without user intervention.
G-543	Once a failed server has been restored to operational capability, the system will send notifications to designated devices and personnel.
G-544	In the event that any disk or other synchronized storage device is out of sync, the system automatically synchronizes the deficient storage device without user intervention and without degrading the system performance.
	Disaster Recovery (DR)
G-545	The system supports a failover process for all [redacted] and/or workstations.
G-546	The system supports regular DR failover tests, switching operations from the primary to the DR site.
G-547	The Disaster Recovery system can be set up at a location physically remote from the primary public safety answering point (PSAP).
G-548	The Disaster Recovery system can be operated and maintained from a remote location.
G-549	The Disaster Recovery system functions as a hot standby Disaster Recovery site.
G-550	All operations of the primary site can be performed at the Disaster Recovery site.

G-551	ate as a fully-functional standalone site.
G-552	Switching operations from the primary facility to the Disaster Recovery facility can be performed by an authorized user.
G-553	Switching operations from the Disaster Recovery facility to the primary facility can be performed by an authorized user.
G-554	The system at the Disaster Recovery facility can be switched to run as the primary CAD system provider, with the workstations at the failover facility and primary facility operating as live CAD workstations.
G-555	The workstations at the Disaster Recovery facility can be configured to operate on the primary system as additional workstations.
G-556	The Disaster Recovery failover does not require system shutdown and restart.
G-557	Events active prior to the Disaster Recovery failover are available as active events after the failover activation with no loss of data.
G-558	The system supports the management of servers and/or workstations using imaging software.
G-559	Redundant servers can be updated and maintained without degradation to primary system operation.
G-560	If placed off-line, backup servers come on-line automatically and synchronize without degradation to primary system operation.
G-561	The switch to the backup servers is seamless and transparent to users and performance is not degraded.
G-562	The system delivers a system message to selected workstations (e.g., supervisor, administrator) that primary operations have been switched to the backup system.
G-563	The system operates on backup servers without degradation to services or response time.
G-564	The system can be switched between the primary and backup servers on a regular basis and operate on either system indefinitely.
	Network Printers and Printing:
G-565	CAD workstations will be assigned a default printer.
G-566	CAD system printers will be networked and available to all workstations on the network.
G-567	When generating a print job, a user does not have to select a printer; the default printer will be automatically selected.

[redacted]

G-568	lotter to print maps, color printer when printing reports).
G-569	Event data can be printed at any time during an event.
G-570	Closed events can be printed.
G-571	Event data may be printed to any CAD-configured printer.
G-572	Print of event data may be restricted to printing at a designated, secure printer at the discretion of the agency.
G-573	Print of event data may be restricted based on user, role and workstation security.
G-574	The system is capable of generating an event print option that does not contain non-public information (e.g., name of caller, caller telephone number, social security number).
G-575	When an item is submitted for printing, a confirmation message is returned to the workstation initiating the print request when completed.
G-576	Print transactions (including print screen) are recorded in the transaction/audit log and include the user identification (ID) and workstation ID initiating the print function.
	Remote Access Workstations
G-577	The system supports access to the CAD system from workstations that are not directly connected to the CAD network.
G-578	The system supports a time-out feature for remote workstations that are inactive for an agency-defined time period.
G-579	The system allows access from a remote workstation through the use of web-based protocols.
G-580	The system is capable of configuring remote status monitor-only workstations.
G-581	Remote status monitor-only workstations may be excluded from the time-out feature.
G-582	System access from a remote workstation does not require a dedicated circuit, unless required to comply with CJIS.
G-583	Remote access is restricted to those authorized through the system security function and secured passwords (e.g., dual-factor authentication).
G-584	System access from a remote workstation will support Advanced Encryption Standard (AES) without degrading system throughput.
G-585	Remote workstation access to the CAD system complies with CJIS, State, and Agency security requirements.
	Logons and Logoffs



G-586	ord for the entire application environment.
G-587	Ability for a single user to be logged onto multiple workstations at the same time (e.g., logged into mobile computer in a vehicle and logged onto a station computer at the same time).
G-588	Ability to require that users logon to the system prior to operating any system functions.
G-589	Ability to track user logon/logoff times and locations for time reporting purposes.
G-590	Ability to support two-factor logon.
G-591	Ability to support third-party identification devices for logons.
G-592	Ability to restrict a logoff if primarily responsible for defined incidents and units.
G-593	Ability to automatically log and report a sign-in on top of someone who is already logged in.
G-594	Ability to automatically logoff a user after an agency-defined predetermined period of inactivity, based on user type and location.
G-595	Ability to Administratively disable automatic logoff for secured workstations.
G-596	Ability to provide system-generated warning message prior to disabling device or user, and extend or reset automatic sign-off timer.
G-597	Ability to save user's data or session prior to automatically logging off the user.
G-598	Ability to display date and time of last session upon user logon.
	Ability to provide system generated message to system administrator or supervisor when an agency-defined number of unsuccessful sign-on attempts have occurred. The message must include, at a minimum:
G-599	Date and time
G-600	Number of attempts
G-601	User ID
G-602	Workstation ID
G-603	Ability to distribute system generated message to system administrator or supervisor via email.
G-604	Ability to “lock out” a user and close applications after agency-defined number of attempted logons.
G-605	Ability to disable "lock out" feature.
G-606	Ability to provide varying security levels (application to be accessed, menu-option level) defined to the user level.

G-607	Ability to provide a secure lock-out with quick re-authentication to restrict access to systems from an unattended workstation.
G-608	Ability to prevent any external agency from having access to update, alter or delete data.
G-609	Ability to highlight, flag or otherwise alert users with the appropriate security access that a record or data element is confidential.
G-610	Ability to display message of "record not on file" or "record contents locked for security reasons - contact <name> for more information" to users without appropriate security access when searching for a confidential item.
G-611	Ability to globally restrict access to operating system.
	User IDs and Passwords
G-612	Ability to maintain a history of de-activated user IDs.
G-613	Ability to have multiple administrative accounts.
G-614	Ability for vendor support to be provided via unique support accounts.
G-615	Ability to require the user to change individual password at logon after a user-defined time interval.
G-616	Ability for the systems administrator to reset password.
G-617	Ability for shift supervisors to reset passwords.
G-618	Ability for all passwords to be changed at agency-defined intervals, by user, with the ability to set a global maximum time.
G-619	Ability to disable password expiration feature.
G-620	Ability to require the user to enter a new password twice (e.g., to verify password).
G-621	Ability to produce auto-notification of impending password expiration.
G-622	Ability to enforce strong passwords per CJIS requirements.
G-623	Ability for user ID to be non-case-sensitive.
G-624	Ability for individual system users to change their own passwords.
G-625	Ability for system administrator to add and delete users.
G-626	Ability for system administrator to delete password when deleting a user.
G-627	Ability to prevent reuse of previous agency-defined number of passwords.
G-628	Ability for system administrator to disable an account.

G-629	t passwords when stored and sent (i.e., no clear text passwords).
G-630	Ability for agency to define which user-groups can reset passwords (or create a security group that can reset passwords).
G-631	Ability for agency to define password and user ID creation criteria.
	Audit Trails
G-632	Ability to create a security group defining who has audit trail access permissions.
	Ability to maintain an audit trail at the following levels:
G-633	Individual
G-634	Record
G-635	Module
G-636	Application
	Ability to log all actions including, but not limited to :
G-637	Changes
G-638	Updates
G-639	Errors
G-640	Security violations
G-641	Attempted breaches
G-642	File maintenance transactions (e.g., create, read, add, update, delete transactions)
G-643	Inquiries to all internal and external systems
G-644	Transaction entries
G-645	Any report sent to a printer
G-646	Override
G-647	Successful sign-on
G-648	Unsuccessful sign-on attempts
G-649	Unauthorized attempts to access data
	Ability to store audit trail data including, but not limited to:
G-650	User ID
G-651	User name
G-652	Terminal ID
G-653	Printer ID
G-654	Security level
G-655	Date and time stamp
G-656	Transaction type
G-657	Input, edit, deletion or inquiry
G-658	Before and after values of modified data
G-659	Type of data accessed during an inquiry
G-660	Reason any information was deleted
G-661	Reason any information was changed or updated

G-663	Ability to review all computer activity performed by a specified user during a period of time.
G-664	Ability to log all vendor access to system (e.g., record a description of all vendor activity).
G-665	Ability to use the master source to synchronize time stamps for all application components.
G-666	Ability to maintain historical data based on an agency-defined length of time.
G-667	Ability to maintain file history so that field value changes can be viewed both before and after change occurred.
G-668	Ability to view all audit records for all databases.
G-669	Ability to view all audit records for all fields.
G-670	Ability to set audit log purge criteria.
G-671	Ability to perform purge based on criteria.
G-672	Ability to date, timestamp, view and audit all inquiries.
G-673	Ability of the system to assign a unique identifier to each record (i.e., log ID).
G-674	Ability to comply with CJIS requirements of NCIC and III transactions.
G-675	Ability for all audit and logging functionality to be configurable.
G-676	Ability to view audit trails online.
	Ability to display a record and see (e.g., via a function key):
G-677	Who made last change to record
G-678	Time and date stamp of last change to record
G-679	Modifications made to record (before and after values)
G-680	Ability to extract reports from the audit trail.
G-681	Ability to search for and by any data in the audit trail.
G-682	Ability to secure audit log from user tampering.
G-683	Ability to archive audit trails based on transaction type and/or date.
G-684	Ability to manually archive information based upon user-specified parameters (time, file size, etc.)
G-685	Ability to automatically archive information based upon user-specified parameters (time, file size, etc.)
G-686	Ability to easily query archived and current information by any combination of criteria.
G-687	Ability to configure the size the audit log must be before it is archived.
G-688	Ability to maintain file history so that field value changes can be viewed both before and after change occurred.

[redacted]

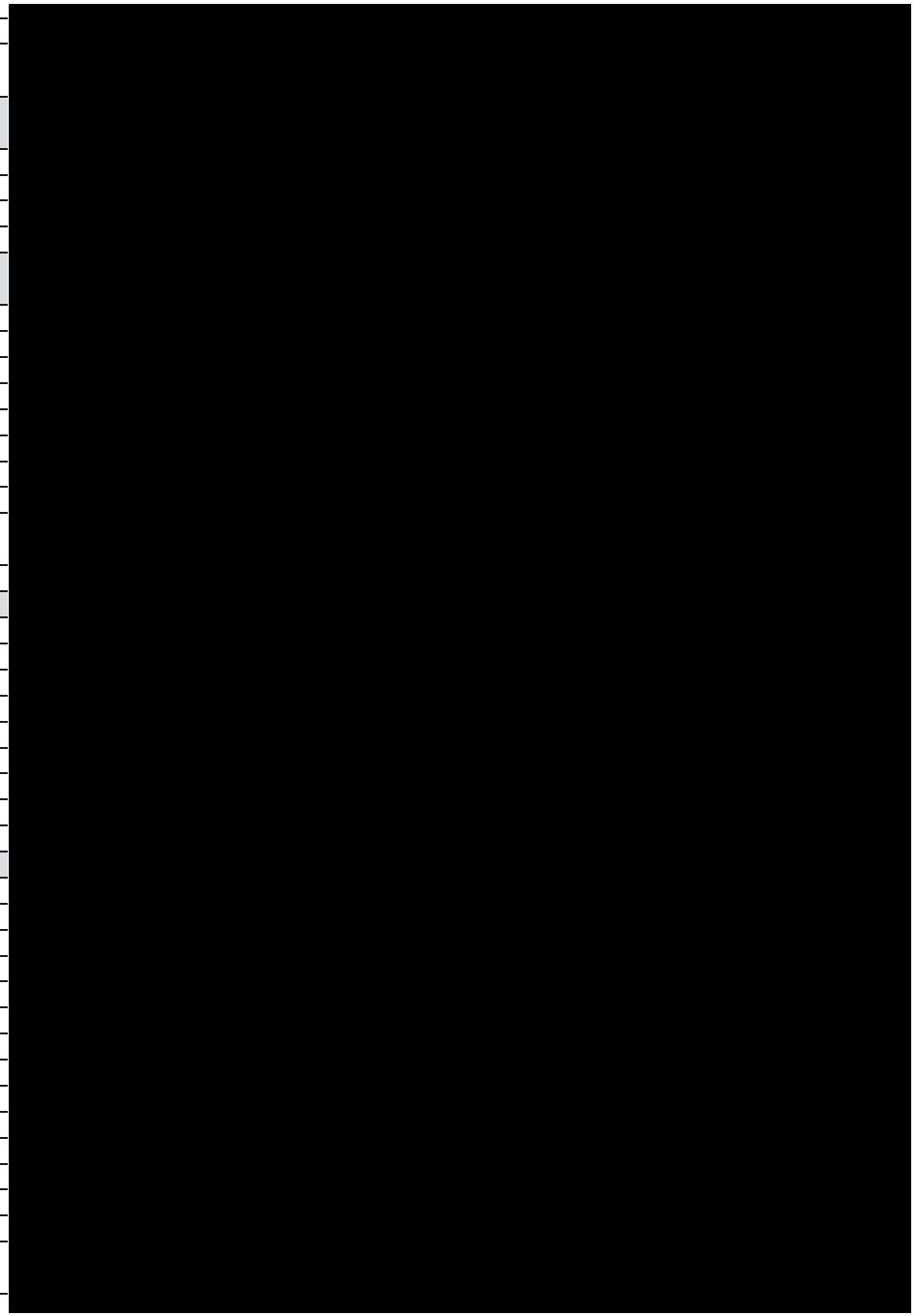
Request for Proposals
Computer Aided Dispatch - Functional Specifications

Item #	Specification	Vendor Response	Vendor Comments
	Global CAD Features		
	Ability to handle multiple types of public safety agencies or disciplines:		
C-1	Law Enforcement		
C-2	Fire		
C-3	EMS		
C-4	Other public service units		
	Ability for authorized user to configure any CAD workstation to handle:		
C-5	Either call taking or dispatching functions		
C-6	Both call taking and dispatching functions		
C-7	CAD Adminstrator functions		
C-8	Ability to configure any CAD workstation to accommodate a color-blind user (e.g., using icons, symbols, or text instead of colors).		
C-9	Ability to dispatch any configured agency/discipline units from the same CAD application windows without significant changes.		
C-10	Ability to comply with all standards associated with NFPA 1221's installation, maintenance and usage of emergency services communications systems.		
C-11	Ability to comply with published NENA NG9-1-1 standards.		

C-12	Ability to comply with all NIEM standards.	[redacted]
C-13	Ability to support both closest, most appropriate unit (based on AVL) dispatching and beat-based or "run card" dispatching.	
C-14	Ability for each agency using the CAD system (i.e., Police and Fire) to enable and disable agency-specific resource recommendations.	
	Ability to log all CAD transactions, including, but not limited to:	
C-15	Additional units added to call	
C-16	Any change in unit location	
C-17	Any status change	
C-18	At patient	
C-19	At staging location	
C-20	Call assigned to unit's call queue	
C-21	Call dispatched	
C-22	Call priority change	
C-23	Call received	
C-24	Call re-routed	
C-25	Call reviewed	
C-26	Call transferred from E9-1-1 to CAD system	
C-27	Cleared	
C-28	Corrections, edits and deletions	
C-29	Other agency notifications	
C-30	Data Entry	
C-31	En route	
C-32	Error messages	
C-33	First due status	
C-34	Geoverification	
C-35	In area	
C-36	Incident appended or merged to another incident	
C-37	Incident closed	
C-38	Incident linked or associated to another incident	
C-39	Incident reopened	
C-40	Incident supplemented	
C-41	Incident updated	
C-42	Last-known unit location	
C-43	Location change	
C-44	Narrative changes	
C-45	On-scene	
C-46	Pre-empt (swap unit between incidents)	
C-47	Subsequent dispatcher reviews call	
C-48	Transferred to dispatcher (call entered)	
C-49	Unit receives call on mobile device and/or Mobile Data Terminal	
C-50	Unit reviews call (if different from unit receives call)	
C-51	Unit name or number	

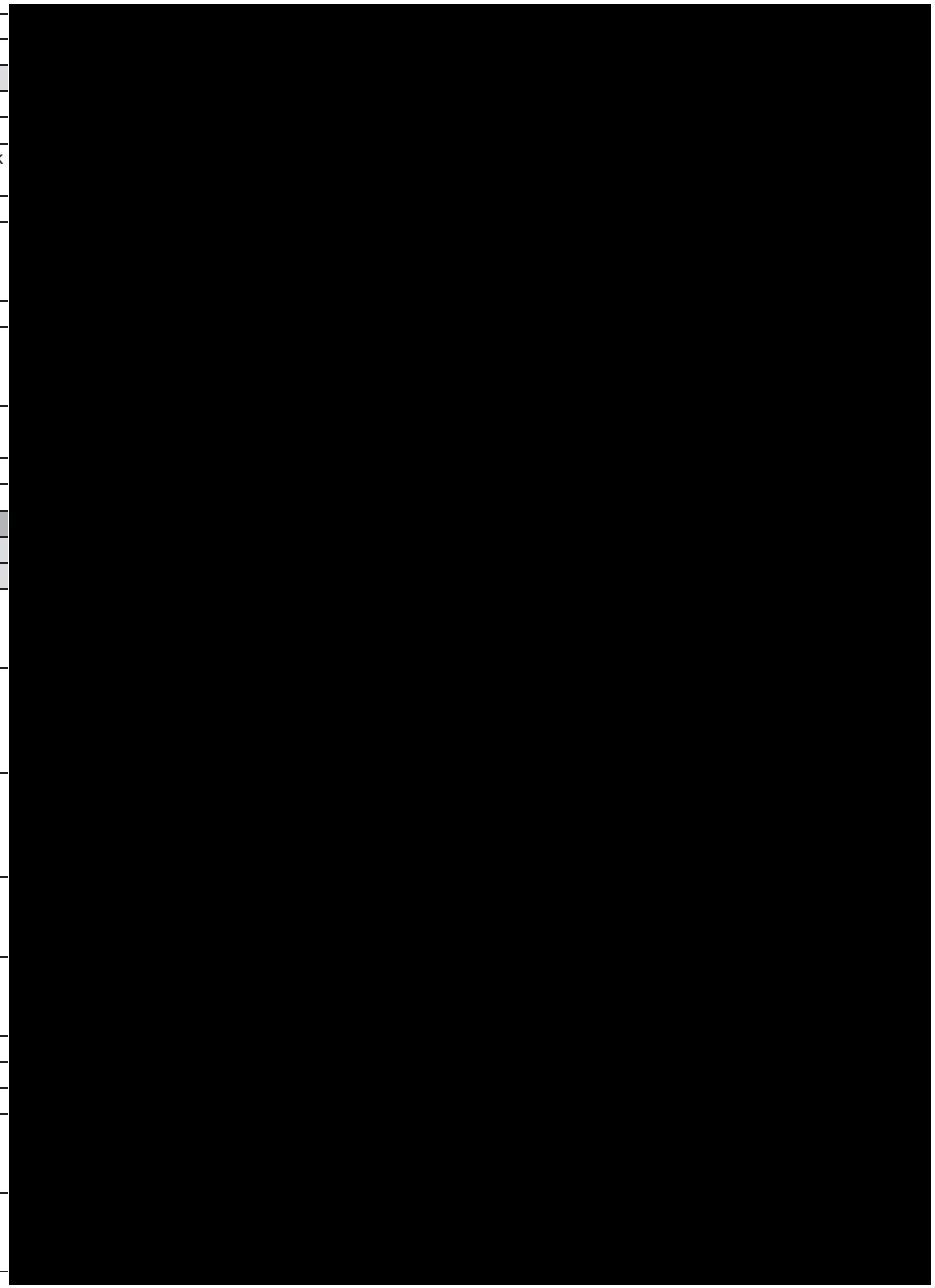
C-52	Vehicle number
C-53	Ability to capture all Mobile logon/logoff data.
C-54	Ability to integrate CAD with existing email system on desktop.
C-55	Ability for CAD system to automatically send email notifications based upon user-defined criteria.
	Ability to access a browser-based CAD for:
C-56	Read-only purposes
C-57	Enter calls
C-58	Edit calls
C-59	Request Case number
C-60	Close calls
C-61	Ability to allow two users to operate on the same CAD screen simultaneously (e.g., to allow a trainer and trainee to work on the same call).
C-62	When multiple users are working on the same call, all user actions are logged but last-entered value retained.
	CAD Dashboard
C-63	Ability to have an agency-configurable external-to CAD dashboard that summarizes ongoing CAD activities.
C-64	Ability to configure CAD dashboard features by agency.
C-65	Ability to configure CAD dashboard features by login.
C-66	Access to CAD dashboard can be publicly-accessible.
	Ability to provide alerts to CAD dashboard when:
C-67	Staffing levels fall below minimum threshold
C-68	Activity exceeds an identified threshold
C-69	Alarm levels exceeds an identified threshold
C-70	Any agency-defind trigger threshold is met
C-71	Any agency-defind trigger threshold is met
	Application User Interface
C-72	Ability for agency to determine which window configuration options are configurable at the user level.
	Ability for users to customize window views, including, but not limited to:
C-73	Font size
C-74	Font colors
C-75	Font type
C-76	Window background color
C-77	Window sizes
C-78	Window locations
C-79	What fields are displayed
C-80	Order in which fields are displayed
C-81	Ability to save window configurations based on user IDs (e.g., not workstation-specific).
C-82	Ability for all configured colors to match throughout the application (e.g., unit status color is the same in active queue as displayed in map)
C-83	Ability to maintain window configuration settings during upgrades.
C-84	Ability to allow a return to system default settings within at least 2 key strokes or a single command.

C-85	Ability to prevent a user from closing critical windows (e.g. unit status window).
C-86	Ability for all minimized windows to re-open if a new user logs onto the workstation.
	Ability to provide system-wide consistent, common screen formats that display the following:
C-87	Current system date and time
C-88	Screen name/description
C-89	System name/description
C-90	User ID
	Ability to perform any system command and function using any of the following methods:
C-91	Command lines
C-92	Toolbar
C-93	Keyboard
C-94	Right mouse click
C-95	Short cut commands
C-96	User defined function keys (hot keys)
C-97	Ability to define function key assignments differently, by agency.
C-98	Ability to execute any CAD function using the keyboard.
C-99	Ability to execute any CAD function without the use of delimiters from the command line.
C-100	Ability to execute any CAD function using the mouse.
	Ability for system to include the following:
C-101	Automatic defaults
C-102	Field prompts (e.g., fields that need to be filled in based on previous responses)
C-103	Online, interactive help
C-104	Ability to display system messages on a pop-up window.
C-105	Ability to display system messages without affecting work in progress.
C-106	Ability to minimize or maximize any activity screen.
C-107	Ability to have multiple windows open at the same time.
C-108	Ability to tile or cascade multiple windows on screen.
C-109	Ability to hyperlink to related information.
	Ability to display the following information on the screen during normal operations:
C-110	Group
C-111	Message alert
C-112	Radio talk group (on dispatcher screen)
C-113	Time
C-114	Date
C-115	Ability to set task triggers or reminders from within the CAD application.
C-116	Ability to provide multiple command lines.
C-117	Ability to create or display a new command line with a single keystroke.
C-118	Ability to link a command line to a distinct incident.
C-119	Ability to enter commands in any order on the command line.
C-120	Ability to enter more than one command on a single command line.
C-121	Ability to provide automatic word wrap when entering free-style text.
C-122	Ability to use arrow and tab keys to scroll around within a window.
C-123	Ability to display one or more status windows at the same time.
C-124	Ability to manually create a time stamp (e.g., writing in the narrative, press CTRL + D to enter date/time)



	Time Stamps
C-125	Ability to date and time stamp all CAD transactions.
	Ability to capture and store time stamps, including but not limited to the following:
C-126	Call pickup in 911
C-127	Call for service created (call entered into system)
C-128	Call dispatched
C-129	Call transferred to another agency
C-130	En route
C-131	Staging
C-132	In area
C-133	Location change
C-134	On scene
C-135	At site of incident (e.g., 6th floor of high rise)
C-136	At patient
C-137	En route hospital
C-138	At hospital
C-139	Call cleared
C-140	Incident level upgrade
C-141	Premise information viewed
C-142	Any unit status change
C-143	Ability to log and display all CAD times to 1/10 of a second.
C-144	Ability to manually override a time stamp (e.g., if a unit forgets to hit "on-scene" and dispatcher needs to "back time" the time stamp).
C-145	Ability to capture a time stamp for the overridden time stamp (e.g., the time the time stamp was overridden).
C-146	Ability for all overridden date and time stamps to be clearly recorded and displayed as a manually entered override time.
	Timers
C-147	Ability to provide incident timers and alerts based upon agency-defined parameters (e.g., type of incident, unit arrival time, priority status) and times.
C-148	Ability to manually set incident timers and alerts.
C-149	Ability to display call timers on CAD screens.
	Ability to notify dispatchers and supervisors of the following upon expiration of a call timer:
C-150	CAD incidents not cleared
C-151	CAD incidents received that have not been opened
C-152	Open incidents that have not been viewed after a user-defined or agency-defined default length of time
C-153	No response from field personnel after an agency-defined length of time
	Ability to alert operator to the expiration of the timer via:
C-154	Audible alert
C-155	Visual alert
C-156	Ability to record acknowledgement of timer alert.
	Ability to provide the operator of the following options when a status timer expires:
C-157	Modify to new time value
C-158	Reset to default value
	Flags and Notifications
	Ability to clearly display the presence of:
C-159	Hazardous information

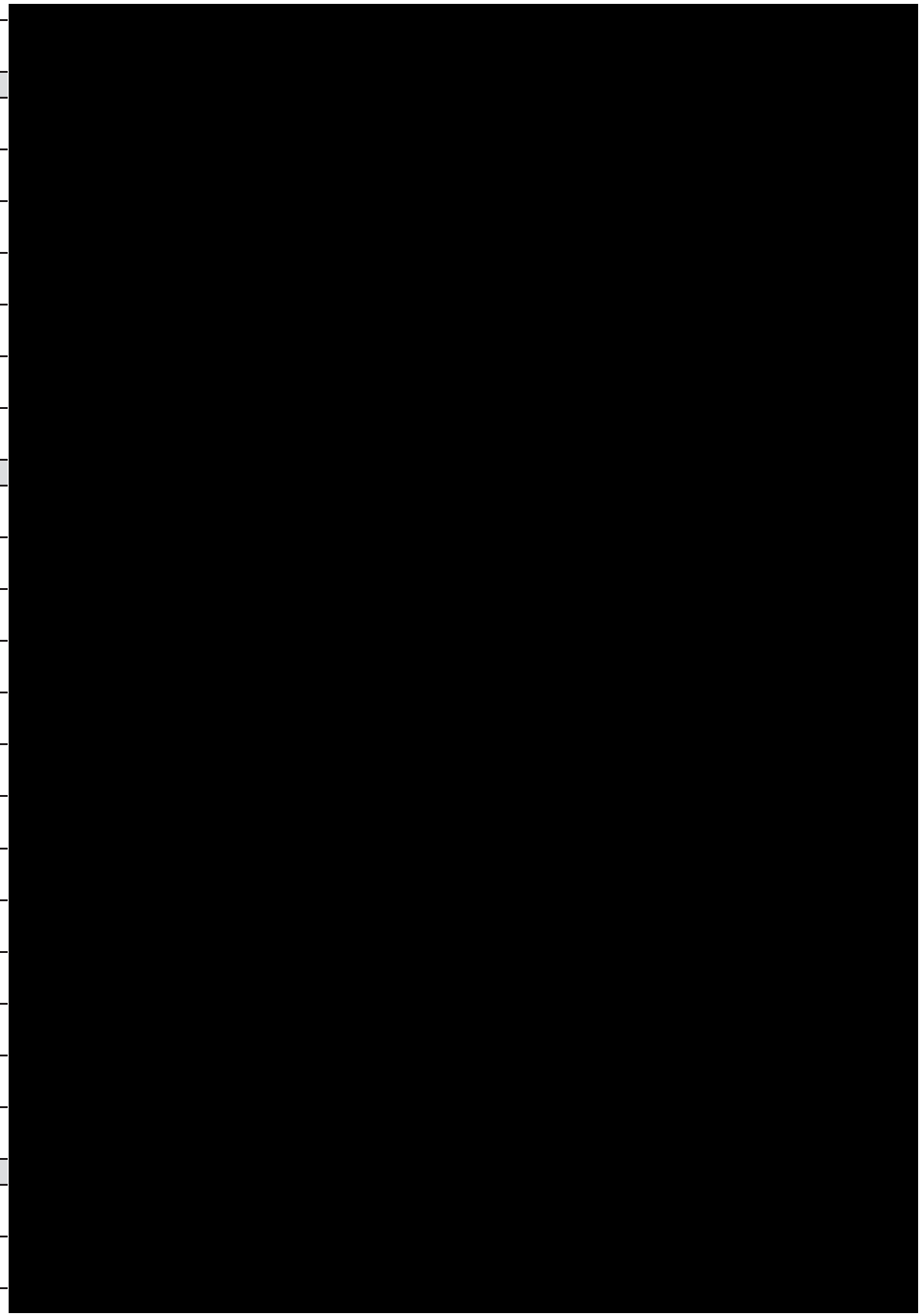
C-160	Premise history
C-161	Pre-Plans
	Ability for notifications to include:
C-162	Audible alert
C-163	Visual flags
C-164	Ability for a user to quickly access information related to a call flag or notification (e.g., click on the flag to pull up the related information).
C-165	Ability to flag multiple addresses associated with a call for service.
C-166	Ability to display information associated with a call flag in such a way that it is easily accessible on the screen but does not interfere with other incident information (e.g., display the related information in a separate tab or window).
C-167	Ability to append call flag text to an incident.
C-168	Ability to filter flags displayed by agency (e.g., have Fire Department information, such as pre-plans, available to Law Enforcement, but allow the Law Enforcement to filter whether or not the flags are displayed).
C-169	Ability to indicate the number of past incidents at a location for a user-defined period of time.
C-170	Ability to add a temporary flag, comment or note to a location.
C-171	Ability to include flagged information with dispatches sent to responding units.
	Call Taking
	Call Receipt
	Ability to receive call data from:
C-172	E9-1-1 phone system
C-173	Other City phone system (e.g., 3-1-1)
C-174	Non-emergency 10 digit phone numbers
C-175	Private alarm companies
C-176	CAD-to-CAD Interface
C-177	Web-based interface/application
C-178	Mobile interface/application (Laptops)
C-179	Handheld interface/application (Phones, tablets)
C-180	Ability to support Phase I wireless location validation from cellular callers.
C-181	Ability to support Phase II wireless location validation from cellular callers.



C-182	Ability to support Next-Gen 9-1-1 location validation from callers.	[redacted]
C-183	Ability to automatically create a call for service when a 911 call comes in through the phone system (e.g., create a call and open a call entry mask).	
C-184	Ability for agency to define a code table for outcomes of incoming 911 calls (e.g., non-dispatched call, abandoned call, hang-up call, etc.).	
	Call Data Entry	
C-185	Ability for users to use either preformatted screens or command lines for incident entry.	
	Ability to capture all incoming call information from the E9-1-1 system, including, but not limited to:	
C-186	Caller name	
C-187	Caller telephone number	
C-188	Caller address/location calling from	
C-189	Incident location	
C-190	Alternate telephone number	
C-191	Cellular phone service provider	
C-192	Phase I or Phase II indication	
C-193	X/Y coordinates	
C-194	TTY conversation	
C-195	Any other information captured by the E9-1-1 system	
	Ability for narrative fields to have the following attributes:	
C-196	Unlimited number of comment lines	
C-197	Word wrap	
C-198	Spell check	
C-199	Ability to document multiple callers/witnesses/suspects for a single incident.	

C-200	Ability to print ANI/ALI import data.	[redacted]
C-201	Ability to capture and save separate file of ANI/ALI import data.	
C-202	Ability to enter standard vehicle information in defined fields and record the entered information as part of the incident record.	
C-203	Ability to enter suspect information in defined fields and record the entered information as part of the incident record.	
C-204	Ability to generate another incident from a previous incident.	
C-205	Ability to generate an incident from a previous incident across agencies (e.g., Police to Fire and vice versa)	
	Location Capture	
C-206	Ability to receive geographic coordinates from a cellular telephone carrier.	
C-207	Ability to automatically populate the location field with ALI information if the new incident is occurring at the ALI reported location.	
C-208	Ability to capture incident location separately from caller location.	
	Ability to type in locations in the following formats:	
C-209	Commonplace name	
C-210	Intersection	
C-211	Named location (e.g., on-ramp on an interstate)	
C-212	Street address	
C-213	Ability to type in either street first when entering intersections.	
C-214	Ability to save intersections as identical address point regardless of order of streets entered (e.g., 1st/Main same as Main/1st)	
C-215	Ability to enter addresses on one line.	
	Ability for system to automatically parse address data into address data fields including:	
C-216	Street number	
C-217	Street name	
C-218	Street prefix	
C-219	Street suffix (NW, SW, NE, SE)	
C-220	Street type (Av, Ln, Rd, "None")	
C-221	Location common name	
C-222	Unit/Building number	
C-223	Apartment	
C-224	City	
C-225	County	
C-226	State	
C-227	Zip	
C-228	Road classification	
C-229	Address extensions (1/2, rear, drive, etc.)	
C-230	Keymap Data (similar to a bookmap, e.g., location based on page number/identifier)	
C-231	Any other common identifiers in regard to addresses	
	Location Verification	
C-232	Ability to verify locations for any address entered into the system.	
C-233	Ability to use the ALI reported location address for address verification.	

C-234	Ability to use the coordinate-based geofile to determine if there are premise or hazard records within the user-defined radius of a new call.
	Ability to verify each incident address entered as part of a CAD incident, including:
C-235	Address range
C-236	Building name
C-237	Business name
C-238	Premise name
C-239	Centerline
C-240	Intersections
C-241	Address
	Ability to display closest address matches based on:
C-242	Block ranges
C-243	Building name
C-244	Business name
C-245	Premise name
C-246	Common place names
C-247	Intersections
C-248	Phonetic spelling
C-249	Previous street name
C-250	Soundex
C-251	Street name
C-252	Ability to display an unlimited number of common place names during the address verification process.
C-253	Ability to limit the number of common place names during the address verification process (e.g., maximum of 25 to prevent system overload).
C-254	Ability to accept as correct an address or location that matches a unique location record in the geofile.
	Ability to enter a valid street name and be presented with:
C-255	Aliases
C-256	Associated address ranges



C-257	List of cross streets	
C-258	Ability to translate call location to appropriate public safety geographical boundary (e.g. district, beat, sector, etc.).	
C-259	Ability to translate alias names to actual street names or addresses.	
C-260	Ability to list address choices by alphabetical and/or numerical sequential order (e.g., 1,2,3 as opposed to 1, 11, 2, 20, 3).	
C-261	Ability to notify dispatcher through a visual and/or audible flag if multiple street addresses/street names/intersections are found in geofile.	
C-262	Ability to offer a list of address options if multiple similar ('soundex', spelling, number/numeric) addresses/intersections/street names are found in geofile.	
C-263	Ability to conduct multiple searches so that, if there is no address match, the system will continue to search for possible address matches and present user with a list of possible matches.	
C-264	Ability to display, on a map the incident location in relation to other active incidents on the map during the incident entry process.	
C-265	Ability to enter a reason for overridden location.	
C-266	Ability to log all locations that fail geofile validation.	
C-267	Ability to indicate in failed validation log if discrepancy was due to ALI discrepancy or a geofile discrepancy.	
C-268	Ability to manually override and correct address/location presented in CAD incident without correction affecting address/location stored in geofile.	
	Ability for notification of correction to be automatically generated and sent to geofile administrator whenever a user manually overrides and corrects an address/location.	
C-269	Email	
C-270	Message	
C-271	Ad hoc or pre-built printable export	
	Ability for the notification of correction to capture the following:	
C-272	Address/location information as presented (ANI/ALI information)	
C-273	Address/location data as corrected by the user	
C-274	Error type	
C-275	Date/time of report	
C-276	User ID	
C-277	Ability to accept and validate "out of jurisdiction" addresses.	
C-278	Ability to flag "out of jurisdiction" addresses.	
	Call Classification and Prioritization	
C-279	Ability to create and maintain call screening menus or prompts that can be used to aid the call-taker in determining the appropriate incident type code.	
C-280	Ability to provide an option to generate automatic notifications to appropriate personnel upon entry of agency-defined call types. [If this functionality can be provided, describe how the message can be sent to the appropriate personnel in the "comments" section]	
C-281	Ability to display a drop-down list containing incident types.	

C-282	Ability for system to automatically enter the appropriate agency-defined priority for each new incident based on call type.
C-283	Ability to override default incident priority.
C-284	Ability to allow the authorized user to manually upgrade or downgrade the system-assigned priority.
C-285	Ability for the system to recognize an escalating alarm level as a single incident and clearly identify when the alarm level was upgraded.
C-286	Ability for dispatcher to change call type without impacting active call data.
C-287	Ability to reclassify a call based upon additional information.
	Incident Initiation
C-288	Ability to initiate an incident from the input of location/address and incident type.
C-289	Ability to input all call and narrative information on one screen.
C-290	Ability to display a blank form for entering new incidents with a single keystroke, mouse click or function key upon initiation of a CAD incident.
C-291	Ability to copy/duplicate an existing incident to create a new incident at the same location.
C-292	Ability to open and view multiple incident entry windows simultaneously.
C-293	Ability to cascade/tile multiple incident entry windows.
	Ability to enter incidents using:
C-294	Standard call entry screen form
C-295	CAD command on a command line
C-296	Map by clicking on a location
	Duplicate Call Management
C-297	Ability to identify potential duplicate calls.
	Ability to automatically identify potential duplicate calls based on:
C-298	Agency-defined radius around incident location
C-299	Agency-defined time parameter
C-300	Incident/type code
C-301	Specific incident address/event location
C-302	Ability to display proximity calls on a map (e.g., to assist dispatchers in identifying possible duplicate calls).
C-303	Ability to include recently closed incidents in the potential duplicate call identification process.
C-304	Ability to include field-initiated calls in the potential duplicate call identification process.
C-305	Ability for system administrator to define "recently closed" through a configuration parameter (e.g., time period).
C-306	Ability to manually identify a duplicate call and then combine entered call details with primary call.
	Ability to provide the dispatcher with the following information about possible duplicate incidents:
C-307	Incident details
C-308	Incident location
C-309	Incident status
C-310	Incident/type code
C-311	Time the incident was initiated
C-312	Units assigned
C-313	User-defined proximity to current incident
C-314	Original dispatcher

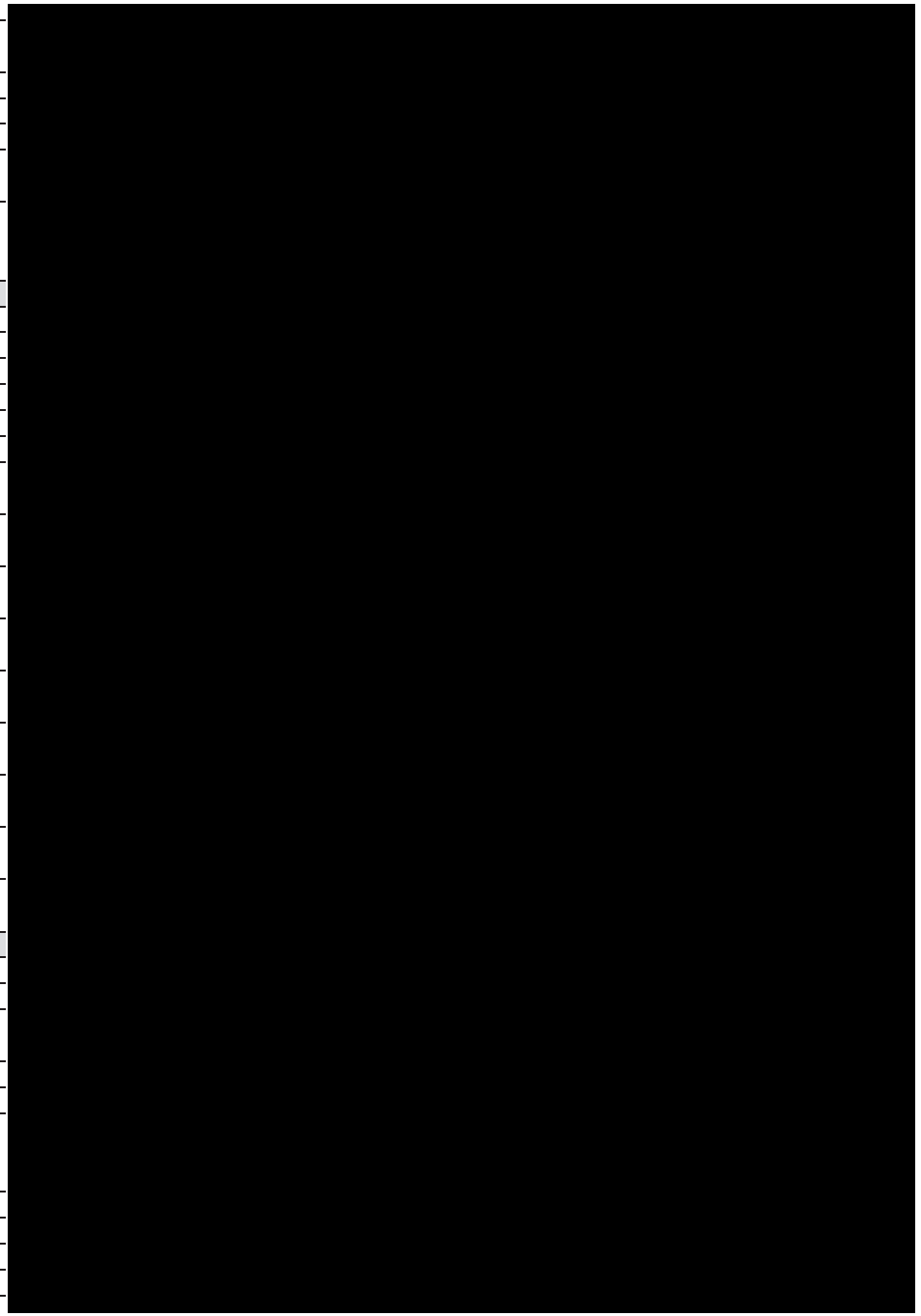
[redacted]

	Ability for the dispatcher to do any of the following if a CAD incident is determined to be a duplicate call:	
C-315	Add to the original incident record a second complainant with complete complainant information and additional incident comments	
C-316	Cancel the newly-entered call.	
C-317	Close a duplicate incident and cross-reference it to the original CAD incident	
C-318	Create an entirely new incident using existing address data	
C-319	Ability to include text from duplicate calls in the primary call.	
C-320	Ability for a dispatcher to handle duplicate calls (e.g., dispatcher identifies a call as a duplicate after the call has been transferred from the call taker).	
	Premise Information Retrieval	
	Ability to automatically initiate, upon address verification, an address inquiry to:	
C-321	Police RMS	
C-322	Fire RMS	
C-323	Regional dataset	
C-324	Agency-defined file	
C-325	Any CAD file containing address information (e.g., trespass, hazardous materials, premise history, etc.)	
	Ability to search for premise information based on:	
C-326	Address with sub-address (i.e., unit number, building floor, apartment number, building complex number/letter, fractions, descriptors)	
C-327	Block ranges	
C-328	Business name	
C-329	Common place names	
C-330	Intersections	
C-331	Ability to automatically show premise history related to a current incident.	
C-332	Ability to view the number of previous calls at a location without having to open a separate screen.	
C-333	Ability to drill down and view past incidents from premise history.	
	Ability to retrieve and attach to a CAD call any information regarding:	
C-334	Alarm/access/entry code	
C-335	Domestic violence	
C-336	Emergency contact information	
C-337	Firearms	
C-338	Hazardous materials	
C-339	Medical concerns	
C-340	Occupancy	
C-341	Pre-plan reference information	
C-342	Previous calls for service	
C-343	Previous contact with vehicle(s) associated with the call	
C-344	Previous contacts with person(s) associated with the call	
C-345	Search caller/reporting party field	
C-346	Other information contained in the premise file	
C-347	Ability for map to display all known hazards within a user-defined radius.	
C-348	Ability to record in the incident history that premise history has been viewed by the user.	

C-349	Ability for premise information to be available to user but not prevent operator from continuing current work (e.g., window does not cover entire workstation screen).	
	Partial Call Entry	
C-350	Ability to save one or more partially complete incidents in order to enter a higher priority incident, keeping all entered data intact.	
C-351	Ability to transfer a partially completed incident with a "details to follow" notification to another user.	
C-352	Ability to provide a warning (visual and/or audible) that a partially complete incident has been held for an agency-defined period of time.	
	Ability to display a summary of all partially completed incidents being held, awaiting completion, including:	
C-353	Elapsed time that the call has been on hold	
C-354	Dispatcher identification number that placed the call on hold	
C-355	Position that placed the call on hold	
C-356	Ability to display a summary of all partially completed incidents being held, awaiting completion, by agency.	
C-357	Ability for any user to select a partially complete incident from the summary list, and complete the incident entry process.	
	Incident Scheduling	
C-358	Ability to enter incidents scheduled for dispatching at a later time (e.g., several hours/days later), maintaining the original time of entry.	
C-359	Ability to modify incidents scheduled for dispatching at a later time (e.g., several hours/days later), maintaining the original time of entry.	
C-360	Ability to cancel incidents scheduled for dispatching at a later time (e.g., several hours/days later), maintaining the original time of entry.	
C-361	Ability to schedule a type of incident to occur on a regular basis.	
	CAD Mapping Requirements	
	General Mapping Requirements	
C-362	Ability for mapping functionality to be integrated into CAD starting at call receipt and continuing through to the conclusion of a CAD incident.	
C-363	Ability to view map through a browser-based interface.	
C-364	Ability to map incoming 911 calls.	
C-365	Ability to map incident location during address verification.	
C-366	Ability to display an address on the map when it is entered into the command line.	
C-367	Ability to provide point and certainty radius of caller as related to wireless Phase I and Phase II mapping.	
C-368	Ability to distinguish between Phase I and Phase II on map by using different symbols, colors and/or text.	
C-369	Ability for system administrator to define Phase I and Phase II symbols and colors.	
C-370	Ability to point with cursor to the incident location on map and have location data populate CAD address fields.	
C-371	Ability to view map in a separate window.	
	Ability to allow users to customize map views including, but not limited to:	
C-372	Font size	
C-373	Level of detail	
C-374	Screen size	

C-375	Ability to use a mouse to "click on" a point at any zoom level and have the street name and latitude/longitude information displayed.	
	Ability to display user-defined street information, at a minimum, by:	
C-376	Block number or address range	
C-377	Latitude/longitude	
C-378	Prefix directional (N, E, S, W, NE, NW, SE, SW)	
C-379	Street name (including alias)	
C-380	Street type	
C-381	Sub-address (i.e., unit number, building floor, apartment number, etc.).	
C-382	Suffix directional (N, E, S, W, NE, NW, SE, SW)	
C-383	Ability to click on a location on a map and pull up any supplemental information (e.g.,. fire pre-plan, hazards, incident history, etc.) associated with that an agency-defined parameter around the location (address, building, block, etc.).	
C-384	Ability to display flags on locations containing additional information (e.g., fire pre-plans, hazards, incident history, etc.).	
C-385	Ability to limit the ability to attach files to addresses based on user ID.	
C-386	Ability to support a map layer for aerial spatial images.	
C-387	Ability to support multiple map configurations by agency.	
C-388	Ability to integrate specific map data associated with an event (e.g., festival, parade, sporting event).	
C-389	Ability to support plume modeling and create it as a GIS layer.	
C-390	Ability to support fire modeling and create it as a GIS layer.	
C-391	Ability to display anticipated response times between two points on a map.	
C-392	Ability to manually display driving directions between two points on a map.	
C-393	Ability to edit map data in industry-standard ESRI applications and formats.	
	Map Navigation	
	Ability to provide the following map navigation functionality:	
C-394	Pan from given area to adjacent area	
C-395	Return back to previous view	
C-396	Zoom in on area for enhanced detail	
C-397	Zoom out of an area	
C-398	Move up and down	
C-399	Move left and right	
C-400	Ability to zoom in on a location and see actual location of unit(s) (if equipped with AVL).	

C-401	Ability for user to update/modify map displays (e.g., preset default zoom levels and views).
C-402	Ability to utilize color, text, and/or symbols to distinguish status of unit.
C-403	Ability for map to center, zoom to call location (via CAD).
C-404	Ability for map to center on and zoom to location upon incident entry.
C-405	Ability for dispatcher to "zoom" map display to predefined views (Jurisdiction, City/County boundary, region, etc.)
C-406	Ability for dispatcher to "zoom" map display for user-defined area by clicking and dragging (i.e., user shall be able to graphically define area to display and system shall present defined area and adjust resolution of map accordingly).
	Ability to center map display on:
C-407	CAD incident location
C-408	Last known location of vehicle (AVL or unit status)
C-409	Specified geographic area
C-410	Specified vehicle/unit
C-411	Vehicle in pursuit mode
C-412	Vehicle activating emergency button
C-413	Ability to close streets by clicking on a specific area (e.g., street, hundred block area) from the CAD map.
C-414	Ability to adjust routing recommendations based on closed streets.
C-415	Ability for user to define an expected duration for street closures.
C-416	Ability to alert user when the expected duration for a street closure has expired.
C-417	Ability to push closed street information to mobile computers.
C-418	Ability to provide directions to an incident from a unit's last known location or, if available, current location based on AVL.
C-419	Ability to provide, in a separate map tab or area, predefined map views of any available map layer.
C-420	Ability for users to define which map layers are displayed.
C-421	Ability to toggle (i.e., reveal/hide) data on the map sucha as, active events, individual discipline units (e.g., ambulances).
	Ability to view on map the locations of:
C-422	All pending and active 911 calls
C-423	Units based on AVL or last known locations
C-424	Ability to display an active, or closed call for service and have it automatically show up on the map.
C-425	Ability to select a unit and have its location automatically display on the map.
C-426	Ability to add user-defined 'pins' to map.
C-427	Ability to label all call locations with the call number.
C-428	Ability to keep an address displayed on the map until it is manually cleared.
C-429	Ability to obtain detailed incident information by double-clicking on map location.
C-430	Ability to display on-scene unit ID with incident number and call type.
C-431	Ability to change the displayed unit location on a map to reflect updated locations.



	Ability to display call information by clicking/hovering on:
C-432	Incident location
C-433	Incident number
C-434	On-scene unit ID
C-435	Units assigned to call
	Ability for agency to define what call information is displayed when clicking/hovering on:
C-436	Incident location
C-437	Incident number
C-438	On-scene unit ID
C-439	Ability for user to turn off "hovering" functionality.
	Ability to zoom to relevant map location by searching on available map layer information including, but not limited to:
C-440	Common names
C-441	Common places
C-442	Intersection
C-443	Hydrants
C-444	Incident number
C-445	Latitude/longitude
C-446	Parcel address including hundred block
C-447	Parcel owner
C-448	Phone numbers
C-449	Owner address
C-450	Owner name
C-451	Owner telephone number
C-452	Street names
	Ability to select vehicles to display on map (filter) by user-defined criteria including, but not limited to:
C-453	Battalion
C-454	Beat
C-455	Fire zone box
C-456	Incident number
C-457	Incident type
C-458	Reporting district
C-459	Sector
C-460	Status
C-461	Type
C-462	Unit ID
	Marquee Functionality
C-463	Ability to display map on a large marquee monitor.

[redacted]

C-464	Ability for the agency to define map layers displayed on the marquee map.	
	Automatic Vehicle Location (AVL)	
C-465	Ability to support the use of a continuous, real-time AVL system via a CAD interface.	
C-466	Ability to support the use of multiple continuous, real-time AVL data feeds for a single unit.	
C-467	Ability to support the use of multiple continuous, real-time AVL data formats (TAIP, NMEA, Windows Location, etc).	
C-468	Ability to control AVL functionality from within the context of CAD so that the user does not have to leave the CAD workstation keyboard or mouse.	
C-469	Ability to integrate AVL and regional routable centerline for most appropriate unit dispatching.	
	Ability to turn AVL on/off by:	
C-470	Agency	
C-471	Unit	
C-472	When a unit's AVL is turned off, ability to default to agency-defined defaults for dispatching.	
C-473	When an agency's AVL is turned off, ability to default to agency-defined defaults for dispatching.	
C-474	Ability to display average speed of vehicle between two points when data is polled.	
C-475	Ability to display the location of all units regardless of status.	
C-476	Ability to display active incident and unit status on the map with colors, text and/or symbols. Colors, text and/or symbols should be same as used in CAD.	
C-477	Ability to display unit numbers.	
C-478	Ability to automatically remove a unit from the map when the unit logs off the Mobile.	
C-479	Ability to log the specific x/y coordinate from where the unit was dispatched prior to responding to an incident.	
C-480	Ability to provide AVL playback, capturing unit location changes indicating the direction and speed of which the resource traveled.	
C-481	Ability to automatically log fire apparatus status as en route to a call upon exiting the station to respond to a call for service.	
C-482	Ability for each agency to define what constitutes on-scene (e.g., police may be considered on-scene a block from an incident location).	
C-483	Ability to prevent or log in the assigned incident, use of on-scene function if unit is not actually on-scene.	
C-484	Ability to utilize AVL location information to create self-initiated incidents and unit recommendations withouth manual intervention.	
	Dispatching	
	CAD Incident Retrieval	
	Ability to cause a distinct user configurable change on the dispatcher's screen to indicate a new incident is waiting, if the window used for incident control is busy:	
C-485	Audible alert	
C-486	Visual alert	
	Ability to cause a distinct user configurable change on the dispatcher's screen to indicate any change in the incident (e.g., comments added, location change, etc.):	
C-487	Audible alert	
C-488	Visual alert	
C-489	Ability for system administrator to create a list of protocols and activities accessible by dispatchers based on incident type and priority.	

C-490	Ability to retrieve a CAD incident and review all available information already entered up to the point of incident retrieval.	[redacted]
C-491	Ability to pull up a specific incident.	
C-492	Ability to retrieve the oldest, highest priority incident from the pending incidents queue for review.	
C-493	Ability to review each pending incident sequentially.	
C-494	Ability to review each pending incident by time entered.	
C-495	Ability to review each pending incident by time elapsed.	
C-496	Ability to keep incidents in pending queue indefinitely.	
	Resource Recommendation	
	Ability to automatically provide appropriate resource recommendations based on any combination of:	
C-497	Station order	
C-498	Agency/Jurisdiction	
C-499	AVL location	
	Closest unit taking into account:	
C-500	Natural boundaries	
C-501	Obstacles	
C-502	Traffic	
C-503	Speed limits	
C-504	Street network	
C-505	Equipment availability	
C-506	Incident area (e.g., unique response for specific response area)	
C-507	Incident location (e.g., unique response for specific location)	
C-508	Incident type	
C-509	Multiple response routes	
C-510	Occupancy type (e.g. residential, office building, etc.)	
C-511	Pre-defined response plans (response area plan)	
C-512	Unit-defined delayed response	
C-513	Special conditions (e.g., heightened response)	
C-514	Special equipment required	
C-515	Type of special skills units required	
C-516	Number of type of special skills units required	
C-517	Type of units required	
C-518	Number of units required	
C-519	Unit identifiers including shift and zone	
C-520	Unit status	
C-521	Ability to prioritize unit response based on incident type so that appropriate units are automatically recommended and/or dispatched in priority order.	
C-522	Ability to enable and disable agency-specific resource recommendations (e.g., specific response plan for Fire, specific response for Police).	
C-523	Ability to re-recommend closest units (e.g., a new unit comes into service).	

C-524	Ability for system to update the unit recommendation if user makes relevant incident information changes (e.g., type, location, alarm level).
C-525	Ability to record the unit recommendation as it was presented to the dispatcher.
	Resource Determination
	Ability to manually display a list of special skills/equipment for:
C-526	All personnel logged on
C-527	A selected person
C-528	Apparatus/vehicle
	Ability to identify all personnel with a specific skill (e.g., language, training, etc.) by:
C-529	Logged on and available
C-530	Logged on and not available (e.g., on another incident)
C-531	Not logged on
	Ability to display potentially available resources based on unit status:
C-532	Assigned to a CAD call
C-533	Assigned to a CAD call with a lower priority
C-534	Unassigned
C-535	Ability to determine appropriate resources based upon any combination of information provided at unit logon.
	Resource Dispatch
	Ability for dispatcher to select and assign/re-assign recommended units using any of the following methods:
C-536	Command line entry
C-537	Function key
C-538	Mouse (drag and drop onto map)
C-539	Ability to preempt units on a call to respond to a different incident.
C-540	Ability to exchange units on a call to replace and re-assign units on two different incidents.
	Ability to dispatch units by:
C-541	Accepting the proposed application recommended units
C-542	Selecting and dispatching units other than those recommended by the application.
C-543	Selecting some, but not all, of the recommended units
C-544	Ability to log recommendation overrides in the audit trail (e.g., recommended units and dispatched units).
C-545	Ability to group and track units that are joined as a team (taskforce, tac team)
	Ability to do the following upon dispatch:
C-546	Automatically assign the recommended or requested units
C-547	Initiate alphanumeric paging
C-548	Remove the incident from the pending queue
C-549	Send the incident to the assigned unit's mobile computer
C-550	Start the status timers
C-551	Update the status display
C-552	Ability to dispatch more than one unit at a time to the same call.
C-553	Ability to assign or add multiple units to an incident with a single command.
C-554	Ability to assign a unit to an incident to which it was not originally recommended.
	Ability to dispatch to multiple types of telecommunications devices simultaneously including, but not limited to:
C-555	Mobile computer
C-556	Smart phone

[redacted]

C-557	Tablet
C-558	Cell phone
C-559	Pager
C-560	Radio
C-561	Ability to configure the system to push out different information based on the receiving device (e.g., short message to alphanumeric paging device and full dispatch message to mobile computer).
C-562	Ability to indicate when typed characters exceed the number of characters allowed when sending data to a device that handles only a limited number of characters.
C-563	Ability to send dispatches to printers (e.g., "rip and run" printers in fire stations).
	Field-Initiated Calls for Service
C-564	Ability for dispatcher to quickly enter field-initiated incidents (e.g., traffic stop).
C-565	Ability to prevent users from self-dispatching to pending incidents from the field.
C-566	Ability to easily add additional units to a field-initiated incident (e.g., traffic stop, subject stop).
C-567	Ability to limit field-initiated calls to agency-defined call types.
C-568	Ability to capture unit ID number when incidents are initiated by a unit in the field.
C-569	Ability to prevent users from creating an incident in the field.
C-570	Ability for dispatcher to "right click" on a unit to bring up the option to place it on a field-initiated incident.
C-571	Ability for dispatcher to verify addresses of field-initiated incidents.
C-572	Ability for dispatcher to use one command line to enter a field-initiated incident and place the initiating unit en route to the incident.
C-573	Ability for dispatcher to use one command line to enter a field-initiated incident and place the initiating unit on-scene.
C-574	Ability for dispatcher to link a field-initiated call to another incident.
	Ability for dispatcher to quickly record the following information when a unit is placed in a traffic stop status:
C-575	Location of the stop
C-576	Number of occupants in the vehicle
C-577	Vehicle license plate
C-578	State of registration
C-579	Make, model and color of vehicle
	Ability for dispatcher to quickly record the following information when a unit is placed in a subject stop status:
C-580	Location of the stop
C-581	Number of subjects
C-582	Vehicle license plate
C-583	State of registration
C-584	Name
C-585	Date of birth
C-586	Driver license number
C-587	Social security number
C-588	Make, model and color of vehicle
C-589	Ability for dispatcher to put a unit on a traffic stop and run the plate in one step.

[redacted]

C-590	Ability for dispatcher to put a unit on a subject stop incident and run a wanted check in one step.
C-591	Ability for field personnel to initiate an administrative incident (e.g., put units out on training or drills).
	Vehicle Pursuit Dispatch
C-592	Ability to use live AVL to track vehicle pursuits real-time.
C-593	Ability to provide a vehicle pursuit command that allows a unit to be pre-empted from its current call, assign the pursuit call, and place the original call back in the queue for the original unit or for another unit.
C-594	After using the vehicle pursuit function command, ability for user to be able to add comments continuously to the record without entering another command or retrieving the incident.
C-595	Ability to time stamp each comment.
C-596	Ability to quickly alert other users logged into the system of active pursuit incident.
	Unit Assignment to CAD Incident
C-597	Ability to update unit status to associate the dispatched unit or units with the CAD incident.
C-598	Ability to differentiate units based on assignment group (e.g., first alarm v. second alarm, primary v. backup, etc.)
	Ability to take a unit off a call and reassign the unit to a new call via:
C-599	Single command
C-600	Drag and drop
C-601	Ability to use one command to both dispatch and put "en route" field personnel (e.g., if field personnel is "assisting another unit").
C-602	Ability to use one command to both dispatch and put "on scene" field personnel (e.g., if field personnel is "out with another unit").
	Call Stacking/Queuing
C-603	Ability to hold an incident for a specific unit.
C-604	Ability to automatically (without user intervention) notify the dispatcher of a held incident when the unit becomes available.
C-605	Ability for dispatcher to hold and/or assign more than one incident to a given unit or resource (call stacking).
C-606	Ability for agency to set time limits for stacked calls by priority (e.g., a queue limit of two hours for priority 5 calls and one hour for priority 3 calls).
C-607	Ability for authorized user to set queue limits for numbers of incidents allowed to be stacked in a given queue.
C-608	Ability for administrator to turn call stacking on and off.
	Call Preemption
C-609	Ability to pull a unit off an incident and reassign the unit to a new incident.
C-610	Ability to visually indicate a preempted call (e.g., color code).
	Ability to support a swap feature to allow two units to exchange incidents via:
C-611	Command line
C-612	Function key
C-613	Drag and drop
C-614	Ability to support a unit exchange command which allows the dispatcher to remove an assigned unit from an incident and assign a second unassigned unit to the first unit's incident in "en route" status. The application shall place the first unit back in service. This to be performed using either the assigned or unassigned unit.

C-615	Ability to support a unit exchange command which allows the dispatcher to exchange two assigned units on two different incidents, placing both units in "en route" status on the respective incidents.	
	Unit Management	
	Unit Placement in Service	
C-616	Ability to log one or more units on-duty or off-duty with a single command.	
C-617	Ability to define a roster (e.g. squad, company, etc.).	
C-618	Ability to place all units in a predefined roster on or off-duty with a single command.	
C-619	Ability to place a roster on-duty with units remaining unavailable or not recommended for calls until they notify the dispatcher that they are in service.	
C-620	Ability to allow for single unit exceptions when placing a roster on or off duty.	
C-621	Ability to log an apparatus into service for assignment without defining staff or personnel.	
C-622	Ability to identify fire units by special equipment (e.g., rescue tools, etc.).	
C-623	Ability to keep vehicles (e.g., fire apparatus) on duty (e.g., 24x7) and change personnel associated with the vehicles (e.g., on shift changes).	
C-624	Ability to make a unit available for only certain types of calls.	
C-625	Ability to allow for supervisor to place units into or out of service.	
C-626	Ability for units to log themselves into or out of service from a workstation or device other than a CAD workstation.	
C-627	Ability for units to log on to the system without being available for calls.	
C-628	Ability for units to indicate when they are available for calls.	
C-629	Ability for dispatchers to place multiple units (e.g., an entire squad or company) into available for call status.	
C-630	Ability for dispatcher to add an staff member to a unit at any time.	
C-631	Ability for dispatcher to remove a staff member from a unit at any time.	
C-632	Ability for personnel to be associated with any mobile unit (e.g., vehicle, apparatus, etc.).	
C-633	Ability to track the activity of each individual associated with a mobile unit.	
C-634	Ability to associate multiple individuals with a unit.	
C-635	Ability to indicate a unit does not have a mobile computer.	
C-636	Ability to indicate a unit does not have an AVL/GPS data source/device.	
C-637	Ability to manage units without a mobile computer.	
C-638	Ability to manage units without an AVL/GPS data source/device.	
C-639	Ability to simultaneously create an incident and log field personnel onto that call (e.g., off-duty field personnel taking calls).	
C-640	Ability to simultaneously clear field personnel from a call and log the personnel out of the system (e.g., for field personnel taking calls when off-duty).	
C-641	Ability to sign a unit on with temporary call sign (e.g., to indicate off-duty or on special assignment).	
	Cross Staffing	
C-642	Ability to identify company personnel capable of staffing multiple resources.	
C-643	Ability to identify apparatus that cannot be used if another apparatus is in service (a brush vehicle cannot be staffed if an Engine from the same station is assigned to an incident)	

C-644	Ability to assign company personnel to the appropriate apparatus depending on the nature of the emergency (e.g., ALS apparatus if medical emergency and fire apparatus if fire emergency).	
C-645	Ability to remove an apparatus from service if personnel are not available to staff the apparatus (e.g., personnel are assigned to another apparatus for a call).	
C-646	Ability to place an apparatus back in service when personnel are available to staff the apparatus.	
	Unit Status Display	
C-647	Ability to monitor an unlimited number of units.	
C-648	Ability to support multiple Agency-configurable status values. Note any application limits (vendor-managed, only 20, etc.) in the Comments.	
C-649	Ability to generate additional unit statuses as needed.	
C-650	Ability to define unit status conditions that support current dispatch center operations.	
C-651	Ability to associate a default assignment availability with each status (e.g., unit available for incident assignment when in particular status).	
C-652	Ability to modify unit availability regardless of status (e.g., on-scene, but available).	
	Ability to display the following unit information:	
C-653	Any portable Radio IDs associated with unit/vehicle	
C-654	Assigned Battalion	
C-655	Assigned Beat	
C-656	Assigned Call type	
C-657	Assigned Division	
C-658	Current location	
C-659	Current Radio channel	
C-660	Current Sector	
C-661	Current status	
C-662	Currently-assigned incident number	
C-663	Elapsed time in current status	
C-664	Last known location	
C-665	Logged onto Mobile (Y/N)	
C-666	Radio Name	
C-667	Receiving AVL/GPS data	
C-668	Special note or comments	
C-669	Special skills/training	
C-670	Unit ID/call sign	
C-671	Vehicle number	
C-672	Vehicle Radio ID	
C-673	Any information captured at logon	
C-674	Ability to dynamically (automatically update) display unit status data.	
C-675	Ability to sort displayed data by any unit information (e.g., incident, unit, location, status, etc.).	
C-676	Ability to create a custom view that can include units from any agency (e.g., combination of Police and Fire units).	
C-677	Ability to perform a secondary sort of displayed data.	
C-678	Ability to limit (include or exclude) the units to be displayed in a single status monitor (e.g., by response area, type, status).	
C-679	Ability of status monitor to automatically apply a scroll-bar at any time the number of units exceed the size of the window.	

C-680	Ability to visually differentiate, through color, text and/or symbol, units in varying status or conditions.
C-681	Ability to visually differentiate, through color, text and/or symbol, types of units at incident.
C-682	Ability to offer the option of an audible alert to accompany the visual signals used to signify changes in status.
C-683	Ability to offer configuration parameters for turning the audible alert on and off for each status.
C-684	Ability to use symbols or characters in the unit status display to supplement unit status color.
	Unit Activity Tracking
C-685	Ability to record all unit incident assignments including but not limited to Traffic Stops, Subject Stops, self-initiated or Dispatch-initiated assignments. This should include timestamps and a record of person performing.
C-686	Ability to record all unit locations or AVL location data. This should include timestamps.
C-687	Ability to record all unit status changes. This should include timestamps and a record of person/application performing the change.
C-688	Ability to review unit status history within the CAD application, through a web interface or another CAD-based feature.
	Ability to time/date stamp all:
C-689	Location updates
C-690	Status changes
C-691	Unit assignments
C-692	Ability to record multiple agency-defined time-stamped status messages (e.g., arrival time, start of extrication, etc.).
	On-Scene Arrival Tracking
	Ability to record multiple arrival times, including:
C-693	Arrival at a staging area
C-694	Arrival in area
C-695	Arrival at the incident location (e.g., room within a building)
C-696	Arrival at the scene (e.g., general location)
C-697	Arrival at patient
C-698	Ability for agency to define recommended order for recording different types of arrival times.
C-699	Ability to automatically populate previous arrival times in the defined sequence.
C-700	Ability to support different arrival time definitions by agency (Law vs. Fire)
C-701	Ability to automatically mark a unit on-scene when it comes within a defined distance of the incident location.
	Ability to record multiple units arriving:
C-702	At one time (all at once)
C-703	At different times
	Unit Status Timers
C-704	Ability for each unit status to have an associated agency-defined timer.
	Ability to alert the dispatcher to the expiration of the timer associated with any unit status change:
C-705	Audible alert
C-706	Visual alert
C-707	Ability to record dispatcher acknowledgement of timer alert.
	Ability for dispatcher to do one of the following upon timer expiration:

[redacted]

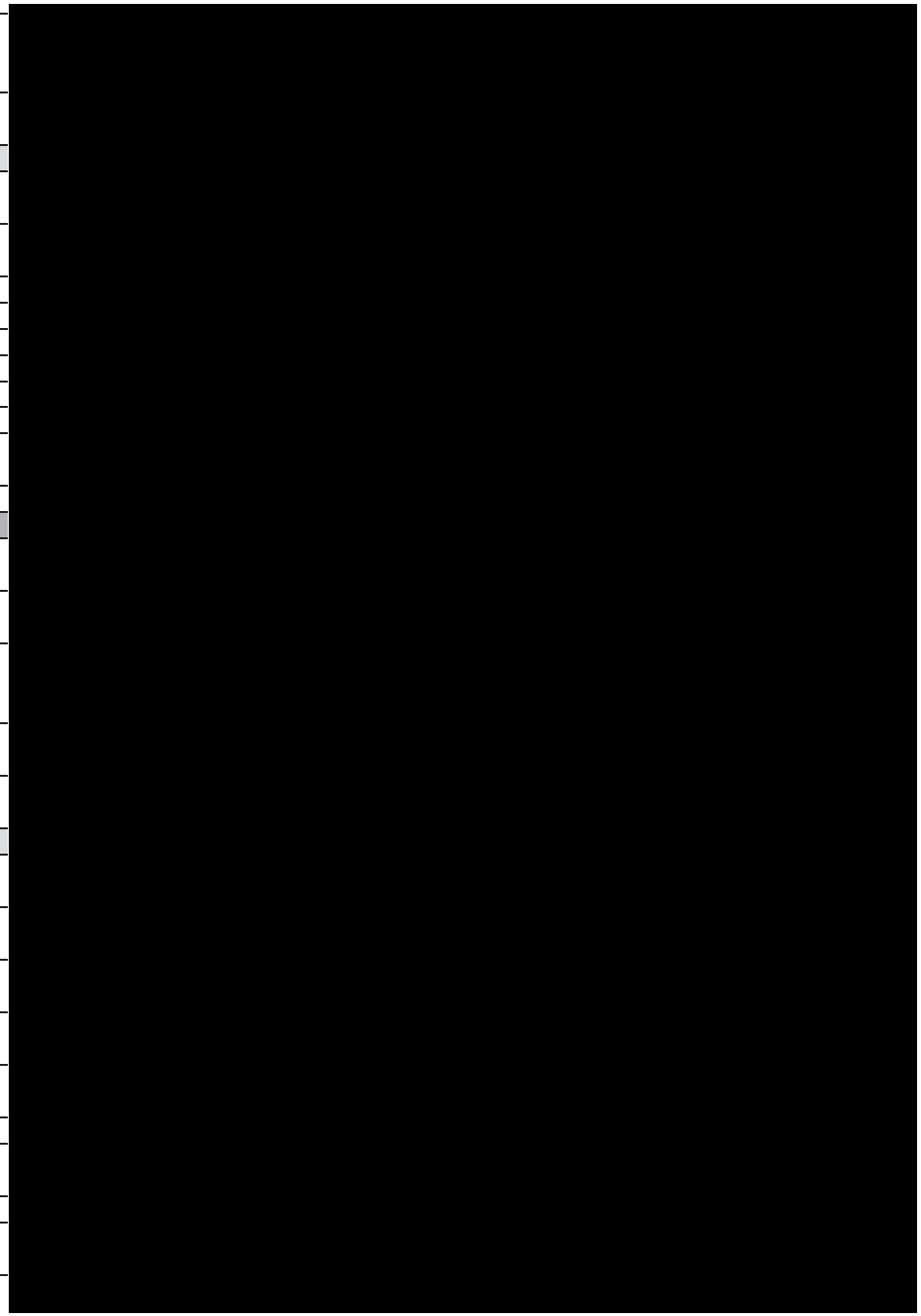
C-708	Modify timer to new time value
C-709	Cancel timer
C-710	Reset to default value
C-711	Ability for dispatchers to reset timers at any time.
	Status Monitoring
	Ability to initiate status changes via the following methods:
C-712	Command line
C-713	Function key
C-714	Mouse click (e.g., screen icon)
C-715	Ability to time stamp and record each status change in the audit trail.
C-716	Ability to track the activity of a field unit by unit number.
C-717	Ability to track the activity of a field unit by personnel ID.
C-718	Ability to track the activity of a field unit by incident number.
C-719	Ability to track times for each unit assigned to a given incident separately.
C-720	Ability to continually display status of all units.
	Ability to automatically notify users monitoring or displaying the incident that information has changed:
C-721	Audible alert
C-722	Visual alert
	Unit Clearance
C-723	Ability to clear one unit from a CAD incident while allowing the other assigned units to remain on the call.
C-724	Ability to select any number of units to clear from CAD incident.
C-725	Ability to clear all units simultaneously from a CAD incident.
C-726	Ability to display confirmation prior to clearing the last unit from a CAD incident.
C-727	Ability to alert responding units when additional units are cleared or assigned to an incident.
	Unit Reassignment
C-728	Ability to reassign a unit to an available status upon clearing from a call.
C-729	Ability to receive Mobile transmissions to update CAD and reflect the new status of the unit.
C-730	Ability for a unit to remain on scene with an available on-scene status.
	Call Management
	CAD Call Display
C-731	Ability to monitor an unlimited number of incidents (if limited, indicate the maximum in the "comments" field).
C-732	Ability to assign and display an unlimited number of units to an incident [if limited, indicate the maximum permissible in the "comments" field]
	Ability for a user to select an incident for continuous monitoring such that:
C-733	Incident appears in a separate window
C-734	All incident or unit activity, regardless of point of entry, is displayed in this window as it is recorded to the CAD database
C-735	Ability to review incident information in reverse chronological order.
C-736	Ability to allow for an unlimited number of incident statuses (if limited, indicate the maximum in the "comments" field).
C-737	Ability to return incident to pending incident queue if the assigned unit has not responded to initial dispatch notification.
C-738	Ability to view incident details of one or more incidents at a time.

C-739	Ability to create pre-defined incident status monitors to accommodate logical groupings (e.g., by status or area).	
C-740	Ability to limit (include or exclude) the units or incidents to be displayed in a single status monitor (e.g., by response area, jurisdiction, type, status).	
C-741	Ability for dispatcher to transfer management of all calls except one (e.g., a hot call) to another dispatcher.	
C-742	Ability to display a call count summary based on agency-defined groupings.	
C-743	Ability to click on an active incident and group or highlight all assigned units in the unit monitoring window.	
C-744	Ability to show incidents on the CAD mapping display.	
C-745	Ability to use color to distinguish incident priority and status on the CAD mapping display.	
	CAD Incident Update Display	
C-746	Ability to dynamically display (e.g., automatically update) incident status data in a summary window (status monitor).	
C-747	Ability for dispatchers of all involved agencies to be notified (with visual and/or audible alerts) of another dispatcher-initiated change (e.g., incident cancellation, unit reassignment, etc.).	
C-748	Ability to provide a special location to display "hot" calls.	
C-749	Ability for agency to define "hot" calls.	
C-750	Ability to initiate a perimeter command to generate a perimeter upon entry of a location and perimeter distance (e.g., set a 3 block perimeter around 300 Main St.).	
C-751	Ability to send suggested perimeter positions to a unit.	
	CAD Incident Updates	
C-752	Ability for one or more operators to simultaneously add incident information to an active (open) incident without losing data.	
	Ability to update the status of the call as new information is received including, but not limited to:	
C-753	Incident Type	
C-754	Incident priority	
C-755	Incident location	
C-756	Fire alarm level	
C-757	Comments	
C-758	Ability for operators to add information to a CAD incident after the incident has been routed to another dispatcher.	
C-759	Ability to update call information immediately after new information is added to an open call.	
C-760	Ability to simultaneously notify call taker, dispatcher and dispatched units of updated information.	
C-761	Ability for dispatcher screen to update automatically as new information is added to a call.	
C-762	Ability for the screen of anyone monitoring a call to update automatically as new information is added to a call.	
C-763	Ability to add information to an existing CAD incident record from the command line without retrieving the CAD incident.	
C-764	Ability for any authorized user to add new or additional information to a CAD incident.	
C-765	Ability to automatically record all CAD incident information changes in chronological order.	
C-766	Ability to date and timestamp all updates to CAD incident record.	

C-767	Ability to record user identification information with updates to CAD incident records.
C-768	Ability to configure system to automatically send supplemented closed call to dispatch supervisor.
C-769	Ability to maintain a record of all CAD incident information changes.
C-770	Ability to automatically display incident updates to all users viewing an incident at the time the update is made (e.g., automatically refresh screens when new information is added to the incident).
C-771	Ability for one or more operators to simultaneously add supplemental information to a closed incident.
C-772	Ability for system to automatically highlight changes made since last entry.
C-773	Ability to cross-reference and link any combination of open and closed incidents.
C-774	Ability to show all associated/linked calls.
C-775	Ability for users to add supplemental information to closed incidents by accessing the incident using the original incident number.
C-776	Ability to establish rules for operator notification of supplemental information being added to closed calls.
C-777	Ability to prompt operator to verify creation of another incident or to add supplemental information to an existing incident.
	Incident Status Timers
C-778	Ability for each incident status to have an associated agency-defined timer.
C-779	Ability to create a custom, one-time incident specific elapsed timer (e.g., unit contact timer).
C-780	Ability to create a recurring timer that is activated at agency-defined intervals.
	Ability to alert the dispatcher to the expiration of the timer associated with any incident status change:
C-781	Audible alert
C-782	Visual alert
C-783	Ability to record dispatcher acknowledgement of timer alert.
	When a status timer expires, dispatcher shall have the following options:
C-784	Modify to new time value
C-785	Cancel timer
C-786	Reset to default value
C-787	Ability for a dispatcher to reset an incident status timer at any time.
	Reopening CAD Incidents
C-788	Ability to reopen closed incidents.
C-789	Ability to reopen a closed call without losing previously recorded date and timestamps.
C-790	Ability to assign units to reopened calls.
C-791	Ability to record the re-opening command in the original incident audit trail and continue recording actions to the original audit trail.
C-792	Ability for dispatchers to add comments to a CAD call record after the call is closed without reopening the incident.
C-793	Ability to notify dispatch that comments were added to a closed CAD call record (e.g., without having to reopen the incident).
	Cross-Referencing Calls
C-794	Ability to cross-reference two or more active incidents.
C-795	Ability to link two or more active incidents (e.g., to enable hyperlinks during subsequent incident queries).
C-796	Ability to cross-reference active and closed incidents.

C-797	Ability to link active and closed incidents (e.g., to enable hyperlinks during subsequent incident queries).	
C-798	Ability to cross-reference closed incidents.	
C-799	Ability to link closed incidents (e.g., to enable hyperlinks during subsequent incident queries).	
	Call Disposition	
	CAD Incident Cancellation	
C-800	Ability to cancel an incident with a single command.	
C-801	Ability to limit the authority to cancel a call by security profile.	
C-802	Ability for the agency to determine who has the authority to cancel a call.	
C-803	Ability to mandate that the user enter a reason for canceling an incident prior to the system executing the command to cancel.	
C-804	Ability to automatically remove the incident from the pending or active incidents queue and add the disposition (e.g., cancelled) upon execution of a command canceling an incident.	
C-805	Ability to automatically clear all dispatched units from the incident upon incident cancellation (e.g. upon invoking the cancel command).	
	Disposition Recording	
C-806	Ability for the agency to define incident disposition types.	
C-807	Ability to support an unlimited number of disposition types [if limited, indicate the maximum permissible in the "comments" field]	
C-808	Ability for the agency to define multiple disposition types for one incident.	
C-809	Ability to define incident disposition types by agency.	
C-810	Ability to enter a disposition to clear an incident.	
C-811	Ability to require a disposition code before an incident can be cleared.	
C-812	Ability for either dispatchers or field personnel to enter the disposition code.	
C-813	Ability to enter comments of unlimited-length along with a disposition [if limited, entered the maximum in the "comments" field]	
C-814	Ability to require comments based on disposition code.	
C-815	Ability to add one or more unit dispositions without affecting the incident disposition.	
C-816	Ability to associate each disposition with the unit giving the disposition.	
C-817	Ability to create a final master disposition for an incident.	
C-818	Ability for each agency to reject a disposition if unsuitable for the incident type based on agency-defined criteria.	
	Report Need Determination	
C-819	Ability to identify based on disposition type or criteria whether a report is required.	
	Ability to transfer call for service data to:	
C-820	Police RMS	
C-821	Police Field Reporting (e.g. to initiate a report)	
C-822	Electronic Patient Care Report	
C-823	Fire RMS	
C-824	LE/CJIS System data sharing	

C-825	CAD-to-CAD Interface
C-826	Ability to initiate a report before incident is closed (e.g., download data to RMS prior to closing the incident in CAD).
	CAD Incident Closure
C-827	Ability to clear more than one selected unit from an incident while leaving one or more selected units on the incident.
C-828	Ability to clear a single unit from an incident without clearing other assigned units from the incident.
C-829	Ability to clear multiple units without closing the incident.
C-830	Ability to clear multiple units with a single disposition.
C-831	Ability to require confirmation before closing a CAD incident.
C-832	Ability to close call that does not require the dispatch of resources.
C-833	Ability to change any call data before closing an incident.
C-834	Ability to change an incident disposition after a call is closed.
C-835	Ability to provide a unique visual indicator (e.g., flag, change in font color) that data has been changed after the call was closed.
C-836	Ability to add an incident disposition after a call is closed.
	Communications Supervisor Support
C-837	Ability for a communications supervisor to monitor system configuration and current staffing (e.g., who is signed-on, at what position, and with what responsibilities).
C-838	Ability for a CAD workstation to be configured as a supervisor workstation upon logon of a user with a CAD supervisor profile.
C-839	Ability to generate statistical information from within the CAD application on all dispatcher activity including all incident management time parameters (time on hold, response time, etc.).
C-840	Ability for a communications supervisor to monitor activity remotely (from a Supervisor desk) on any user workstation.
C-841	Ability for a communications supervisor to remotely take direct control over a workstation.
	CAD Testing/Training Environment
C-842	Ability to support a CAD testing/training environment that is identical to the CAD production environment.
C-843	Ability to designate any production workstation as a training workstation based on user log on.
C-844	Ability to designate any training workstation as a production workstation based on user log on.
C-845	Ability for accurate testing and training to occur without impacting the production environment.
C-846	Ability to visually distinguish testing/training environments from production environments.
C-847	Ability to include all code tables in the testing/training environment.
C-848	Ability for code table updates to propagate throughout the CAD system (e.g., be CAD-wide, not just agency-specific) when appropriate.
C-849	Ability for testing/training code tables to reflect current production code tables.
C-850	Ability to update testing/training system with historical data from production system at agency-defined intervals.

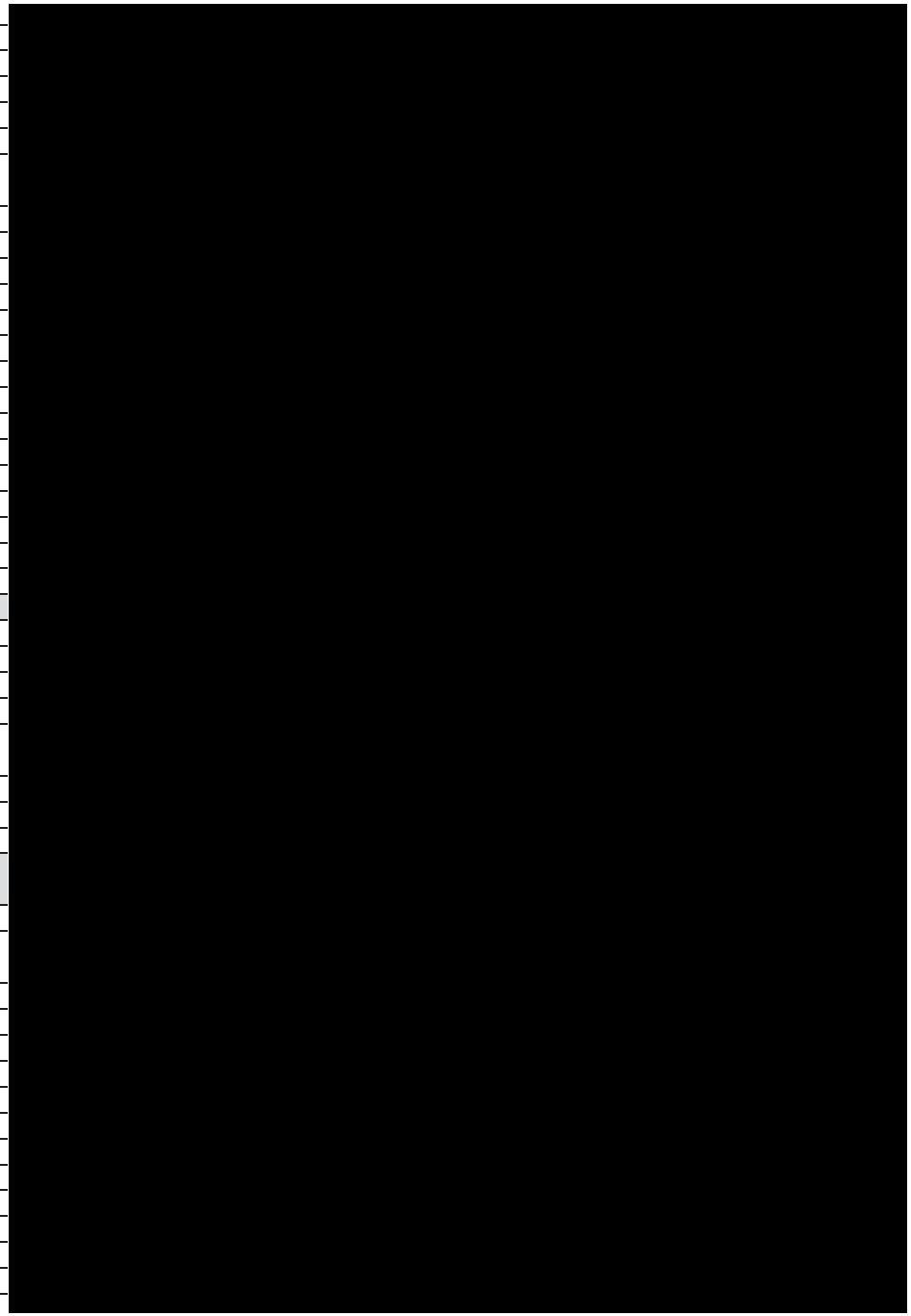


C-851	Ability to seamlessly export changes made to code tables in the testing/training system to the production system.	[redacted]
C-852	Ability to support separate interfaces, to mirror production, in the test and training environments (E9-1-1, Mobile, call triage, RapidSOS, paging, etc.).	
	Operational Queries	
	Ability to query and view the following by any layer (e.g., beat, sector etc.):	
C-853	Active calls	
C-854	Assigned calls	
C-855	Closed calls	
C-856	Priority calls	
C-857	Waiting (pending) calls	
C-858	Any agency-defined data	
	Ability to review a summary of all active calls that have been entered for dispatch by:	
C-859	Group	
C-860	Priority	
C-861	Any agency-defined data	
C-862	Ability to review a summary of all pending calls that have been entered for dispatch.	
	Ability to query unit history by any combination of:	
C-863	Date and time range (e.g., start and end date and time parameters)	
C-864	Unit ID(s)	
C-865	Personnel ID(s)	
	Ability to query resource availability by:	
C-866	Current location	
C-867	Dispatch group	
C-868	Geographic area (e.g., fire zone box, beat, sector)	
C-869	Special skills	
C-870	Unit types (e.g., apparatus, patrol units, Hazmat, etc.)	
	Ability to query unit status by:	
C-871	Date and time range	
C-872	Dispatch group	
C-873	Personnel ID	
C-874	Geographic area (e.g., fire zone box, beat, sector)	
C-875	Incident type	
C-876	Unit ID	
C-877	Unit types (e.g., apparatus, patrol units)	
	Ability to query the following unit status summary information:	
C-878	Elapsed time in current status	
C-879	Incident type	
C-880	Unit ID	
C-881	Unit status	
C-882	Ability to search and review historical information by any data entry field.	
	Ability to query activity by:	
C-883	Unit ID	
C-884	Personnel ID	
C-885	Date and time range	
C-886	Disposition	

C-887	Geographic area (e.g., fire zone box, beat, sector)	[redacted]
C-888	Incident type	
C-889	Location	
C-890	Reporting area	
C-891	Shift	
	Query Return Features	
C-892	Ability to narrow down searches (search within a search).	
C-893	Ability to drill down on query results.	
C-894	Ability to save queries for later use.	
	Ability to restrict queries that result in large volumes of data by:	
C-895	Providing a warning of the numbers of records found	
C-896	Providing a warning of the size of records found	
C-897	Requesting users to prompt the system to continue the query	
C-898	Ability to limit the number of records viewed at a time to a user-defined number.	
C-899	Ability to clearly indicate when additional information (e.g., more query returns) is available.	
C-900	Ability to print query returns at any time.	
C-901	Ability to direct query results to any printer.	
C-902	Ability to direct query results to any terminal.	
C-903	Ability to sort query results by any criteria (e.g., most recent to oldest, by priority, etc.).	
	BOLOs	
C-904	Ability to create and maintain BOLOs (based upon level of security clearance).	
C-905	Ability to provide an audit trail for BOLOs.	
C-906	Ability for field personnel to create BOLOs.	
C-907	Ability to associate a BOLO with a case number.	
	Ability to provide the following fields for a BOLO record:	
C-908	Date issued	
C-909	BOLO expiration date	
C-910	Nature of the BOLO	
C-911	BOLO priority	
	Subject name:	
C-912	Description	
C-913	Known address or location	
C-914	Date of birth	
C-915	Height	
C-916	Weight	
C-917	Hair color	
C-918	Eye color	
C-919	Subject driver's license number	
C-920	Vehicle description	
C-921	Vehicle license plate	
C-922	Weapon (multiple)	
C-923	Known associates	
C-924	Last known location	
C-925	Direction of travel	
C-926	Contact Information	
C-927	Person issuing the BOLO	
C-928	Additional information in free-form text field	

C-929	Ability to search for BOLO based upon any of the above-mentioned items.	[redacted]
C-930	Ability to accommodate multiple subjects in a BOLO.	
C-931	Ability to accommodate multiple vehicles in a BOLO.	
C-932	Ability to accommodate multiple weapons in a BOLO.	
C-933	Ability to attach a file to a BOLO.	
C-934	Ability to embed a photo in a BOLO.	
C-935	Ability to update a BOLO.	
C-936	Ability to set time limits for BOLO retention.	
C-937	Ability to delete a BOLO.	
C-938	Ability to generate, at user-defined times, reports listing expired BOLOs.	
C-939	Ability to designate groups or individuals to whom BOLOs should be sent.	
C-940	Ability to archive expired BOLO records.	
C-941	Ability to search expired BOLO records.	
C-942	Ability to view BOLO from any device connected to CAD, including Mobile, Smart phone, Web interface, etc	
	Management Reporting	
	Public Release of Information	
C-943	Ability to generate a list of incidents to be shared with the public based on agency-specific business rules.	
C-944	Ability to generate a report containing a summary of incidents for an agency-defined period of time for distribution to the public.	
	CAD Searches	
C-945	Ability to conduct searches in CAD on any available operational data field.	
	CAD Reporting	
C-946	Ability to isolate queries in the database to a single agency's incidents (e.g., Police or Fire/EMS only).	
C-947	Ability to conduct queries system-wide.	
C-948	Ability to run CAD reports without exiting the operational CAD application.	
C-949	Ability to create, within the CAD application, ad hoc CAD reports on any data fields in the CAD database (e.g., without using a third party reporting tool).	
C-950	Ability to create, within the CAD application, standard reports consistent with NFPA 1221 benchmarks.	
C-951	Ability to create, within the CAD application, standard reports consistent with NFPA 1710 benchmarks.	
	Ability to generate the following standard reports from within the CAD application:	

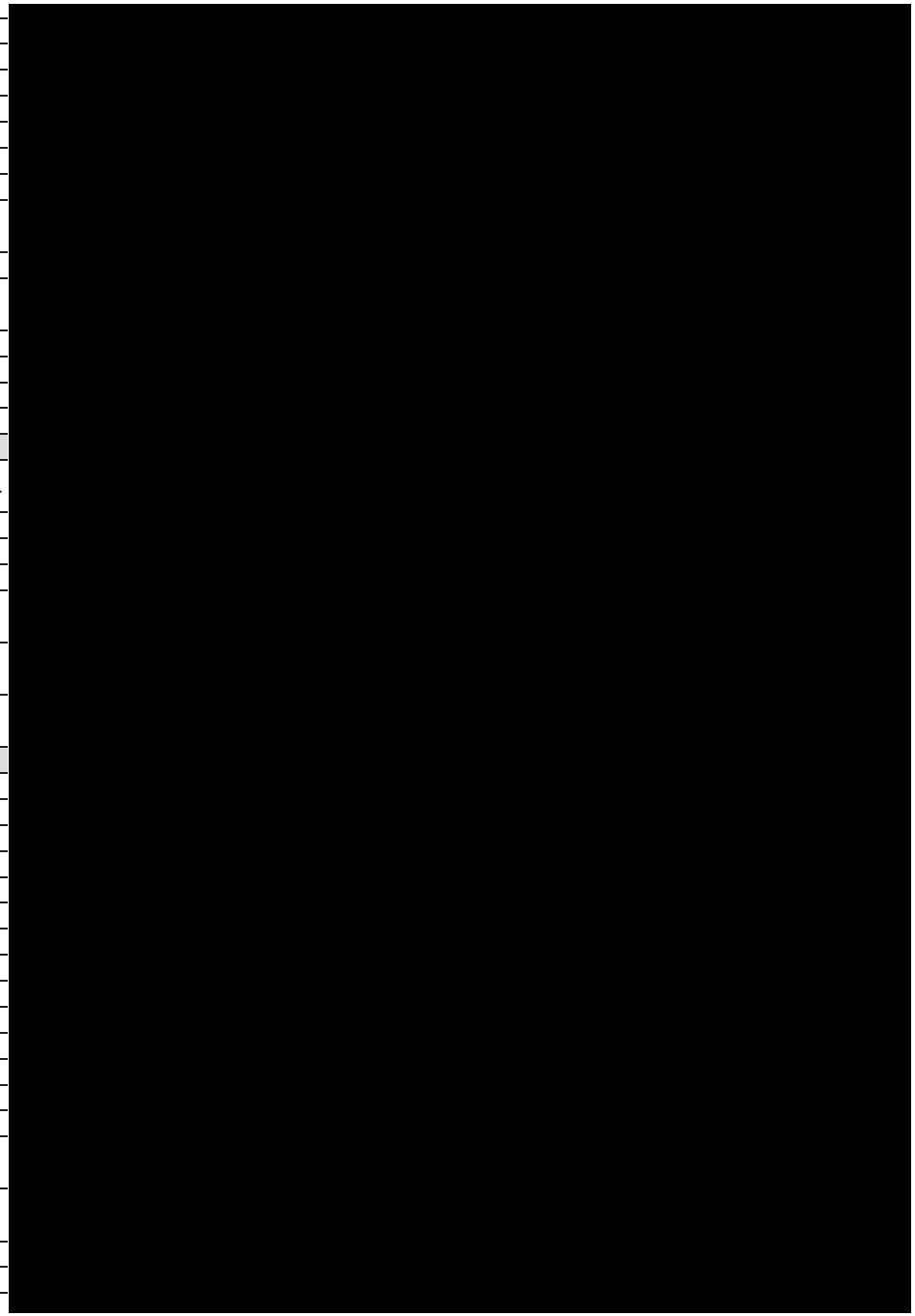
C-952	Incident analysis by day of week
C-953	Incident analysis by geographic area
C-954	Incident analysis by hour of day
C-955	Incident analysis by shift
C-956	Incident analysis by call type
C-957	Incident analysis by TTY/TDD
C-958	Incident analysis by geographic area by hour of day
C-959	Incident analysis by census tract
C-960	Incident analysis by zip code
C-961	Incident analysis by any agency-defined layer
C-962	Incident analysis by responding agency
C-963	False alarm reports
C-964	Premise history list
C-965	Processing time by method of call receipt.
C-966	Response times by geographic area
C-967	Response times by type of call/priority
C-968	Response times by original call destination
C-969	Response times by assigned unit
C-970	Total and average time on call – by day of week
C-971	Total and average time on call – by geographic area
C-972	Total and average time on call – by hour of day
	Total calls for service by:
C-973	Date or date range
C-974	Disposition
C-975	Time of day
C-976	Total incidents by date by nature or disposition
C-977	Non-availability of defined resources (e.g., units, apparatus type, equipment type, etc.)
C-978	Mutual aid - received
C-979	Mutual aid - given
C-980	Agency-defined query
	Ability to record and create reports from within the CAD application using a combination of any of the following information:
C-981	Alarm type
C-982	All associated geofile information
C-983	ANI/ALI data including address and phone number
C-984	Business or premise name
C-985	Call priority
C-986	Call taker/dispatcher ID
C-987	Comments/narrative (unlimited)
C-988	Commonplace name (e.g., parks, streets, schools)
C-989	Date and time call answered
C-990	Date and time call disconnected
C-991	Date and time call received by 911
C-992	Date and time incident entered
C-993	Date and time incident routed to dispatch
C-994	Date and time location verified



C-995	Date and time of cleared incidents
C-996	Date range
C-997	En route to on-scene time
C-998	Final disposition
C-999	Gap between time a call was received by a dispatcher and the time it was dispatched to a unit
C-1000	Geographical areas defined by the user (e.g., sector, fire zone box, patrol area, etc.)
C-1001	Hazard information
C-1002	Incident number
C-1003	Incident priority
C-1004	Incident type
C-1005	Location address, description, supplemental location
C-1006	Premise and prior information flag
C-1007	Premise type (e.g., building, location, person)
C-1008	Reporting party information, including name, address and phone
C-1009	Source (e.g., 9-1-1 or 10-digit, radio, other codes as defined by agency)
C-1010	Staffing levels
C-1011	Subject stops
C-1012	Time range (any time-stamped incident to any other time-stamped incident
C-1013	Traffic stops
C-1014	Unit/field personnel
C-1015	Unit status
C-1016	User name and ID of all users associated with the incident
C-1017	Workstation ID associated with all CAD functions performed on incident
	Ability to provide an analytical tool that reviews workload by, but not limited to:
C-1018	Workstation
C-1019	Call taker/dispatcher
C-1020	Ability to track when no field personnel are available to respond to a call.
C-1021	Ability to account for unavailable resources in response time calculations.
	Ability to capture a snap shot, based on day and time parameters, of:
C-1022	A workstation
C-1023	General CAD system
C-1024	Ability to print a chronological incident report.
	Ability to generate, from within the CAD application, a daily listing of incidents and personnel assigned to the incidents including, but not limited to:
C-1025	Workstation/terminal
C-1026	Call taker/dispatcher ID
C-1027	Date/time received
C-1028	Disposition
C-1029	Field personnel name
C-1030	Field personnel ID
C-1031	Incident location
C-1032	Incident number

C-1033	Ability to view requested reports prior to printing.	
	Global Report Features	
C-1034	Ability to use functionality within the CAD application to create standard reports that can be made available to all system users.	
C-1035	Ability to maintain a general library of user-created ad hoc reports.	
C-1036	Ability for all authorized users to access the general library of user-created ad-hoc reports.	
C-1037	Ability for users to put their own queries/reports in a "dashboard" for later use.	
C-1038	Ability for dashboard to utilize real-time information from user-specified RMS components (e.g., training, hydrants, equipment, stations, incidents, activity logs, etc.).	
C-1039	Ability to route reports to pre-selected individuals or groups (via system or agency email).	
C-1040	Ability to schedule reports to be automatically created and distributed.	
C-1041	Ability to save reports for subsequent viewing and/or printing.	
C-1042	Ability to delete reports after viewing and/or printing.	
C-1043	Ability to schedule report generating at specified time frames.	
C-1044	Ability to optionally generate a report in HTML (i.e., for viewing on the intranet or internet).	
C-1045	Ability to make standard reports available for publishing on the intranet or internet.	
	Messaging	
	General Messaging Features	
C-1046	Ability to send messages to a user who is not logged into CAD and cache that message for retrieval when the user logs onto CAD.	
C-1047	Ability for message server to continuously attempt to deliver a message until received and confirmed.	
C-1048	Ability for user to retrieve cached messages upon logon.	
	Ability to support a minimum of the following messaging functions to and from any CAD address:	
C-1049	Desktop-to-desktop messaging	
C-1050	Desktop-to-dispatch messaging	
C-1051	Desktop-to-pager messaging	
C-1052	Desktop-to-unit messaging	
C-1053	Unit-to-desktop messaging	
C-1054	Unit-to-dispatch messaging	
C-1055	Unit-to-pager messaging	
C-1056	Unit-to-unit messaging	
C-1057	Ability to send broadcast messages (e.g. to all users).	
C-1058	Ability to support real-time instant messaging.	
	Ability to display the following identifiers within a message:	
C-1059	Sender name	
C-1060	Sender date	
C-1061	Sender time	
C-1062	Sender workstation ID	
C-1063	Sender unit ID	

C-1064	Receiver name
C-1065	Receiver date
C-1066	Receiver time
C-1067	Receiver workstation ID
C-1068	Receiver unit ID
C-1069	Ability to assign and change a priority to a message (e.g., routine, urgent, emergency).
C-1070	Ability for system administrator to define message precedence.
C-1071	Ability for each terminal to have a unique identifier included in each transmission to the host.
C-1072	Ability to provide a web-based version of messaging capabilities.
C-1073	Ability for web version of messaging to be accessed with customer-defined security procedures (i.e., user ID and personal security number).
C-1074	Ability to automatically integrate dispatch-related messages to an incident.
C-1075	Ability to store messages for later viewing.
C-1076	Ability for host computer to store unread messages when user logs off.
C-1077	Ability for messages to be sorted by most recent or first received.
	Sending Messages
C-1078	Ability to create easily accessible agency-defined message forms for specific message types.
C-1079	Ability to create and save agency-defined message groups.
C-1080	Ability to create and save user-defined message groups.
C-1081	Ability to send messages across agencies (e.g., police to fire and vice versa).
C-1082	Ability to select a recipient via a single keystroke or mouse click from the unit status window within CAD.
C-1083	Ability of users to select any number of people as part of a message group with no limitation on the number of people in a group.
C-1084	Ability to enter unlimited narrative with wrap-around feature [if characters are limited, indicate the maximum in the "comments" section]
	Ability to send a message to the following:
C-1085	Battalion
C-1086	District
C-1087	Sector
C-1088	Group of user IDs
C-1089	Group of workstations names
C-1090	Units associated with an incident number
C-1091	Units within a user-defined location (based on selected radius on map)
C-1092	Logged on units
C-1093	Mobile Data Device ID/Name
C-1094	Position IDs (e.g., dispatcher)
C-1095	Unit ID
C-1096	User ID
C-1097	User name
C-1098	Workstation ID or name
C-1099	Ability to automatically populate the "To" field on the message mask when selecting recipients.
C-1100	Ability to select a recipient by a single command to create a message (e.g., double click on a logged on user and message screen pops up)
C-1101	Ability to add to a message before forwarding to another user.
C-1102	Ability to attach files to messages.



C-1103	Ability to imbed images within messages.
C-1104	Ability to set agency-defined file size limit.
C-1105	Ability to automatically compress and resize images to comply with agency-defined file size limits.
C-1106	Ability to send a message to all units handling a specific incident.
C-1107	Ability to send information displayed on screen to another workstation.
C-1108	Ability to transmit a reply message to the originator of a currently displayed message without having to reenter the originator's address.
C-1109	Ability to transmit a "reply all" message to multiple recipients that were part of the originator's message group.
C-1110	Ability to create messages that are retained in the system and sent at pre-specified times.
C-1111	Ability to provide a notification for delivery of messages to the device.
C-1112	Ability to provide a notification for non-delivery of messages (i.e., a message sent to a device or group of devices could not be delivered if a user is not signed-on to the device(s)).
	Receiving Messages
C-1113	Ability to notify receiver via an audible and/or visual flag that a new message has arrived in mailbox.
C-1114	Ability to notify receiver of an unread message after an agency-defined time period.
	Ability to provide a visual distinction between the following:
C-1115	External messages (from external system)
C-1116	General messages
C-1117	System messages
C-1118	Query returns
C-1119	Ability to segregate query returns from general messages (e.g., separate folders or windows).
C-1120	Ability to prevent incoming messages from interfering with current work.
C-1121	Ability to notify receiver of total number of unread messages.
C-1122	Ability for each message to be displayed in a separate window.
C-1123	Ability for messages to be queued in an "inbox" for later viewing at the convenience of users.
C-1124	Ability to identify high priority messages by type of priority (e.g., felony warrant return versus user-defined urgency).
C-1125	Ability of the receiving user to enter a single keystroke command to retrieve and display the message.
C-1126	Ability to set message priority of specific system generated messages (e.g., high priority of warrant file returns).
C-1127	Ability to query message logs by agency-defined criteria (e.g., date/time range, sender, recipient, device).
C-1128	Ability to note time opened/read by receiver.
C-1129	Ability to queue and display message waiting by priority.
C-1130	Ability to clear a message from the queue.
C-1131	Ability to retain a message in the queue.
	Ability to provide the following message indicators:
C-1132	Message acknowledged or not received
C-1133	Message viewed

[redacted]

C-1134	Number and priority of queued messages
C-1135	Number of messages received
C-1136	Number of messages waiting
	Ability to utilize standard keys/touch screen functions to perform the following with one keystroke:
C-1137	Clear display
C-1138	Clear/erase message
C-1139	Clear/erase operator's entire message queue with prompt to confirm deletion
C-1140	Display next message
C-1141	Print/routing
C-1142	Store/recall message from message queue
	Ability to audit messages at a minimum, using the below:
C-1143	Sender name
C-1144	Sender ID
C-1145	Receiver Name
C-1146	Receiver ID
C-1147	Subject keyword
C-1148	Message body keyword
C-1149	Date range
C-1150	Time Range
C-1151	Attachments
C-1152	Any combination of the above
C-1153	Ability to store messages in an agency-defined buffer size.
C-1154	Ability to delete oldest messages as buffer fills.
	CAD System Administration
	CAD Table Maintenance
	Ability to include, at a minimum, the following data tables:
C-1155	Call source (e.g., officer-initiated, 9-1-1, 10-digit, etc.)
C-1156	Call types and priorities
C-1157	Caution or Hazard information
C-1158	Commands
C-1159	Common Locations
C-1160	Devices (Mobile devices, handhelds, workstations, etc.)
C-1161	Dispositions
C-1162	Equipment
C-1163	Event error logs (so vendor can identify and troubleshoot errors)
C-1164	Fire zone box
C-1165	Patrol and command area definitions
C-1166	Personnel, including emergency contact information and current assignment
C-1167	Recommendation plans
C-1168	Skills or capabiltiies of personnel and units
C-1169	Stations or Sub-stations
C-1170	Timers
C-1171	Unit status types (i.e., assigned, unassigned, assigned but available)
C-1172	Units
C-1173	Ability for data tables to be agency-specific.
C-1174	Ability for a user to add a unit for use "on the fly."
	Ability to allow the agency to define the following:
C-1175	Category codes for pull-down lists

C-1176	Codes for each valid call disposition used when clearing a call	
C-1177	Codes for the methods the agency receives calls (e.g., 9-1-1, cell phone, etc.)	
C-1178	Codes used to identify areas for statistical reporting reasons	
C-1179	Dispatch codes	
C-1180	Priorities assigned to call codes	
C-1181	Response procedures	
C-1182	Subtypes of calls	
C-1183	Ability to configure commands (e.g., VS = vehicle stop).	
C-1184	Ability to configure status code colors.	
C-1185	Ability to create and maintain a call type classification that is based upon the time of day.	
C-1186	Ability to modify code tables without advanced database knowledge.	
	CAD Configuration	
C-1187	Ability to create agency-defined data entry screens.	
C-1188	Ability to create agency-defined data fields within entry screens.	
C-1189	Ability to configure the field entry sequence.	
C-1190	Ability to create conditional fields and mandatory data elements based on agency-defined criteria.	
C-1191	Ability for agency to add or change data elements on any screen based on defined system permissions.	
C-1192	Ability to create agency-defined data lists for all configurable drop-down menus.	
	Ability for agency to configure alerts:	
C-1193	Associated message displayed	
C-1194	Audible indicator	
C-1195	Visual indicator	
	Deployment Plans	
C-1196	Ability to generate temporary deployment plans.	
C-1197	Ability to include multiple agencies in deployment plans.	
C-1198	Ability for user to override temporary deployment plan recommendation.	
C-1199	Ability to maintain deployment plans for a location.	
C-1200	Ability to retrieve and load a new deployment plan with a single command.	
C-1201	Ability to load a new deployment plan without stopping or pausing application operations.	
	Agency-Configurable Response Plans	
	Ability to develop agency-configurable response plans based on:	
C-1202	Geographic area (e.g., beat, sector, fire zone box, etc.)	
C-1203	Multiple response route configuration (e.g., divided highway).	
C-1204	Time of day	
C-1205	Alarm level	
C-1206	Call type	
C-1207	Fire pre-plan	
C-1208	Resource availability	
C-1209	Station coverage requirements	
C-1210	Ability to accommodate a minimum of ten alarm levels.	
C-1211	Ability to assign a single response plan with multiple call types.	
C-1212	Ability for a communications supervisor to update the response plans (e.g., without assistance from technical support or vendor).	
	Premise History File Maintenance	
C-1213	Ability to update/create CAD premise history files.	

C-1214	Ability to automatically update premise history when an incident occurs.
	Ability to capture the following information when creating premise history:
C-1215	Date and time stamp
C-1216	Date of incident
C-1217	Disposition
C-1218	Type of incident
C-1219	Incident number
C-1220	Narrative text of unlimited length [if limited, indicate maximum in the "comments" field]
C-1221	Premise safety flag (e.g., checkbox for common types such as Domestic Violence, Gang, etc.)
	Ability to capture and maintain specific premise information, including but not limited to the following:
C-1222	Alarm/access information
C-1223	Officer Safety issues at location
C-1224	Emergency contact information
C-1225	Hazardous conditions
	Previous calls for service based on at least the following:
C-1226	Address/Location
C-1227	Contact information
C-1228	Date and time
C-1229	Incident number
C-1230	Incident type
C-1231	Previous contacts with person(s) associated with the call
C-1232	Protective orders at location
C-1233	Sexual offender at location
C-1234	Special populations
C-1235	Total number of previous calls for service based on a customer-defined period of time
C-1236	Ability to store premise information for an agency-defined length of time.
C-1237	Ability to store premise information for a specific apartment unit/suite number.
C-1238	Ability to define valid date ranges for time limited premise information at a given location (e.g., information valid between <start date> and <end date>.
	Ability to include in a premise record the following information when premise information is added or changed:
C-1239	Expiration date (can be auto filled based on user-defined expiration dates and date stamp)
C-1240	Time and date stamp at time of entry
C-1241	Unit ID of person entering information
C-1242	Agency of person entering information
	Hazard File Maintenance
	Ability to enter hazards associated with:
C-1243	Persons
C-1244	Specific locations
C-1245	Address ranges
C-1246	Vehicles
	Ability to enter a hazard with at least:
C-1247	Expiration date (can be auto filled based on user-defined expiration dates and date stamp)
C-1248	Time and date stamp at time of entry

[redacted]

C-1249	Unit ID of person entering information	
C-1250	Agency of person entering information	
C-1251	Name of person entering hazard	
C-1252	Time and date stamp at time of entry	
C-1253	Ability to assign codes to hazard types.	
C-1254	Ability to create templates for hazards (e.g., chlorine storage) that are triggered by agency-defined location types (e.g., swimming pool).	
C-1255	Ability to assign priorities to hazard codes.	
C-1256	Ability to assign expiration dates to hazards.	
	Pre-Plans	
C-1257	Ability for CAD to access existing pre-plan information.	
	Ability to provide data fields to maintain pre-plans information, including, but not limited to:	
C-1258	Facility Address	
C-1259	Facility Name	
C-1260	Facility Phone Number	
C-1261	Occupancy Type	
C-1262	Emergency contact name (multiple)	
C-1263	Emergency contact phone number (multiple)	
C-1264	Lock Box Location	
C-1265	Fire Department Connection Location	
C-1266	Hours of Operation	
C-1267	Life Hazards	
C-1268	Maximum Occupancy	
C-1269	Special Information	

C-1270	Invalids	[redacted]
C-1271	Construction type	
C-1272	Exterior Walls	
C-1273	Interior Walls	
C-1274	Roof type	
C-1275	Hazard Rating	
C-1276	Special Hazards	
C-1277	Building Height	
C-1278	Above Grade	
C-1279	Below Grade	
	Fire Protection:	
C-1280	Standpipe/Sprinkler Connection (multiple)	
C-1281	Primary Hydrant	
C-1282	Secondary Hydrant	
C-1283	Hydrant on Alternate Main	
C-1284	Other system (e.g., Halon)	
	Utilities:	

C-1285	Gas shutoff location
C-1286	Electric shutoff location
C-1287	Water shutoff location
C-1288	Fuels (type) shutoff location)
C-1289	Fire Box No.
	Exposures:
C-1290	Interior (type and amount)
C-1291	Exterior (type and amount)
C-1292	HazMat (type and amount)
C-1293	Narrative
	Completed by:
C-1294	Name
C-1295	Badge No.
C-1296	Date
C-1297	Reviewer
C-1298	Ability to create templates for pre-plans.
C-1299	Ability to include images on pre-plan information.
	Flags and Notifications Maintenance

[redacted]

C-1300	Ability to prevent users from disabling audible warning tones.	
C-1301	Ability for high priority incident flags to be available to user but not prevent operator from continuing current work (e.g., window does not cover entire workstation screen).	
C-1302	Ability to provide narrative information with flags.	
C-1303	Ability to keep hazard and event flags in CAD system for an unlimited length of time until manually removed by administrator/supervisor.	
C-1304	Ability to notify system administrator when flags exceed a customer-defined time period.	
C-1305	Ability to archive deleted hazards and event flags.	
C-1306	Ability to maintain a record of deleted hazards and event flags.	
	Administrative Contact Database	
C-1307	Ability to maintain a searchable list of contact information and telephone numbers related to other city and state departments, utility companies, hospitals, ambulance companies, and other law, fire, and EMS agencies.	
C-1308	Ability for assigned staff with proper security clearance to update contact list on an as needed basis.	
C-1309	Ability to access administrative contact database directly from CAD window.	
C-1310	Ability to access administrative contact database from other than a CAD workstation based on security permission (Mobile, web, handheld, etc.)	
C-1311	Ability to create and maintain an agency-defined centralized database of indexed resource telephone, pager and unit radio assignments accessible by all CAD users (Mobile, handheld, web, etc.).	
C-1312	Ability to access external RMS Personnel modules directly from CAD.	
	CAD Recovery	
C-1313	Ability to retain and display last-known unit and incident status in the event of a catastrophic system failure (e.g., at the workstation, remote external logging device or similar solution).	
C-1314	Ability to reset numbering after CAD system has been restarted.	
C-1315	Ability to retain CAD numbering sequence after system has been restarted.	
C-1316	Ability to add incidents retroactively independent of incident number order or sequential time sequence (i.e., incident 15 may have occurred after incident 20) in the event that the CAD system is unavailable for a time.	
C-1317	Ability to process retroactive incidents and assign incident numbers in the same manner as new incidents; the times associated with the incident can be manually edited to preserve actual timeline.	
C-1318	Ability to recreate a moment in time - snapshots (including map) of what was happening at a given time (e.g., every hour) either electronically or in printed form.	
C-1319	Ability to set aside a block of call for service numbers in the event of a catastrophic CAD failure to enable a manual workflow and tracking.	
C-1320	Ability to indicate in the audit trail that an incident was entered "retroactively".	
	Additional Fire Dispatching Requirements	
	Move-up Management	

C-1321	Ability to identify station coverage deficiencies based on minimum staffing levels by apparatus type.	
	Ability to recommend move-ups based on:	
C-1322	Fixed station order	
C-1323	Current vehicle location (e.g., AVL)	
C-1324	Alarm levels	
	Ability for dispatchers to:	
C-1325	Accept move-up recommendations	
C-1326	Override move-up recommendations	
C-1327	Ability to reverse move-ups as apparatus clear calls.	
C-1328	Ability to distinguish between assigned units and units in move-up or cover status.	
C-1329	Ability to provide an alert when locations are nearing station coverage deficiencies.	
C-1330	Ability for move-up recommendations to take into account units from neighboring jurisdictions (e.g., other cities, mutual aid).	
C-1331	Ability for move-up recommendations to take into account the number of nearby units that are attending the incident and recommend units from farther away (e.g., Pull units from 5 miles away as opposed to 2 miles away to prevent a coverage "black hole")	
	Integrated Dispatching Protocols	
C-1332	Ability to provide integrated questionnaires to assist call takers with logically ordered questions to assess the nature of the emergency.	
C-1333	Ability for the agency to configure the questionnaires to meet local call classification requirements.	
C-1334	Ability to capture the questions and answers as part of the CAD incident record.	
C-1335	Ability to recommend a call type and priority based on the responses to the questionnaire.	

C-1336	Ability to recommend the most appropriate unit based on the responses to the questionnaire.	[redacted]
C-1337	Ability to provide protocols for pre-arrival instructions based on the nature of the emergency.	
C-1338	Ability to integrate with Dispatch protocols (EPD, EMD, EFD).	

Request for Proposals
Mobile - Functional Specifications

Item #	Specification	Vendor Response	Vendor Comments
	General Mobile Data Computing Features		
M-1	Ability to timestamp all field and dispatch transmissions to and from Mobile.		
M-2	Ability for user to select printer for which to print from.		
	Ability to log all mobile activities (e.g., chats, queries, uploads/downloads of field reports) by the following:		
M-3	Agency (i.e., Sheriff, Police Departments, Fire Departments)		
M-4	Date and time of transmission		
M-5	Incident number		
M-6	IP Address		
M-7	Mobile Terminal ID		
M-8	Unit call sign		
M-9	User ID		
M-10	User name		
M-11	Vehicle ID		
M-12	Ability to provide a visual alert if Mobile is receiving negative response from CAD system (no connection to CAD).		
M-13	Ability to continuously attempt to reconnect to CAD system in the event connectivity is lost.		
M-14	Ability to "store and forward" any actions performed while disconnected, upon reconnection. Timestamps of any actions while disconnected are retained and used in CAD (not the reconnection time)		
M-15	Ability to provide screen display formats that are consistent across the application.		
M-16	Ability to configure screen formats based upon agency (e.g., different display screens for FD and PD).		
M-17	Ability to support multiple screen formats on the same Mobile (e.g., allow certain members of FD access to Law functions).		
	Ability for each user to configure the display of their Mobile, including:		
M-18	Font color		
M-19	Font size		
M-20	Window size		
M-21	Window location		
M-22	Day/Night mode		
M-23	Ability to store a user profile for mobile display configuration for auto-configuration upon log-in.		
	Ability to perform the following tasks at any Mobile:		
M-24	Access and display electronic maps		
M-25	Access and display electronic photos		
M-26	Electronic messaging between all Mobiles		
M-27	Electronic messaging between Mobiles and CAD		
M-28	Store files on removable media (CD, thumb drive, etc.)		
M-29	Access any systems interfaced to CAD		
	Mobile Application User Interface		
M-30	Ability for user to toggle among applications on the Mobiles.		

M-31	Ability for all information to be displayed in real time without user intervention.
M-32	Ability for user to toggle among windows.
M-33	Ability for user to minimize or expand any window.
M-34	Ability to support touch-screen functionality.
M-35	Ability to support voice activated (voice command) functionality.
M-36	Ability to support text-to-voice functionality.
M-37	Ability to display all timers created by CAD operator.
M-38	Ability to fully support APS functionality (e.g., voice-to-text, text-to-voice, etc.).
	Ability to accept input from:
M-39	2D barcode reader (driver's license)
M-40	Card swipe device
M-41	Command entries on a command line
M-42	Fingerprint reader
M-43	Function keys (one touch keys)
M-44	Point-and-click devices (i.e., mouse, trackball, touch pad)
M-45	Voice
	Ability to configure a default for the following application settings:
M-46	Audible message
M-47	Audible tones
M-48	Color
M-49	Reverse video (e.g., day/night mode)
M-50	Ability to allow users to return to application default settings.
M-51	Ability for users to select a configuration scheme that accommodates color-blindness.
M-52	Ability for users to select a touch screen configuration that accommodates protective hand gear (e.g., big buttons).
M-53	Ability to support multiple on-screen button configurations (e.g., left side, right side, top or bottom).
M-54	Ability to provide visible differentiation (e.g., color) between active applications.
	Ability to display the following information on the screen during normal operations:
M-55	Availability of wireless connectivity
M-56	Communication verification and other Mobile operational status indicators
M-57	Current unit
M-58	Current unit status (regardless of who assigned the updated status)
M-59	Current system date and time
M-60	Incident number
M-61	Message alert
M-62	Radio talk group (if assigned)
M-63	Screen name/description
M-64	Unit ID
M-65	User ID
M-66	Vehicle location
M-67	Ability to view multiple calls simultaneously (e.g., in different windows).
M-68	Ability to view all incident data on a single window with scroll down capabilities.
M-69	Ability to view all incident data and map in same window (e.g. incident info on left, map on right)
M-70	Ability to open any incident to view dispatch data, units and incident notes.
M-71	Ability to display incident status based on incident priority.
M-72	Ability to display incidents using different colors for different priorities.
M-73	Ability to utilize backwards and forwards buttons to maneuver through screens.
M-74	Ability to set user-defined criteria for how data is displayed (e.g., incident screen, unit screen)

M-75	Ability for all data displayed within columns to be updated in real-time without user intervention (e.g., incidents, unit statuses, etc.)
M-76	Ability to share view screens with other users logged onto the system (e.g., whiteboard/SharePoint type functionality)
M-77	Ability for each unit status to be displayed in a unique color.
	Ability to select other units from the Mobile and show:
M-78	Coordinates
M-79	Location on a map
M-80	Staff assigned
M-81	Agency information
M-82	Incident assignments
M-83	Message log between users
M-84	Ability to have City intranet access embedded in the Mobile client.
M-85	Ability for each user to turn on/off alerts.
	Function Keys/Commands
M-86	Ability to support single keystroke commands.
M-87	Ability to define sub-menus for buttons and function keys so that button and function key commands are based on previous commands.
	Ability for each agency to define keystroke shortcuts for common tasks, including, but not limited to:
M-88	Access to mobile map
M-89	Arrived/unit on-scene
M-90	Arrived/unit at staging location
M-91	Arrived/in area
M-92	At hospital
M-93	At patient
M-94	Clear/available
M-95	Display message
M-96	Display active incidents
M-97	Disposition call
M-98	Emergency
M-99	En route
M-100	In-service
M-101	In-quarters
M-102	Logon/logoff
M-103	Out-of-service
M-104	Retrieve call information
M-105	Retrieve premise information
M-106	Retrieve roster
M-107	Retrieve unit status
M-108	Routine queries (e.g., license plate or name lookup)
M-109	Units assigned to call
M-110	Update unit status
M-111	Ability to pull up a "call disposition" mask.
M-112	Ability to provide a drop down menu for call dispositions.
M-113	Ability for each agency to define call dispositions.
M-114	Ability to reject a disposition if unsuitable for the incident type.
M-115	Ability to provide a text field for disposition comments.
M-116	Ability to clear all units from a call upon the entry of a disposition from the Mobile.
M-117	Ability to require a confirmation prior to clearing all units from a call from the Mobile.

[redacted]

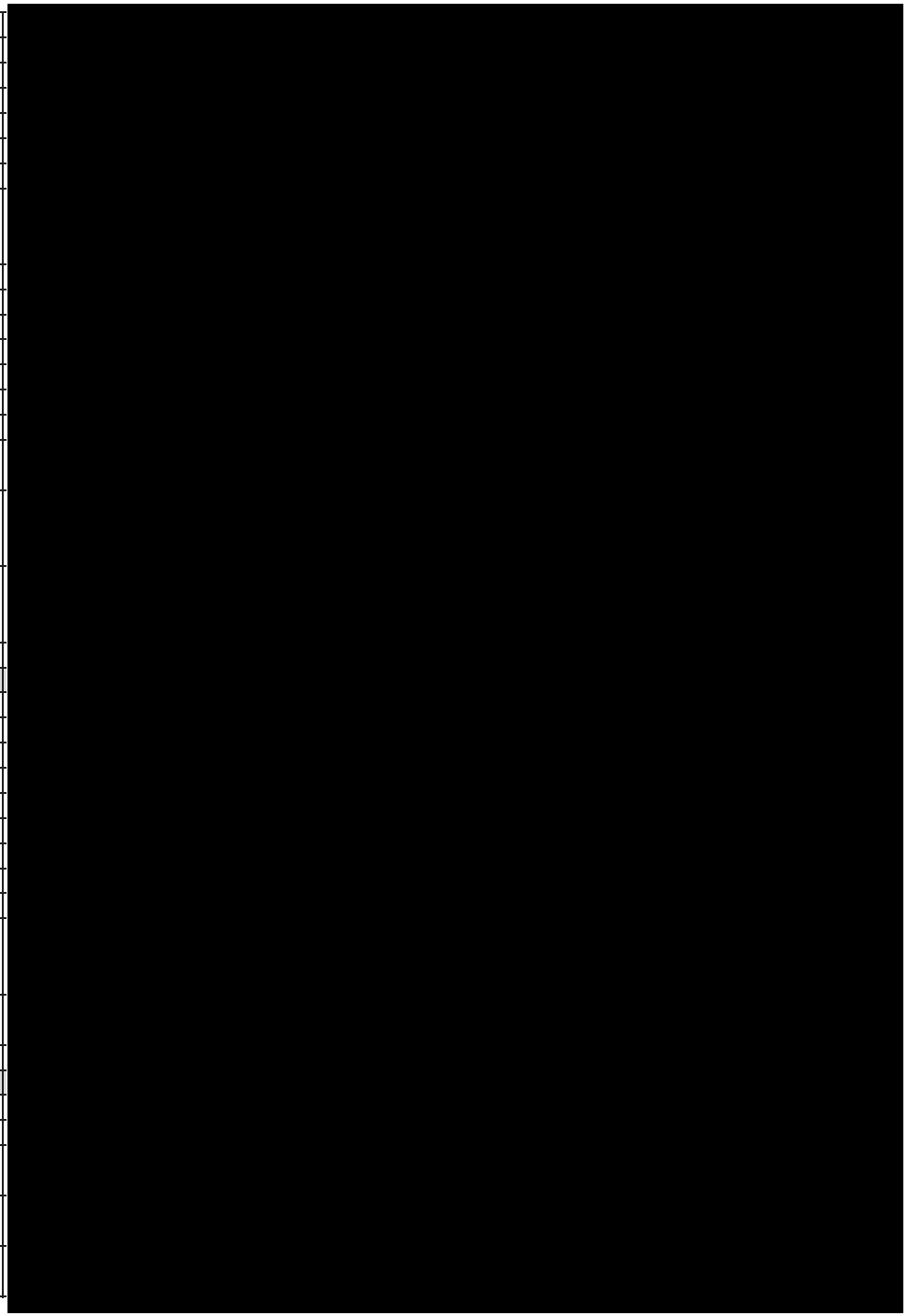
M-118	Ability to require a Mobile user to enter a disposition prior to clearing the last unit from the Mobile.
M-119	Ability for each agency to have their own unique disposition codes and not be presented with disposition codes used by other agencies (e.g., FD only sees Fire disposition codes).
M-120	Ability to configure a Mobile button (tool bar or function key) to launch any third-party program (e.g., Adobe, Word, etc.).
	Security
M-121	Ability to require both user identification and password.
M-122	Ability to require two-factor authentication
M-123	Ability for agency to set the time a Mobile can remain inactive before automatically logging out the user.
M-124	Ability for agency to set the time a Mobile can remain inactive before automatically locking out the user.
M-125	Ability to print a log of all transactions for a Mobile computer.
M-126	Ability for client to remain logged in (to CAD), despite software shut-downs or computer re-boot.
	Systems Integration
	CAD/Mobile Integration
M-127	Ability to log onto the CAD system from the Mobile.
M-128	Ability to view all incident information available in CAD on the Mobile.
M-129	Ability to view all location information available in CAD on the Mobile.
M-130	Ability to confirm the receipt of status updates from the Mobile.
M-131	Ability to run multiple applications (e.g., mobile, automated field reporting) on the Mobile at the same time, with CAD operations having precedence over reporting operations.
M-132	Ability to receive dispatch alerts and/or indicators without losing current work.
M-133	Ability to acknowledge dispatch without losing current work.
M-134	Ability to bring dispatch to forefront without losing current work.
M-135	Ability to configure audible alert tone for dispatch notification.
M-136	Ability to receive and acknowledge a dispatch notification without losing any data from other applications.
M-137	Ability to query employee database of contact information.
M-138	Ability to query any database within the CAD application from the Mobile.
M-139	Ability to query any system interfaced to the CAD application.
	Police RMS/Mobile Integration
M-140	Ability to have a direct link to RMS queries, and pull name and vehicle queries directly from the name and vehicle form without an additional login or retyping the words.
M-141	Ability to run queries from the Mobile into the Police RMS.
M-142	Ability to message between CAD/Mobile stations and users on the Police RMS.
M-143	Ability to automatically query the Police RMS upon dispatch to a location.
M-144	Ability for Police to access Fire RMS information (e.g., pre-plans) from the Mobile.
M-145	Ability for alerts created in CAD or RMS to be made available to users in the Mobile environment.
M-146	Ability to link log-on information with Personnel data in the Police RMS (e.g., User ID identifies special skills associated with user)

[redacted]

	Fire RMS/Mobile Integration
M-147	Ability to run queries from the Mobile into the Fire RMS.
M-148	Ability to message between CAD/Mobile stations and users on the Fire RMS.
M-149	Ability to automatically query the Fire RMS upon dispatch to a location (e.g., pre-plans, hazardous information made available to user).
M-150	Ability to utilize any Fire RMS data in Mobile (inspections, hydrants, staffing, schedules, etc.)
M-151	Ability to link log-on information with Personnel data in the Fire RMS.
M-152	Ability for alerts created in CAD or Fire RMS to be made available to users in the Mobile environment.
	Logon/Logoff
	Ability to require any agency-determined combination of the following information to logon to CAD/Mobile system:
M-153	Biometrically obtained information (two-factor authentication)
M-154	Equipment (equipment serial numbers, equipment descriptions, etc.)
M-155	Identification card
M-156	License plate number
M-157	Partner ID(s)
M-158	Password
M-159	Personnel/badge number
M-160	Radio ID(s)
M-161	Position ID(s) (e.g., driver)
M-162	Unit ID
M-163	User ID
M-164	User name(s)
M-165	Vehicle ID
M-166	Status (e.g., in service, out-of service, etc.)
M-167	Agency-defined
M-168	Ability to save data entered into user logon fields that remains the same from session to session (e.g., all information other than password).
M-169	Ability for each agency to define mandatory logon fields.

M-170	Ability to allow agency to define mandatory logon fields for users not logging on to CAD through a Mobile.	
	Ability to logoff with the following information:	
M-171	Mileage	
M-172	Unit ID	
M-173	Miscellaneous comments	
M-174	Ability to support a single password sign-on to CAD, the Mobile and the operating system.	
M-175	Ability to automatically provide notification following a Mobile-defined number of unsuccessful logon attempts.	
	Ability to automatically notify the following of Mobile logon and logoffs (e.g., name, ID, etc.):	
M-176	Dispatchers	
M-177	Field supervisors	
M-178	Ability to logon multiple individuals per unit. (up to 6 for fire)	
M-179	Ability to assign an individual to a unit at any time from within the mobile application.	
M-180	Ability to remove an individual from a unit at any time from within the mobile application.	
M-181	Ability, when there are multiple users logged onto one Mobile to allow one user to logoff the system while allowing another to remain logged on.	
M-182	Ability for a resource to be logged on but not available for service.	
M-183	Ability for a unit logged on to automatically default to a defined status (Available, In Quarters, Out of Service, etc.).	
M-184	Ability to assign a log-on status at login.	
M-185	Ability to logoff personnel without logging off the associated apparatus (e.g., firefighters changing shift).	
M-186	Ability to logoff a Mobile and remain logged into CAD system.	
	Ability for a user to logoff the system and save information on the Mobile including:	
M-187	In-progress reports	
M-188	Messages	
M-189	Notes	
M-190	Query returns	
	Ability to store the following until manually deleted by the user:	
M-191	In-progress reports	
M-192	Messages	
M-193	Notes	
M-194	Query returns	
M-195	Ability to support a user-initiated download of software/files at logon without interfering with operational performance.	
M-196	Ability to support an automatic download of software/files at logon without interfering with operational performance.	
M-197	Ability to separate Mobile logoff from designating status as off-shift.	
M-198	Ability to separate Mobile logon from designating status as on-shift.	
M-199	Ability to provide a confirmation window upon a user attempting to log out of the Mobile application.	
	Mobile Mapping	
M-200	Ability to support AVL functionality.	
	Ability to support AVL Data using, but not limited to the below protocols and integrations:	
M-201	NMEA AVL Data Protocol.	

M-202	TAIP AVL Data Protocol.
M-203	Windows Location Services.
M-204	TCP
M-205	UDP
M-206	Bluetooth
M-207	USB
M-208	Ability to cache map layers to minimize the amount of data transmitted wirelessly.
M-209	Ability to utilize Google map data for display.
M-210	Ability to update unit and incident locations on map without resetting the entire map.
M-211	Ability to update map wirelessly.
M-212	Ability for map to function in the background and not supersede other applications.
M-213	Ability to zoom in/out to fixed extents.
M-214	Ability to pan by swiping across touchscreen.
M-215	Ability to display map legend.
M-216	Ability to display compass direction between two user selected points.
M-217	Ability to graphically display street network for a desired coverage area.
M-218	Ability to select map layers for display.
M-219	Ability to create an agency-defined boundary layer (e.g., beat, fire zone box)
M-220	Ability to automatically refresh current vehicle location at agency-defined intervals.
	Ability to center map display on:
M-221	Current vehicle location (with AVL)
M-222	Midpoint between vehicle location and dispatch location
M-223	Dispatch location
M-224	Location of cursor when mouse button is clicked
M-225	Vehicle activating emergency activation key
M-226	Specified geographic area (e.g., entering an address via text entry)
M-227	Other user logged on
M-228	Incident location
M-229	Ability to display location at cursor when mouse button is clicked.
M-230	Ability for user to access apartment complex maps upon clicking on the location for a complex (assuming user-created map layer containing site maps).
M-231	Ability to add and/or delete bookmarks.
M-232	Ability to center the map on a verified location and mark the location with a unique icon.
	Ability to select and view X/Y (lat/long) coordinates:
M-233	Current location
M-234	Selected location on a map
M-235	Ability to display other field units in the same agency on mobile map (assuming AVL and sufficient bandwidth).
M-236	Ability to display other field units in other agencies, by user selection, on mobile map (assuming AVL and sufficient bandwidth).
M-237	Ability to display other field units responding on the same assigned incident (regardless of Agency) on mobile map (assuming AVL and sufficient bandwidth).

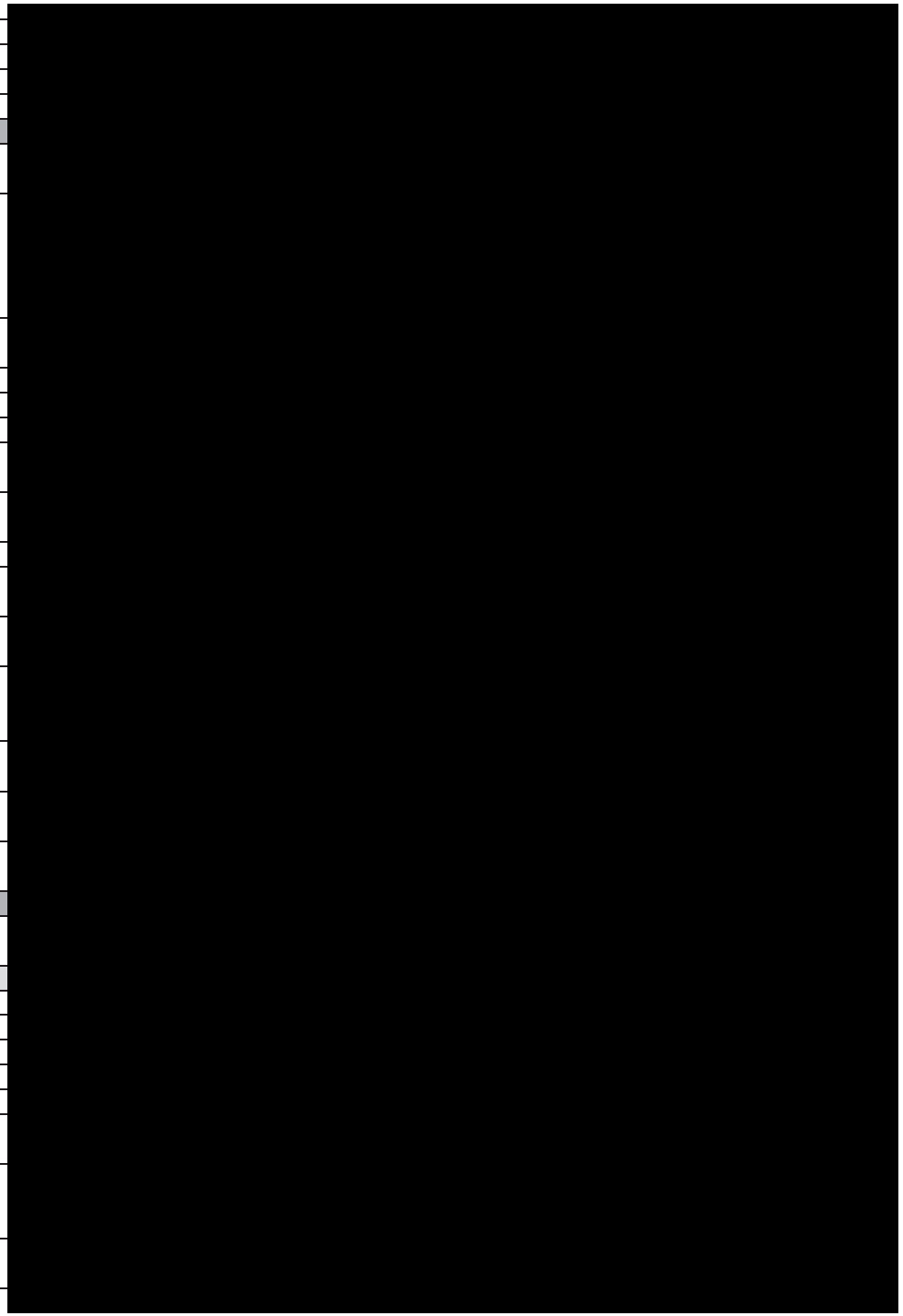


M-238	Ability to make temporary "marks" on map (e.g., to note locations of a perimeter or the locations of apparatus at a large scene).
M-239	Ability to display active incidents and unit statuses on the map.
M-240	Ability to filter the display of active incident and unit status based on map scale.
M-241	Ability to enter an address and display map along with indicators of additional information available in the system.
M-242	Ability to display user-specified map layers (e.g., hydrants, hazards) surrounding an incident location.
M-243	Ability to provide closest cross streets.
M-244	Ability to automatically generate a perimeter upon entry of a location and perimeter distance (e.g., set a 3 block perimeter around 300 Main St.).
M-245	Ability to receive suggested perimeter positions from dispatch.
M-246	Ability for suggested perimeter positions to automatically appear on a map upon receipt.
M-247	Ability for map to function without wireless connectivity.
M-248	Ability to click on a unit or incident in the incident queue or unit status bar and have it displayed on the map.
M-249	Ability to calculate distance between two points on the map.
M-250	Ability to embed or attach users map as an image in message.
M-251	Ability to support orthophoto (aerial photographs) data layers.
M-252	Ability to support integration with Pictometry (side angle photograph of buildings) data layers.
M-253	Ability for system administrator to set layer tolerances to enable/restrict data displayed based on zoom level and criteria within the layer data.
M-254	Ability for user to override layer tolerances to display layers that are hidden based on zoom tolerances.
M-255	Ability to map layers using multiple datasets (unserved arrest warrants, premise history files, etc.).
M-256	Ability to display units that have Mobile computers but are not logged into CAD.
	Mapping Configurability
M-257	Ability for the system administrator to assign mobile icon shapes.
M-258	Ability for mapping client to load automatically upon system boot.
M-259	Ability for the system administrator to assign incident icon shapes and colors, based on status.
	Ability to filter display by:
M-260	Unit type
M-261	Unit status
M-262	Incident type
M-263	Incident priority
M-264	Vehicle type (e.g., Fire apparatus only)
M-265	Radio devices
M-266	Incident number
M-267	Response area
M-268	Sector
M-269	Fire zone box
M-270	Active incidents
M-271	Subsets of pending or active incidents (e.g., only fire)
M-272	Ability to present user with a list of available layers that can easily be modified (e.g., checkbox of layers) and turned on/off.

M-273	Ability for users to create custom maps.
M-274	Ability to share custom maps with other users
M-275	Ability to create user-defined map distribution groups.
	Ability to share custom maps by the following methods:
M-276	All users assigned to an incident
M-277	Individual users
M-278	Ability to draw custom objects on a map.
	Routing
M-279	Ability to automatically calculate directions from user's current location (on Mobile using AVL) to dispatched location.
M-280	Ability to support quickest-time routing for all dispatches.
M-281	Ability to suggest multiple routes if other routes are within an agency-defined time period (e.g., suggest multiple routes if within .5 minutes)
M-282	Ability to recalculate directions to incident/specified location on the fly.
M-283	Ability to display shortest route from point-A to point-B (i.e., street network routing), and highlight quickest route, including directions based upon roadway/access availability (e.g., construction, detours).
M-284	Ability to provide audible routing information.
M-285	Ability to provide text based routing information.
	Ability to take into account the following when calculating routing directions:
M-286	Street speed limits
M-287	Weather
M-288	Closed streets
M-289	Dispatch entered obstacles
M-290	Mobile user entered obstacles
M-291	Apparatus-/unit-specific limitations (large fire apparatus vs motorcycle)
M-292	Distance between vehicle and incident location
M-293	Ability to highlight on the map the recommended route from current location to a dispatched incident site.
M-294	Ability for Mobile user to turn recommended route ability on/off.
M-295	Ability to clearly display potential obstacles along route.
M-296	Ability to provide estimated travel time.
M-297	Ability to record all routing displays within CAD (e.g., map displays, travel time, travel time estimation, etc.) for analysis to improve routing alogarithms.
	Vehicle Pursuit
	Ability to enter into "Pursuit Mode" which automatically performs the following functions:
M-298	Pre-empts user from all other calls
M-299	Increases rate of AVL updates (e.g., updates every 2 seconds as opposed to standard)
M-300	Automatically notifies other Mobile users.

[redacted]

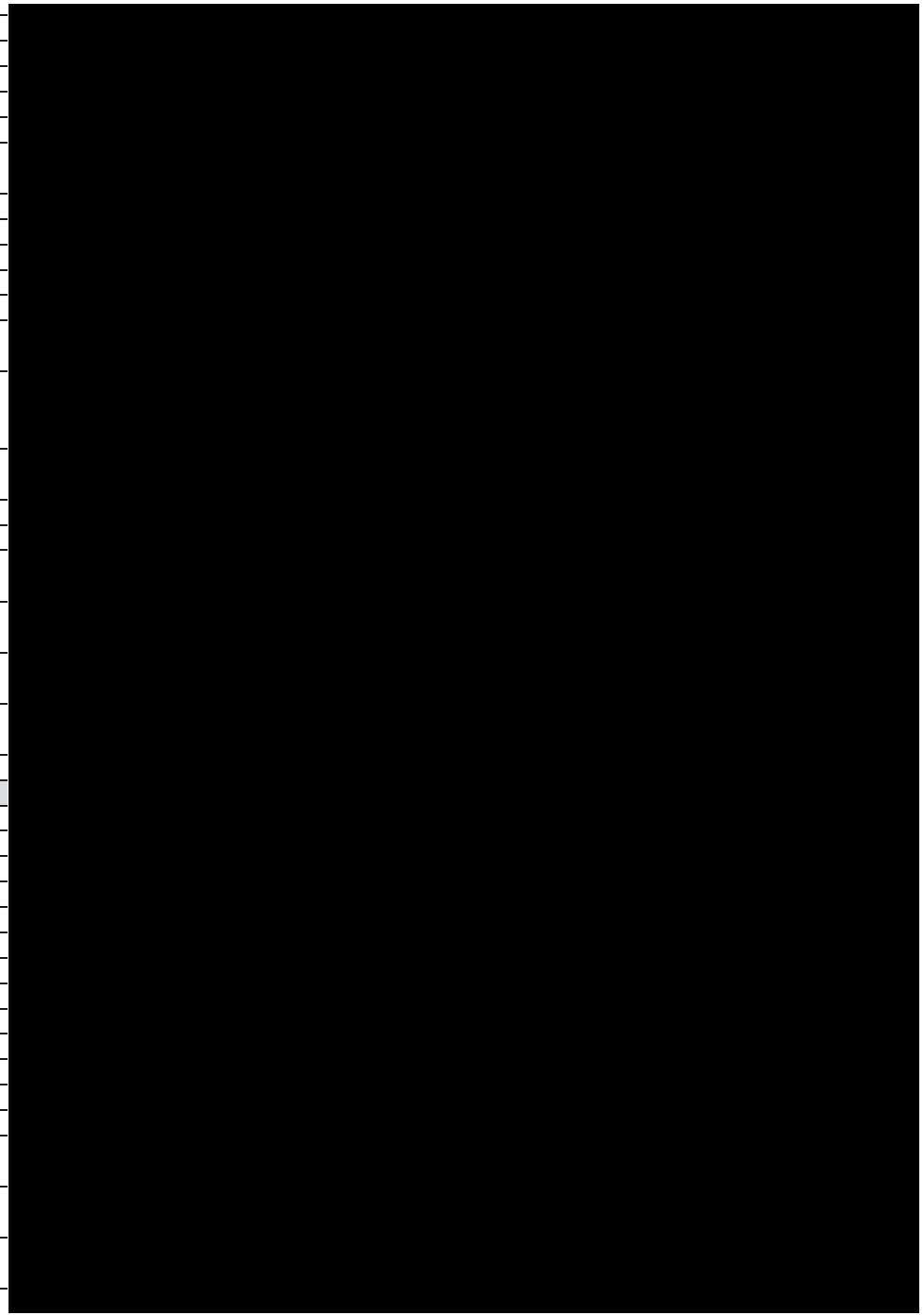
M-301	Centers map on vehicle
M-302	Changes color, size or type of map icon
M-303	Prevents overlay of agency-defined screen updates and alerts
M-304	Ability to display a "bread crumb" trail of vehicle when in pursuit.
	AVL Integration
M-305	Ability to view other unit locations and last known locations (and time stamp) in real time.
M-306	Ability to integrate GPS (radio or mobile phone) into mapping client.
M-307	Ability to accept AVL/GPS data from multiple sources for a unit/user (Vehicle Laptop, handheld radio, smartphone, GPS tag, etc.) in mobile as well as CAD.
M-308	Ability for agencies to define who is able to view unit locations.
M-309	Ability to display vehicle location on a map and view progress toward incident location.
M-310	Ability to display direction of travel of units.
M-311	Ability to automatically rotate map so that unit is automatically displayed moving the same direction.
M-312	Ability to receive automatic alerts for agency-defined criteria (e.g., hazards, outstanding warrant, sex offender) based on proximity of unit to coordinate.
M-313	Ability for user to turn off and on the automatic alerts based on location.
M-314	Ability to provide a unique alert field units when other field units are in a agency-defined radius (e.g., to avoid collisions at intersections).
M-315	Ability to update map display based on AVL location such that as vehicle moves closer to a destination location the map zooms in to provide more detail.
M-316	Ability for system to automatically recognize a unit location and update status appropriately and logically (En Route to On Scene, In Quarters to Available, Available to In Quarters, etc.).
M-317	Ability for system administrator to turn on/off AVL functionality for individual units (e.g., undercover units)
M-318	Ability for certain mobile users to turn on/off AVL functionality (Supervisors).
M-319	Ability for users to input unit location (e.g., zone box number, beat, etc.) in the event AVL is unavailable.
	Emergency Key Functionality
M-320	Ability to initiate an emergency message transmission from a touch screen button or hot key.
	Ability to automatically transmit the following information in an emergency situation:
M-321	Last known location
M-322	Current location (with AVL)
M-323	Reference to incident
M-324	User ID
M-325	User name
M-326	Ability to configure emergency key to capture agency-defined combination of above information.
M-327	Ability to link emergency key function in mobile to a portable radio emergency activation.
M-328	Ability to send to all Mobile and CAD users (except the sender) an emergency notification with unit ID and location (if known) when the emergency key is activated.



M-329	Ability to prevent emergency notification from appearing on the sender's screen.
M-330	Ability for the Mobile screen to revert to its prior view after the user dismisses an emergency message.
M-331	Ability to send location coordinates upon triggering an emergency key.
	Ability for system administrator to turn off emergency key functionality by:
M-332	Device
M-333	User
	Mobile Dispatch Operations
M-334	Ability to receive dispatches on the Mobile.
M-335	Ability for dispatches to open automatically on mobile computers.
M-336	Ability to provide identical functionality as within a Mobile as a handheld device (e.g., smart phone, etc.)
	Ability to alert mobile users that a new dispatch has arrived using:
M-337	Audible alert
M-338	Visual alert
	Ability to provide a distinguishable alert for high priority calls (as defined by each agency):
M-339	Audible
M-340	Visible
M-341	Ability for all personnel dispatched to an incident to receive notification when other personnel are en route.
M-342	Ability for Mobile users to add themselves to an incident.
M-343	Ability for all personnel dispatched to an incident to received notification of status and location changes of other personnel dispatched to the call.
M-344	Ability for a supervisor to automatically receive Mobile activity reports (e.g., supervisors receive carbon copies of all user activity)
M-345	Ability for authorized personnel to create user-defined groups or lists for which they will be copied on all activity.
M-346	Ability to access and read all call comments associated with a call regardless of whether assigned to the call.
	Ability to display the following information in distinct fields or tabs (as opposed to in the call narrative) upon receipt of dispatch:
M-347	Agency Case Number
M-348	Assisting unit(s)
M-349	Comments/narrative (unlimited)
M-350	Date and time incident entered
M-351	Driver registration information
M-352	HAZMAT code and instructions
M-353	HAZMAT status
M-354	Incident location with cross streets
M-355	Incident priority
M-356	Incident type
M-357	Number of previous calls at a location.
M-358	Pre-plan information
M-359	Reporting party address
M-360	Reporting party name
M-361	Reporting party phone
	Additional information:
M-362	Name

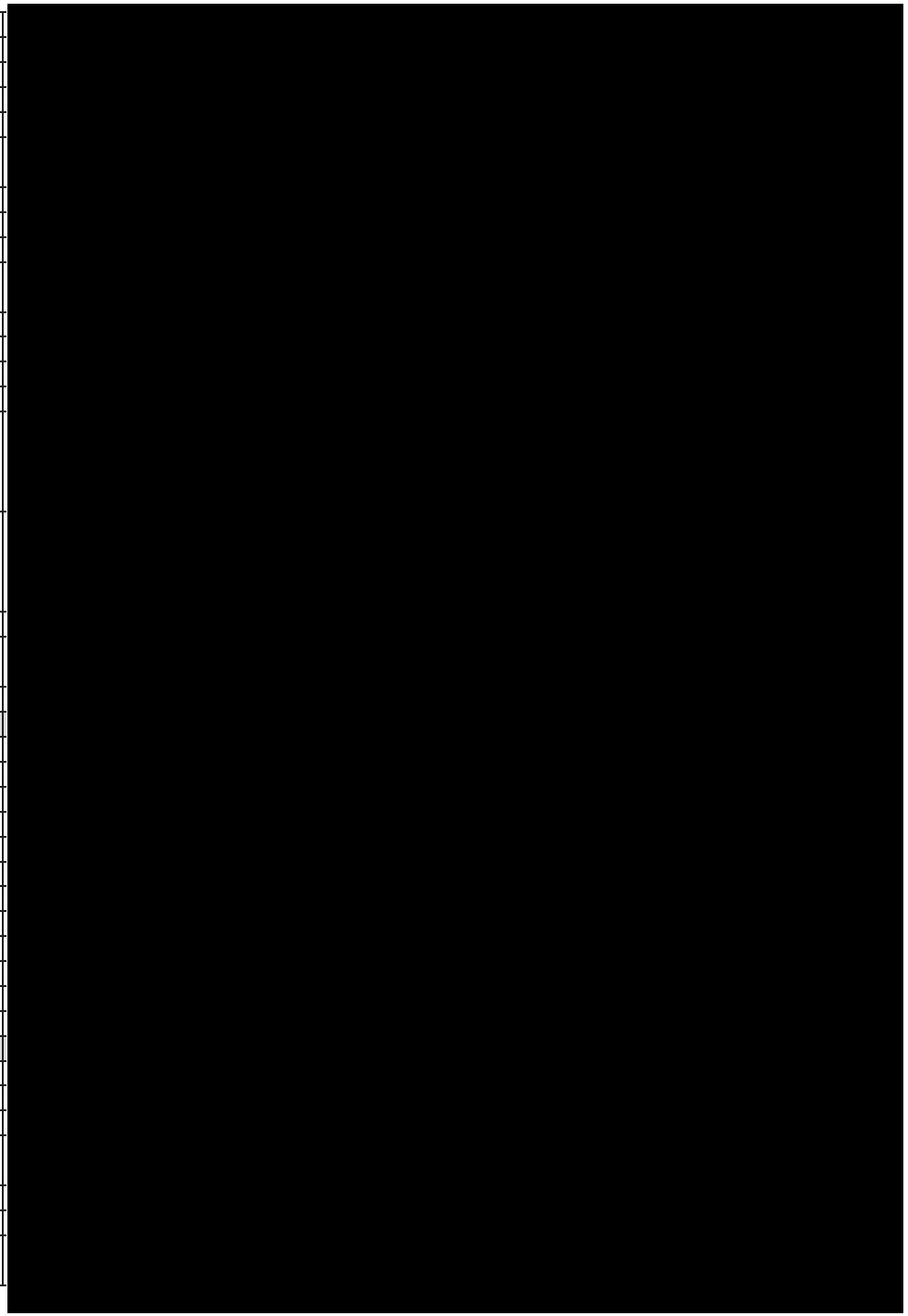
[redacted]

M-363	Description
M-364	Location
M-365	Phone number at incident location (if different)
M-366	Premise and prior information flag
M-367	Premise history information
M-368	Recommended route
M-369	System generated incident number
M-370	Weapons involved
M-371	Agency-defined data
M-372	Ability to display most current incident data at the top of the screen.
M-373	Ability to double click on an incident and retrieve additional information.
M-374	Ability for user to filter information displayed on incident screen (e.g., to allow most important information top priority).
M-375	Ability to have different types of information on different screens (e.g., tabs - one for current incident, one for related premise history, etc.) such that users can easily filter or access information.
M-376	Ability to limit access to incident information if there is sensitive information (e.g., police information only).
M-377	Ability to alert user that premise history or hazards are associated with a location.
M-378	Ability to alert user that pre-plan information is available when deployed to a location.
M-379	Ability to create hyperlinks within the application to search for additional information on agency-defined data fields.
M-380	Ability to pull up a previous call in a premise history file and show any hazards that were valid at the time of the call.
M-381	Ability to provide periodic (agency-defined) alerts to user of available premise history or hazards until the user has opened the file containing the information.
M-382	Ability to time and date stamp when the user has opened the file containing premise history or hazard information.
M-383	Ability to indicate to dispatcher that mobile device has received the dispatch message.
	Ability to update unit status including, but not limited to:
M-384	Available
M-385	Busy
M-386	Clear
M-387	Delayed response
M-388	In training
M-389	On-scene
M-390	Out-of-service
M-391	Responding
M-392	Staging
M-393	In area
M-394	At patient
M-395	Fire Extinguished
M-396	Agency-defined
M-397	Ability to prompt user for an expected time delay upon entry of delayed response unit status.
M-398	Ability to receive supplemental incident information (e.g., location, suspect, vehicle information, etc.) without interrupting or overlaying current screen.
M-399	Ability to indicate type of premise information that is attached to a call (e.g., gate code, hazard, etc.) so that user can decide whether or not to retrieve the information.

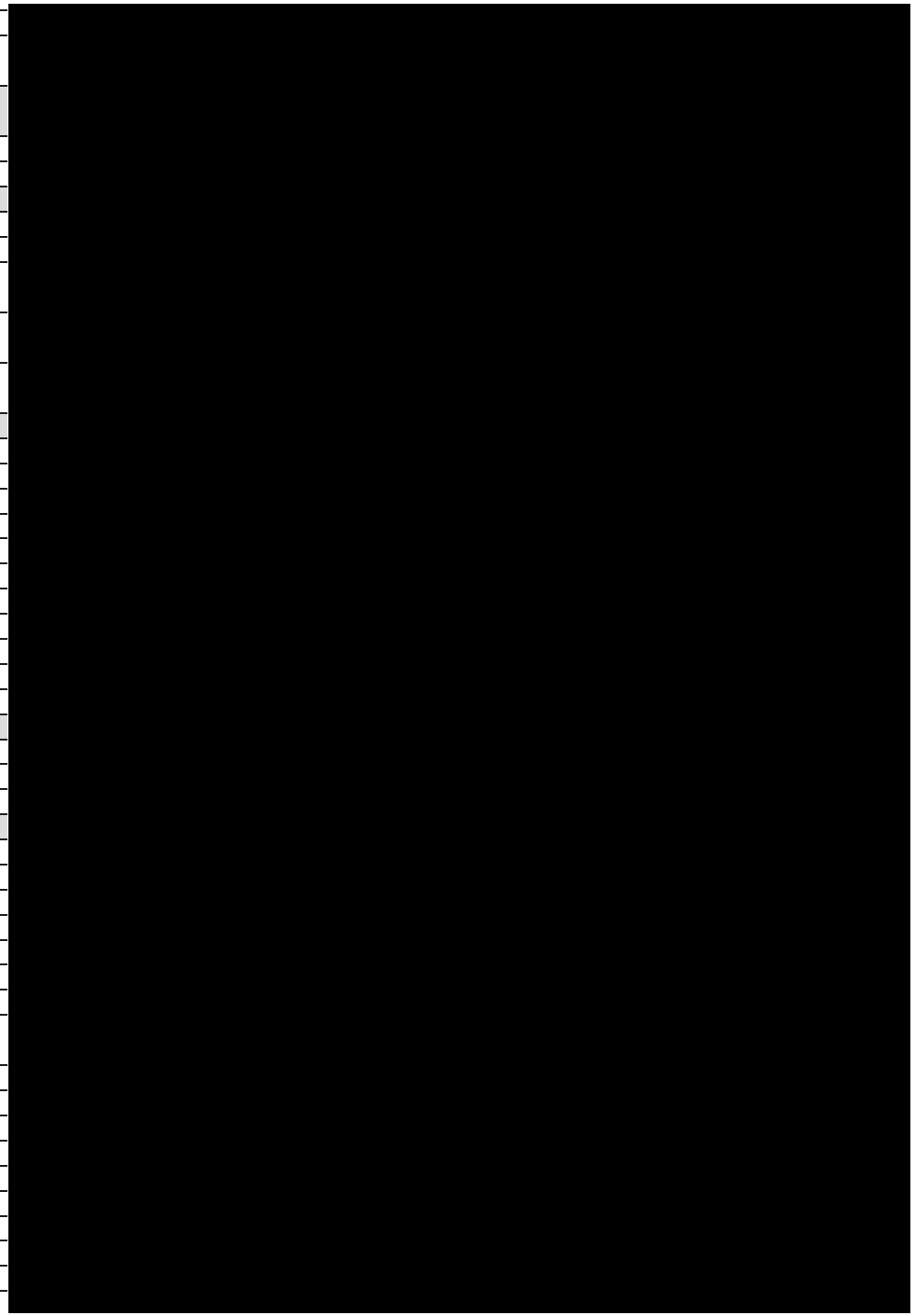


M-400	Ability for field units to have the option of displaying premise information attached to the call.	
M-401	Ability to identify categories of premise information that must be viewed prior to call being closed.	
M-402	Ability to record the viewing of premise information in the audit trail.	
	Ability to alert user that supplemental incident information is available for viewing via:	
M-403	Audible alert	
M-404	Visual alert	
M-405	Ability for supplemental information to be visually distinct from information previously received by Mobile user (e.g., separate font color, highlighted, etc.)	
M-406	Ability for mobile screen to update automatically as new information is added to a call (e.g., without user intervention).	
M-407	Ability to configure application such that user intervention is required to refresh a mobile screen to display new information.	
M-408	Ability to transmit status information to the CAD system in real time.	
M-409	Ability to retrieve previous incidents at incident location.	
M-410	Ability to clear calls from the Mobile.	
M-411	Ability to require a call clearance code in order to clear a call from the Mobile.	
M-412	Ability for all agencies to see incident information sent to other agencies dispatched to the same incident.	
M-413	Ability for law enforcement personnel to view related Fire/EMS calls (e.g., if dispatched to a Fire/EMS call).	
M-414	Ability for Fire/EMS personnel to view related law enforcement calls (e.g., if dispatched to a law enforcement call).	
	Field-Initiated Incident	
	Ability to initiate a call for service from the Mobile, including:	
M-415	Call for service	
M-416	Traffic stop	
M-417	Subject stop	
M-418	Administrative activity (e.g. training, field inspections, etc.)	
M-419	Ability to initiate a call for service with a function-key.	
M-420	Ability, with appropriate supporting mapping/AVL technology, to indicate unit/incident location when initiating an incident from the field.	
M-421	Ability to validate self-initiated call for service location at the dispatch level.	
	Queries	
M-422	Ability to query and view pending calls.	
M-423	Ability to query and view active calls.	
	Ability to query and view unit status by:	
M-424	Area command	
M-425	Beat	
M-426	Battalion	
M-427	City	
M-428	Sector	
M-429	Fire zone box	
M-430	Individual unit/apparatus	
M-431	Squad/company	
M-432	Staff assigned to unit	
M-433	Ability to query and retrieve premise information for an address not associated with a call for service.	
	Ability to query the following systems from the mobile computer:	
M-434	CAD	

M-435	Police RMS (with permission)
M-436	Fire RMS (with permission)
M-437	NLETS (including the ability to view images)
M-438	NCIC
M-439	State Law Enforcement Telecommunications Systems/Criminal Justice Information
M-440	Any databases interfaced to CAD
M-441	Ability to search and query all appropriate databases with one query request.
M-442	Ability to provide check boxes for users to indicate which databases to query.
M-443	Ability to set agency-defined defaults for databases to query.
M-444	Ability to search and query all appropriate databases without impacting dispatching performance.
M-445	Ability to attach any database query return to incident records.
M-446	Ability to cut and paste any database query return into incident records.
M-447	Ability to consolidate query returns when multiple databases are searched.
M-448	Ability to indicate source of information in consolidated query returns.
M-449	Ability to query a location to obtain contact (e.g., responsible party) information.
M-450	Ability to query a location to access pre-plans.
M-451	Ability to initiate queries with a single key stroke.
M-452	Ability to use predefined data entry forms/screens (masks) to minimize data transmitted during queries.
M-453	Ability for agency to create standard query screen formats (masks).
	Ability to provide pre-defined data entry/query forms, including, but not limited to:
M-454	Articles
M-455	Accident Investigation
M-456	Driver license query
M-457	Incident status
M-458	Location
M-459	License plate query
M-460	Logon/logoff
M-461	Missing person information
M-462	Name query
M-463	Premise information query
M-464	Previous events
M-465	Vehicles
	Ability to access query forms by:
M-466	Command line entry
M-467	Dedicated function keys
M-468	Drop down menus
M-469	Ability for authorized users to enter vehicle stops on the command line or entry form and automatically run the license plate against all available relevant databases.
M-470	Ability for authorized users to conduct multiple license plate searches simultaneously.
M-471	Ability to save all previous license plate searches until user clears data.
M-472	Ability for authorized users to automatically run the registered owner of the vehicle in a license plate query return.

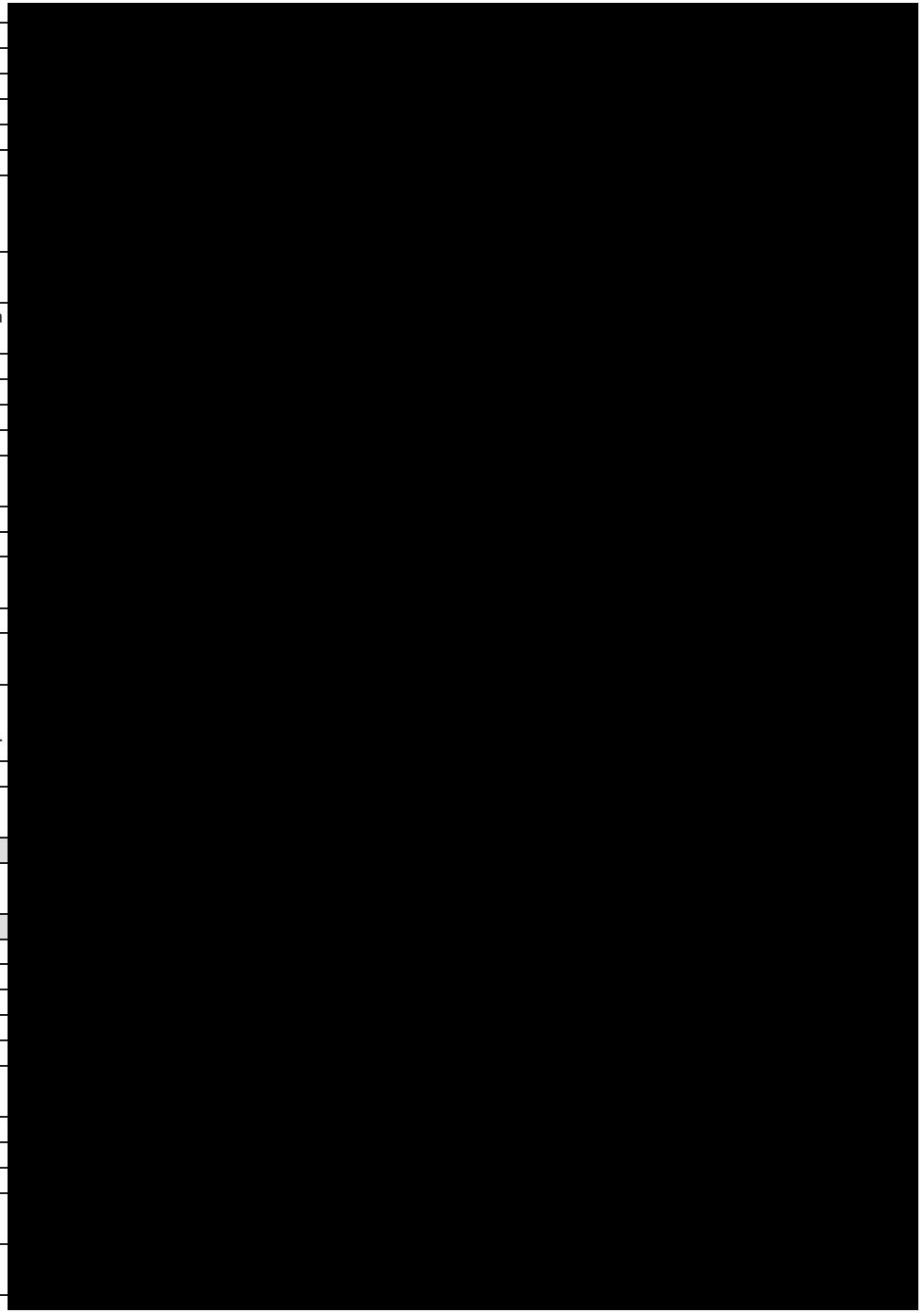


M-473	Ability to save all query returns until user clears data.
M-474	Ability to save all stored query returns after logoff (e.g., returns are still there the next time user logs onto the system).
	Ability to produce an alert when a query return contains a record marked as potentially hazardous:
M-475	Audible alert
M-476	Visual alert
	Ability to produce an alert when a record returns a record containing a stolen vehicle:
M-477	Audible alert
M-478	Visual alert
M-479	Ability for mobile query returns to appear on dispatcher's screen as well as the mobile computer screen.
M-480	Ability to drill down into query returns regarding a potentially hazardous subject, vehicle, and/or location to find the details of that hazard.
M-481	Ability to differentiate between call data and query results (e.g., color, font, screen location).
	Ability to query unit status by:
M-482	Resource
M-483	Comments
M-484	Date and time range
M-485	Dispatch group
M-486	Elapsed time in current status
M-487	Geographic area (e.g., area, beat, sector, etc.)
M-488	Incident type
M-489	Location
M-490	Unit ID
M-491	Personnel ID
M-492	Unit status
	Ability to query unit history detail by:
M-493	Date and time range (i.e., start and end dates or times)
M-494	Personnel ID
M-495	Unit ID
	Ability to query and retrieve incident records by:
M-496	Any operator ID associated with the incident
M-497	Any unit ID assigned to the incident
M-498	Case number
M-499	Cross streets
M-500	Date and time range (e.g., start and end data and time parameters)
M-501	Unit ID
M-502	Personnel ID
M-503	Geographic area (e.g., area, beat, sector, etc.)
M-504	Incident number
M-505	Incident priority
M-506	Incident type
M-507	License plate
M-508	Location or partial location
M-509	Name (suspect, reporting party, witness, victim)
M-510	Census tract
M-511	Reporting district
M-512	Ability to sort query results on any returned field.



	Messaging		
	General Messaging Features	[redacted]	
M-513	Ability to send messages to a user who is not logged into CAD and cache that message for retrieval when the user logs onto CAD.		
M-514	Ability for message server to continuously attempt to deliver a message until received and confirmed.		
M-515	Ability for user to retrieve cached messages upon logon.		
M-516	Ability to send broadcast messages.		
M-517	Ability to support real-time instant messaging.		
	Ability to display the following identifiers within a message:		
M-518	Sender name		
M-519	Sender date		
M-520	Sender time		
M-521	Sender workstation ID		
M-522	Sender unit ID		
M-523	Receiver name		
M-524	Receiver date		
M-525	Receiver time		
M-526	Receiver workstation ID		
M-527	Receiver unit ID		
M-528	Ability to assign and change a priority to a message (e.g., routine, urgent, emergency).		
M-529	Ability for system administrator to define message precedence.		
M-530	Ability for system administrator to set forced display based on message type.		
M-531	Ability for each terminal to have a unique identifier included in each transmission to the host.		
M-532	Ability to provide a web-based version of messaging capabilities.		
M-533	Ability for web version of messaging to be accessed with agency-defined security procedures.		
M-534	Ability to automatically integrate dispatch-related messages to an incident.		
M-535	Ability to store messages for later viewing.		
M-536	Ability for host computer to store unread messages when user logs off.		
M-537	Ability for messages to be sorted by most recent or first received.		
	Sending Messages		
M-538	Ability to create easily accessible agency-defined message forms for specific message types.		
M-539	Ability to create and save agency-defined message groups.		
M-540	Ability to create and save user-defined message groups.		
M-541	Ability to send messages across agencies (e.g., police to fire and vice versa).		
M-542	Ability to recall or cancel a sent message.		
M-543	Ability of users to select any number of people as part of a message group with no limitation on the number of people in a group.		
M-544	Ability to enter unlimited narrative with wrap-around feature [if characters are limited, indicate the maximum in the "comments" section].		
	Ability to send a message to the following:		
M-545	Battalion		
M-546	District		
M-547	Group of user IDs		
M-548	Group of workstations names		
M-549	Units associated with an incident number		
M-550	Units within a user-defined location (based on selected radius on map)		
M-551	Logged on units		

M-552	Mobile Data Device ID/Name
M-553	Position IDs (e.g., dispatcher)
M-554	Sector
M-555	Unit ID
M-556	User ID
M-557	User name
M-558	Workstation ID or name
M-559	Ability to automatically populate the "To" field on the message mask when selecting recipients.
M-560	Ability to select a recipient by a single command to create a message (e.g., double click on a logged on user and message screen pops up)
M-561	Ability to add to a message before forwarding to another user.
M-562	Ability to attach files to messages.
M-563	Ability to embed images in messages.
M-564	Ability to set agency-defined file size limit.
M-565	Ability to automatically compress and resize images to comply with agency-defined file size limits.
M-566	Ability to send a message to all units handling a specific incident.
M-567	Ability to send information displayed on screen to another workstation.
M-568	Ability to transmit a reply message to the originator of a currently displayed message without having to reenter the originator's address.
M-569	Ability to "reply all" to message recipients.
M-570	Ability to create messages that are retained in the system and sent at pre-specified times.
M-571	Ability to provide a notification for non-delivery of messages (i.e., a message sent to a device or group of devices could not be delivered if a user is not signed-on to the device(s)).
M-572	Ability to provide a notification of delivery of messages.
M-573	Ability to send messages to Mobile regardless of log on.
	Receiving Messages
M-574	Ability to notify receiver via an audible and/or visual flag that a new message has arrived in mailbox.
	Ability to provide a visual distinction between the following:
M-575	External messages
M-576	General messages
M-577	System messages
M-578	Query returns
M-579	Ability to provide a visual distinction between general messages and query returns.
M-580	Ability to segregate query returns from general messages (e.g., separate folders or windows).
M-581	Ability to prevent incoming messages from interfering with current work.
M-582	Ability to notify receiver of total number of unread messages.
M-583	Ability for each message to be displayed in a separate window.
M-584	Ability for messages to be queued in an "inbox" for later viewing at the convenience of users.
M-585	Ability to identify high priority messages by type of priority (e.g., felony warrant return versus user-defined urgency).

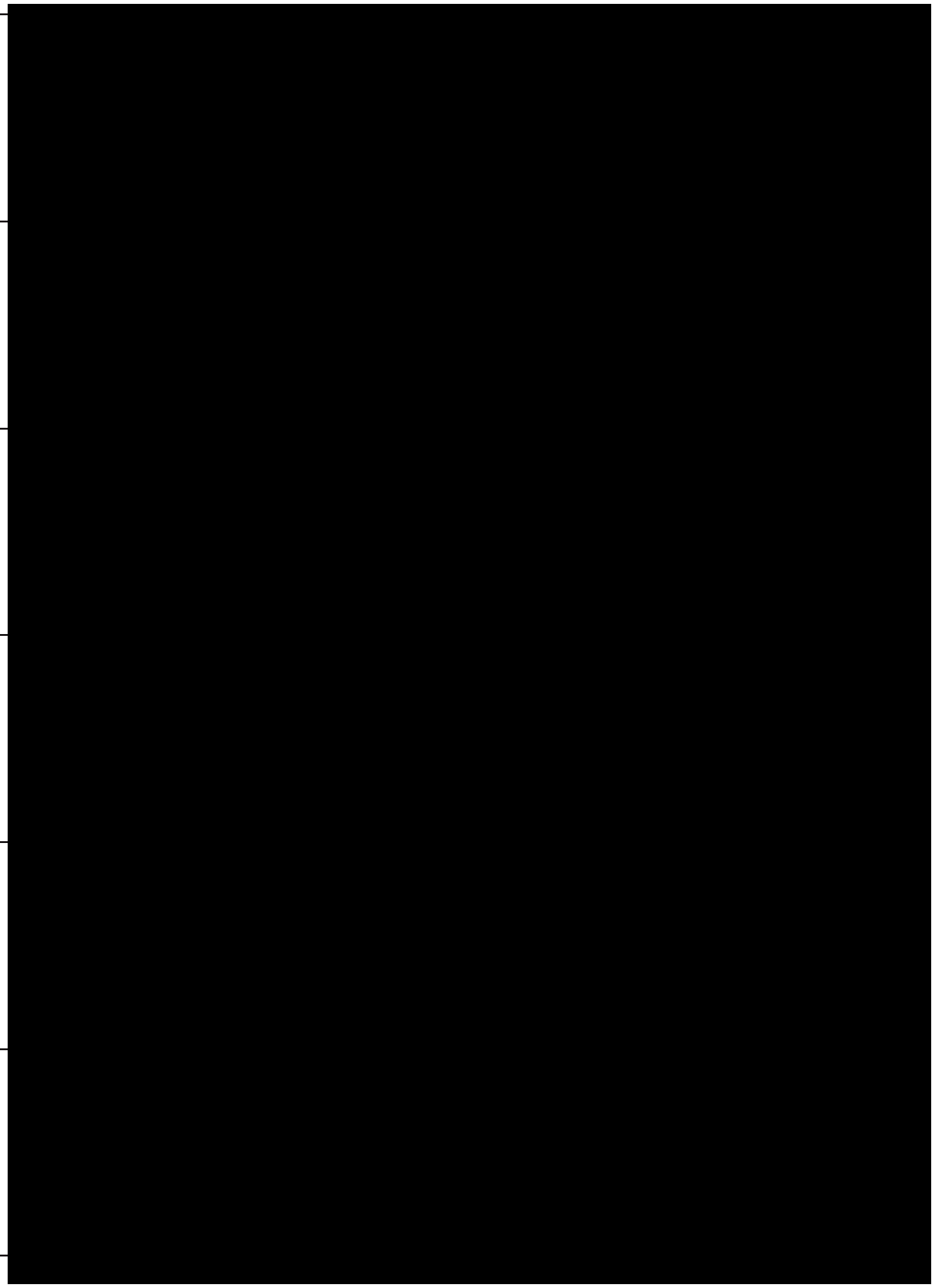


M-586	Ability of the receiving user to enter a single keystroke command to retrieve and display the message.
M-587	Ability to set message priority of specific system generated messages (e.g., high priority of warrant file returns).
M-588	Ability to notify receiver that message has not been read after an agency-defined period of time.
M-589	Ability to note time opened/read by receiver.
M-590	Ability to queue and display message waiting by priority.
M-591	Ability to clear a message from the queue.
M-592	Ability to retain a message in the queue.
	Ability to provide the following message indicators:
M-593	Message acknowledged or not received
M-594	Message viewed
M-595	Number and priority of queued messages
M-596	Number of messages received
M-597	Number of messages waiting
	Ability to utilize standard keys/touch screen functions to perform the following with one keystroke:
M-598	Clear display
M-599	Clear/erase message
M-600	Clear/erase operator's entire message queue with prompt to confirm deletion
M-601	Display next message
M-602	Store/recall message from message queue
M-603	Reply
M-604	Forward
M-605	Ability for supervisors to monitor or audit messages.
M-606	Ability for supervisors to disable the monitoring of messages.
M-607	Ability to store messages in an agency-defined buffer size.
M-608	Ability to delete oldest messages as buffer fills.
M-609	Ability to have a preview pane in the inbox.
	Incident Command
	Incident Command Data Capture and General Features
	Ability to provide an incident command system that tracks:
M-610	Personnel on-scene
M-611	Incident location

[redacted]

M-612	Situation status	[redacted]
M-613	Radio channel(s)	
M-614	Resource(s) on-scene	
M-615	Resource(s) assigned	
M-616	Resource(s) assigned to a functional management group (e.g., group, division, task force, staging/base, rehab, etc.)	
M-617	Resource(s) en route	

M-618	Resource(s) staging
M-619	Resource(s) location
M-620	Resource(s) status
M-621	Resource(s) role(s)
M-622	Next-in resources
M-623	Patient count and status



M-624	Suggested additional resources	[redacted]
	Tasks/Request/Objective:	
M-625	Assigned to	
M-626	Status	
M-627	Title	
M-628	Completed [Y/N]	
M-629	Narrative	
M-630	Agency-defined criteria	
M-631	Ability to support an alternate/secondary dispatching mode (e.g., dispatch is overloaded in major storm).	
M-632	Ability to time stamp entries (for chronological tracking of events).	
M-633	Ability to provide access to agency protocols and SOPs.	

M-634	Ability to support incident timers.	[redacted]
M-635	Ability to associate timers and alerts with specific tasks.	
M-636	Ability for data fields to have agency-defined drop down lists.	
M-637	Ability to add data elements to the incident command module.	
M-638	Ability to support voice commands.	
	Ability for incident command system to support:	
M-639	Police	
M-640	Fire/EMS	
M-641	Unified command (i.e., Police and Fire/EMS)	
M-642	Ability for multiple users to enter data in the incident command system simultaneously from separate terminals.	
M-643	Ability to provide an organizational breakdown/hierarchy of resources on scene (e.g., organizational chart)	
M-644	Ability for each agency to define hierarchy of positions based upon response type (e.g., initial incident command, rapid intervention, etc.)	
M-645	Ability for each agency to define tasks necessary to complete as determined by the incident type.	
M-646	Ability to provide messaging capabilities within the Incident Command module.	
M-647	Ability to have templates that are dedicated to specific functional areas (e.g., treatment areas, staging areas, etc.).	
M-648	Ability to link certain data fields to a global view within the incident command module (e.g., provide high level summary of each functional area on a master display).	
M-649	Ability to use incident command modules from various mobile devices (MDC, wireless laptop, handheld device).	
M-650	Ability to transfer information from the Incident Command module to WebEOC.	
M-651	Ability to add images.	

M-652	Ability to add videos.
M-653	Ability to save information in progress.
	Incident Diagramming
M-654	Ability to provide a scene diagramming tool.
M-655	Ability to import a preplan or GIS later and then add to it.
M-656	Ability to provide standard icons to be used within the scene diagramming tool (e.g., building, apparatus, etc.)
M-657	Ability to provide a free-form drawing tool on the scene diagramming feature.
M-658	Ability to add text to any drawn images.
M-659	Ability to support "white-board" functionality (e.g., user edits a large white board with data automatically sent electronically to the system)
M-660	Ability to import images onto "white-board."
M-661	Ability for diagramming tool to support three-dimensions.
M-662	Ability for system to support plume modeling.
M-663	Ability for system to support fire modeling.
M-664	Ability to zoom in and out of diagramming tool.
	System Access/Sharing
M-665	Ability to use the Incident Management module without wireless connectivity.
M-666	Ability to share incident management screen with other Mobile workstations.
M-667	Ability for Incident Management feature to only be available to authorized users based upon agency-defined rights and privileges.
	Systems Integration
M-668	Ability for incident management information to be integrated with a Mobile unit's map upon assignment to an incident.
M-669	Ability for Incident Management command screen to be automatically updated with information from CAD.
M-670	Ability for all information documented in the Incident Management module be automatically transferred to the appropriate RMS.
M-671	Ability for, upon entry of a location into the Incident Command module, the system to automatically recall all pre-plan information for that location.
M-672	Ability for roster information (including equipment) from CAD to be available in the Incident Command system.
M-673	Ability for incident management actions to update CAD and other Mobile users.
	After Action Reporting
M-674	Ability for system to create a log of all actions taken within the Incident Management module.
M-675	Ability to provide a system playback to allow users to review step-by-step actions of users.

Attachment G-2 – Exhibit B – Law Enforcement RMS Functional Specifications Matrix

[following this page]

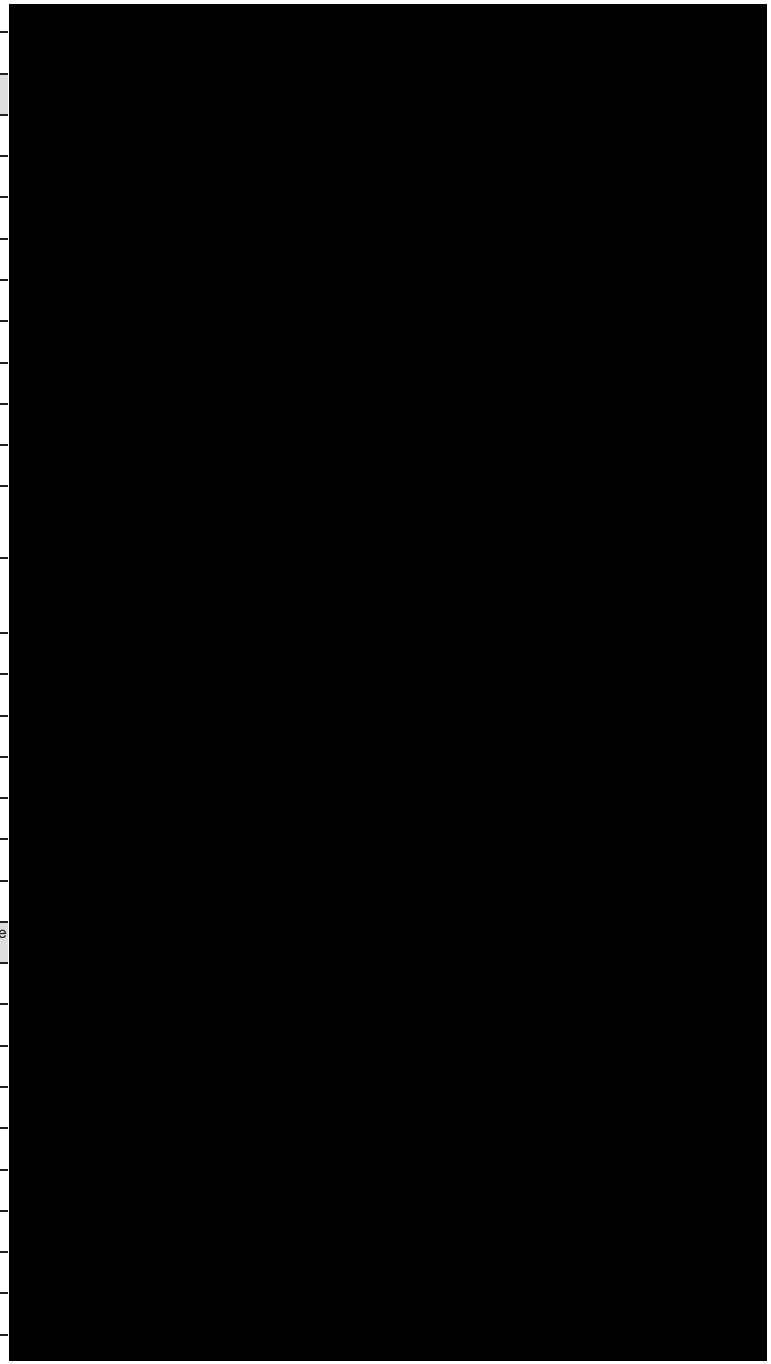
County of Williamson Texas
Law Enforcement Records Management System Specification

	Law Enforcement RMS General Requirements	Vendor Response	Vendor Comments
LGen-1	All transactions, whether successful or not, are captured for audit reporting.		
LGen-2	Once created, audit report records are not able to be deleted or edited.		
LGen-3	Audit report records will include date, time, user ID, workstation ID, transaction description and success or failure.		
LGen-4	RMS will allow more than one module to be open at a time and to work between the multiple modules, and autosave on all.		
LGen-5	Location alerts, special situations, and flags can be scheduled for validation based on agency criteria.		
	Security		
LGen-6	Once a report is completed and approved by the appropriate supervisor, it is locked and non-editable without the intervention of an authorized user with appropriate security designation(s).		
LGen-7	During report approval process, updates and edits are tracked.		
LGen-8	The system provides for a spell check capability on narrative entries.		
LGen-9	The system allows for the addition of user defined/regional spellings.		
LGen-10	The system provides for a grammar check capability on narrative entries.		
LGen-11	The ability to restrict access to individual records related to persons and activities when performed by an authorized user.		
LGen-12	RMS records are accessible from authorized mobile devices (e.g. cell phones, tablets).		
LGen-13	RMS records are accessible by authorized, external workstations from other jurisdictions with appropriate security and controls.		
LGen-14	The system meets current CJIS security policy requirements and internal controls.		
LGen-15	Solution is capable of CJIS Advanced Authentication methodology for access security and internal controls.		
LGen-16	Authorized user access to RMS modules, records, and juvenile files are based on active directory permissions .		
LGen-17	Access to data can be restricted by jurisdiction, agency, department, discipline and bureau within a department.		
	Basic Capabilities		
LGen-18	LERMS data fields fully integrate with the CAD software.		
LGen-19	Full integration include automatic, seamless transfer of critical information between CAD, mobile computing, and LERMS.		
LGen-20	The system is capable of interfacing to TLETS law enforcement database.		
LGen-21	The system can support the sharing of certain data between law enforcement agencies.		
LGen-22	The system will notify a user, or users, designated by the Agency in the event of any interface failure.		
LGen-23	LERMS records functions are tightly integrated to the proposed CAD system.		
LGen-24	LERMS records functions is tightly integrated to the proposed mobile data system.		
LGen-25	Drop down lists throughout the application, in all modules, utilize common data and do not require separate entry for similar fields.		

LGen-26	Drop down lists throughout the application, in all modules, remain in sync as changes are made to the list data.
LGen-27	The software allows for agency defined colors on all forms and screens.
LGen-28	The software allow toolbars and toolbar buttons to be agency defined.
LGen-29	The software allows patches and updates to be distributed and deployed to remote and mobile workstations from a single management console.
LGen-30	The system supports forms incorporating dynamic data entry user interfaces. For example, if data entered in field of a form has a certain value, other fields of that form can be made mandatory entry fields.
LGen-31	The system is capable of denoting an officer as the primary officer for a report.
LGen-32	The system is capable of denoting an officer as the secondary officer for a report.
LGen-33	The system is capable of switching the primary and secondary officers on a report with a built-in command.
	The system, at a minimum, supports the capture/transfer from CAD of the following data elements for each CAD event:
LGen-34	Event number
LGen-35	Case number
LGen-36	Event location
LGen-37	Event type - initial
LGen-38	Event type - final
LGen-39	Caller location
LGen-40	Caller name
LGen-41	Call back number
LGen-42	Alternate call back number
LGen-43	Event priority
LGen-44	Call Back field (date and time)
LGen-45	Comments text fields
LGen-46	Disposition (unlimited)
LGen-47	Time call received
LGen-48	Time dispatched
LGen-49	Time each unit responded
LGen-50	Time each unit arrived
LGen-51	Time each unit cleared
	The system, at a minimum, supports the capture/transfer from CAD of the following data elements for each unit logged on during a shift:
LGen-52	Unit ID of all units assigned to the CFS
LGen-53	Vehicle ID number
LGen-54	MDC log in times
LGen-55	MDC log out times

[redacted]

LGen-56	All Personnel assigned to the CFS
	The system supports the capture/transfer from CAD of the following, at a minimum, data elements for each event to which the unit was assigned:
LGen-57	Time dispatched
LGen-58	Time acknowledged
LGen-59	Time enroute
LGen-60	Time arrived
LGen-61	User defined milestones (shots fired, in custody, in pursuit, pursuit terminated)
LGen-62	Time departed for transport
LGen-63	Time arrived for transport
LGen-64	Time available
LGen-65	Time cleared
LGen-66	If the data is available in CAD, the system will accept and store State/NCIC inquiry and return data from the CAD system in accordance with CJIS security policy.
LGen-67	The State/NCIC inquiry data will be associated with the CAD incident report for which it was captured in accordance with CJIS security policy.
LGen-68	Available call data for completing incident reports, is updated and available to an authorized user at any time. The intent of this requirement is to ensure that it is not necessary for a unit to wait until an event is closed before they can complete their report.
LGen-69	The system provides a method, including full audit trail information, for an authorized user to re-open a report for changes.
LGen-70	All CAD data fields are capable of import to the LERMS.
LGen-71	The database tables are shared between CAD & LERMS Systems.
LGen-72	The system allows any active workstation to print to any printer available on the network.
LGen-73	An authorized user is capable of generating hard-copy incident reports.
LGen-74	Redaction capabilities function across all RMS system modules.
	The system allows authorized users to automatically redact, at a minimum but not limited to, the following items from any printed case report:
LGen-75	Information for all involved parties
LGen-76	Juvenile Information
LGen-77	Social Security Numbers
LGen-78	Case Narratives
LGen-79	Personnel Information
LGen-80	Phone Numbers
LGen-81	Date of Birth (DoB)
LGen-82	Any data selected by the Agency
LGen-83	Any protected data as determined by the Agency



	Reporting
LGen-84	The system provides user maintainable workflow defined by report, by user and by department (agency), e.g., Report submitted -> Supervisor review -> Report returned to officer for correction if necessary -> Report resubmitted -> Supervisor approval.
LGen-85	Reports are available for viewing by multiple users simultaneously and at any point in the report development process. (e.g. Reporting officer and supervisor)
LGen-86	The system has the ability to identify outstanding reports by personnel name and ID.
LGen-87	Field Reporting is capable of referencing and including data in reports across all disciplines requiring data to only be added once.
LGen-88	The system is able to generate electronic NIBRS reports for submission to the State and or Federal agencies as required.
LGen-89	The system is able to generate electronic UCR reports for submission to the State and/or Federal agencies as required (if State has not transitioned to NIBRS).
LGen-90	Ability to generate multiple standard reports per module to facilitate statistical analysis.
LGen-91	The system provides for the ability to create and modify ad-hoc reports and queries.
LGen-92	Field Reporting provides the ability to create, modify and store user-defined reports.
LGen-93	All entry fields are available for inquiry.
LGen-94	All entry fields are available for inclusion in reports.
LGen-95	Field Reporting will support batch uploads of attachments.
LGen-96	Batch uploads will be able to specify an alternate path/location for storage of certain file types (example: jpeg, mp4, mov)
LGen-97	Field Reporting is capable of creating, displaying and printing maps and GIS-data including data from all modules.
LGen-98	The system provides the capability to schedule report generation.
LGen-99	The reporting system is capable of generating user defined statistical reports.
LGen-100	The reporting system is capable of printing graphs.
LGen-101	The reporting system is capable of printing charts.
LGen-102	The reporting system will have the ability to query DB data warehouse to generate custom reports.
LGen-103	A Data dictionary is mandatory with fields/tables identified within application.
LGen-104	The reporting system will have the ability to display in BI/Dashboard format thoughout the modules.
	Law Enforcement Master Name Index
LMNI-1	A Master Name Index (MNI) is provided.
LMNI-2	All master name activity for a subject can be accessed via one record.
LMNI-3	The system should have controls to prevent duplicate entries.
LMNI-4	Master name properties outlined above are an agency-level or client level configuration option.
LMNI-5	Any activity for a subject can be viewed from the subject activity records (i.e. a case record can be accessed from the case suspect activity record contained within the master name file).
LMNI-6	The system is able to attach multiple supporting documents/files of various types (e.g., Word, Excel, JPG, MPG, WAV, PDF, PNG) to a master name record.
LMNI-7	Mug Shots can be attached to MNI records.
LMNI-8	Once a master name record is created, an authorized user is able to update any basic data fields and add or modify other information as necessary.
LMNI-9	The MNI is accessible and integrated with all modules where name information is needed/referenced.

[redacted]

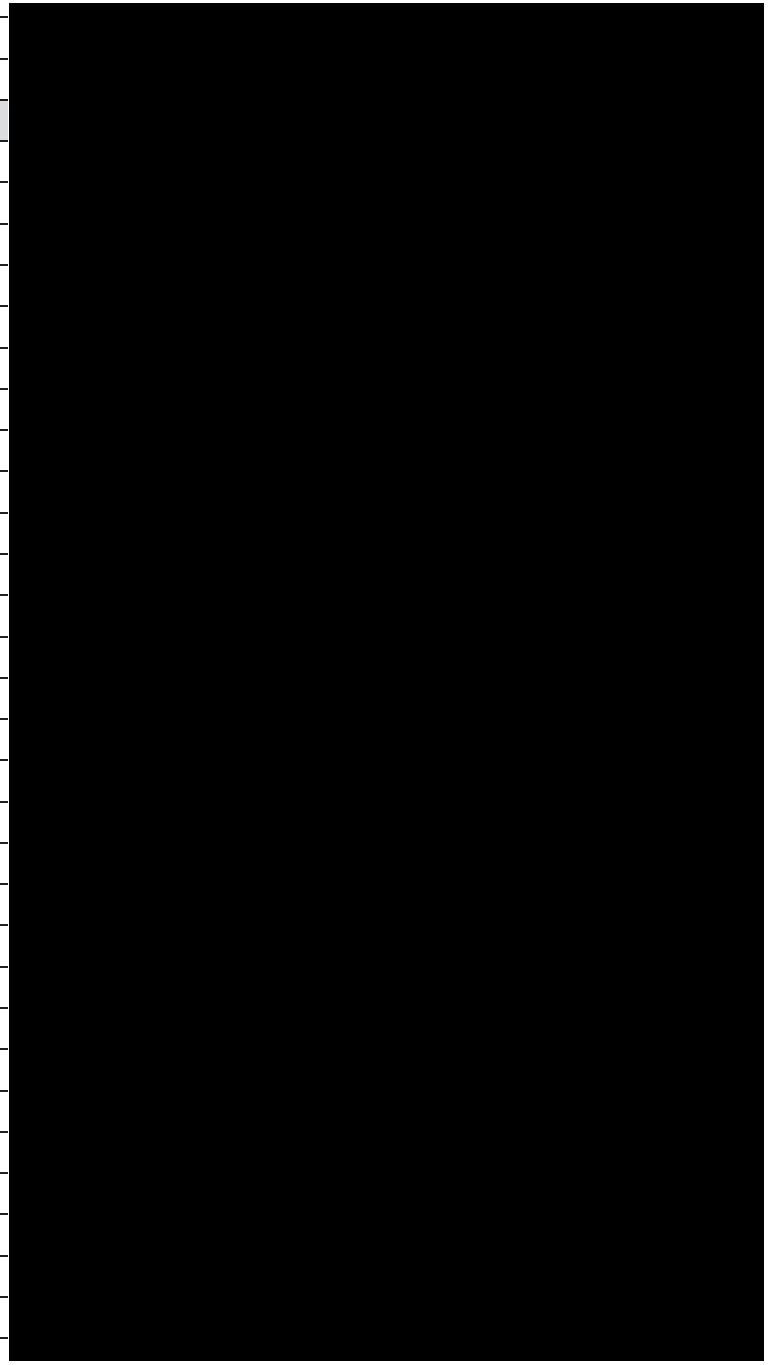
LMNI-10	The system provides a process to merge/consolidate duplicate master name records.
LMNI-11	The system will display cautions (e.g. warrants, career criminal) associated with any names when displaying the master name record.
LMNI-12	The system allows for the tracking of business names (e.g. McDonalds), and associated business-related fields, to be entered within the MNI.
LMNI-13	The MNI integrates with the MLI (Master Location Index).
LMNI-14	The system provides field level auditing within a master name record.
LMNI-15	Edits to master name records initiates an alert to agency defined records manager.
LMNI-16	The system shall display the most current image of a subject, if available, within all master name screens.
LMNI-17	The system shall display the most current image of a subject, if available, within all master name screens with controls to prevent juvenile images from being displayed on public facing applications.
LMNI-18	The system allows authorized users to access images from a single source across all modules.
LMNI-19	Image access can be restricted based on module (e.g. narcotics) or an incident being highly confidential or sensitive. (e.g. political figure, celebrity, high public interest) or juveniles.
LMNI-20	The system is able to retrieve and display all associated images of the subject, if available, within all master name screens.
LMNI-21	The system is capable of restricting access to social security number.
LMNI-22	The system shall provide the capability to track, chronologically, the changes to an individual's master name record, including the user who made the change.
LMNI-23	The system will track workstation Name/ID or MAC address.
	The consolidation/merge process allows searching the master name index by any combination of the following demographic information:
LMNI-24	First Name
LMNI-25	Middle Name
LMNI-26	Last Name
LMNI-27	Name Suffix
LMNI-28	DOB
LMNI-29	Age
LMNI-30	Social Security #
LMNI-31	Phone Number
LMNI-32	Address
LMNI-33	Race
LMNI-34	Ethnicity
LMNI-35	Sex
LMNI-36	Height
LMNI-37	Weight
LMNI-38	Drivers License #
LMNI-39	All activities related to the records being merged will also be consolidated in the same master name record.
LMNI-40	Any record affected by a master name merge will be updated with the selected master name record.

[redacted]

LMNI-41	Merged records will be listed in the chronological order (see above).
LMNI-42	The record being merged into the master record could be listed as an alias record.
LMNI-43	Aliased records can be kept in a separate name index.
	The MNI is accessible and integrated with the following activities, at a minimum:
LMNI-44	Arrests
LMNI-45	Crashes
LMNI-46	Bookings
LMNI-47	Case entry
LMNI-48	Case management
LMNI-49	Tickets and Citations
LMNI-50	Warrants
LMNI-51	Mug shots
LMNI-52	Gang Tracking
LMNI-53	Narcotics Tracking
LMNI-54	Field Reporting
LMNI-55	Civil Process
LMNI-56	Field Interviews
LMNI-57	Career Criminal
LMNI-58	Criminal Trespass Log
LMNI-59	The ability to view MNI entries by modules is configurable by authorized users. This functionality can be toggled on/off by agencies.
LMNI-60	The MNI is accessible from CAD, but is not editable.
LMNI-61	Only authorized users can access MNI information from the CAD
LMNI-62	The system supports a MNI where any events in the system will associate with the master name.
LMNI-63	An authorized user is able to expunge names and specific activity related to any individual.
LMNI-64	An authorized user is able to expunge names and specific activity related to any record.
LMNI-65	Expungement will result in the record or selected portion of the record being hidden from view without being deleted from the system.
LMNI-66	Expungement will result in the record or selected portion of the record being deleted from the system, not hidden.
LMNI-67	The system supports inquiry of the MNI that will return both first name and commonly associated nicknames (e.g. Jonathan and John, Michael and Mike).
LMNI-68	The system supports inquiry of the MNI which can use wild card substitution.
LMNI-69	The system supports inquiry of the MNI which can use soundex name substitution.
	The system provides a method (e.g., soundex) for identifying possible name matches for non-english pronunciation, including but not limited to:
LMNI-70	Hispanic names

[redacted]

LMNI-71	Middle Eastern names
LMNI-72	Asian names
	At a minimum, the system tracks the following data as a part of the MNI:
LMNI-73	First, middle and last names as individual fields
LMNI-74	Former names, legally changed (e.g., maiden name)
LMNI-75	Current address
LMNI-76	Prior addresses (unlimited number)
LMNI-77	Temporary address
LMNI-78	Suffix(s)
LMNI-79	Multiple Phone Numbers (home, cell, work)
LMNI-80	Social Security number (verified)
LMNI-81	Date of Birth (verified)
LMNI-82	State of Birth
LMNI-83	Driver's license number and State
LMNI-84	State issued ID and State
LMNI-85	FBI number
LMNI-86	SID
LMNI-87	Local ID number
LMNI-88	Race
LMNI-89	Ethnicity
LMNI-90	Sex/Gender Identity
LMNI-91	Height
LMNI-92	Weight
LMNI-93	Build
LMNI-94	Hair color
LMNI-95	Hair length
LMNI-96	Hair style
LMNI-97	Eye color
LMNI-98	Complexion
LMNI-99	Facial Hair
LMNI-100	Glasses
LMNI-101	Photo



LMNI-102	Scar, Marks and Tattoos (unlimited) with defined fields for partial, side and a description.
LMNI-103	Fingerprint data
LMNI-104	Known associates, linked back to MNI.
LMNI-105	Relatives
LMNI-106	Employer information
LMNI-107	Emergency contact information (Multiple)
LMNI-108	E-mail addresses (multiple)
LMNI-109	All social media profiles
LMNI-110	School information.
LMNI-111	Parents, if a Juvenile
LMNI-112	Chronology of the changes to be tracked for an individual.
LMNI-113	Use caution flag.
LMNI-114	Narrative (unlimited)
LMNI-115	Narrative entries are date/time stamped.
LMNI-116	Narrative entries are displayed in reverse chronological order (newest entry first).
	At a minimum, the system provides a mechanism to allow an unlimited number of versions of the following information to be tracked for each unique individual in the system:
LMNI-117	Aliases / nicknames, each of which may contain all the above-described identifying information.
LMNI-118	Addresses, current and prior, with user-defined types, e.g., home, work.
LMNI-119	Telephone numbers, current and prior, with user-defined types, e.g., home, work, cell, pager.
LMNI-120	E-mail addresses
LMNI-121	Alias SSN/DOB
LMNI-122	Identifying numbers, e.g., SID, FBI, DL.
LMNI-123	State issuing Drivers License or ID
LMNI-124	State issued ID and State ID number
	At a minimum, the system provides the following types to be associated with individuals:
LMNI-125	Victim
LMNI-126	Witness
LMNI-127	Suspect/Person of Interest
LMNI-128	Associate/Involved Other/Reporting Party
LMNI-129	Relative
LMNI-130	Offender
LMNI-131	Owner

[redacted]

LMNI-132	Driver
LMNI-133	Passenger
LMNI-134	The System has the ability to search the MNI by any field available in a MNI record.
LMNI-135	Within a case folder, authorized users have the ability to easily see, all associations to person(s) throughout the system.
	Law Enforcement Master Vehicle Index
LMVI-1	A Master Vehicle Index (MVI) is provided.
LMVI-2	Where available, the system allows the import of standardized code tables from external sources, e.g., NIBRS, FBI.
LMVI-3	The system shall provide the capability to track, chronologically, the changes to an individual's master vehicle record.
	At a minimum, the system provides the following data as a part of the MVI:
LMVI-4	VIN
LMVI-5	Make of Vehicle (dropdown)
LMVI-6	Model (dropdown)
LMVI-7	Year
LMVI-8	Type (dropdown)
LMVI-9	Exterior Color (including top / bottom fields)
LMVI-10	Interior Color (including top / bottom fields)
LMVI-11	Narrative box for unique identifiers e.g., rims, stickers, vehicle damage.
LMVI-12	Vehicle registration (license plate number)
LMVI-13	State issuing vehicle registration (dropdown)
LMVI-14	Decal number
LMVI-15	Expiration date
LMVI-16	Owner (associated with a DMV record)
LMVI-17	Owner address
LMVI-18	Chronology of changes made to a vehicle record.
LMVI-19	The system allows the attachment of standard PC files to any record (e.g., PDF, JPG, WAV).
LMVI-20	The MVI is accessible and integrated with all modules where vehicle information is needed/referenced.
LMVI-21	The system will perform VIN format verification and alerts the operator when the format verification fails
LMVI-22	The user will have the ability to override a VIN verification failure.
	At a minimum, the MVI is integrated with the following activities:
LMVI-23	Accidents
LMVI-24	Field Interview contact information
LMVI-25	BOLOs

[redacted]

LMVI-26	Impounds
LMVI-27	Property
LMVI-28	Repossession
LMVI-29	Suspect vehicle (Incidents)
LMVI-30	Suspect vehicle (Cases)
LMVI-31	Tickets and Citations
LMVI-32	Towing
LMVI-33	The system supports inquiry of the MVI which can use any or all fields of the MVI record.
LMVI-34	The system supports inquiry of the MVI which can use wild card substitution.
LMVI-35	The system supports inquiry of the MVI which allows partial tag.
LMVI-36	The system supports inquiry of the MVI which allows partial VIN.
	Law Enforcement Master Location Index
LMLI-1	The system supports a Master Location Index (MLI) which could integrate with the CAD system.
LMLI-2	Where multiple MLI specifications are described in this RFP (e.g., Mobile, LERMS, FRMS, JMS), the system will provide a single Master Location file which encompasses the MLI specifications from each discipline.
LMLI-3	The system provides links between MLI and CAD to prior activity and history at addresses that will provide alerts in the CAD System.
LMLI-4	On a match between the CAD address and the MLI record, the system will visually alert the user.
LMLI-5	The Agency can determine the type of match causing an alert to be sent to the user.
LMLI-6	The system provides the ability to see in one location all information and activities related to a specific address throughout the system
LMLI-7	The MLI is accessible from all modules where location information is needed/referenced.
LMLI-8	The system supports a Master Location Index (MLI) which will integrate with CAD, providing links to prior activity and history at addresses that will provide alerts in the CAD System.
LMLI-9	Ability to see in one location all activities related to a specific address throughout the system (e.g., any fire incidents, EMS incidents, investigations, permits, inspections, etc.).
LMLI-10	MNI persons related to the location can be associated with the location record.
	The MLI must be accessible by:
LMLI-11	Specific address
LMLI-12	Range of addresses
LMLI-13	Common place name
	The MLI will include the following data elements:
LMLI-14	Common place name
LMLI-15	Alarm permits
LMLI-16	Neighborhood
LMLI-17	Districts/Zone/Beat/Grid
LMLI-18	X/Y/Z Coordinates

[redacted]

LMLI-19	Alerts
LMLI-20	Hazards
LMLI-21	Images (unlimited)
	The MLI is capable of performing the functions and/or capture data for the following:
LMLI-22	Record basic location information
LMLI-23	Automatic assignment of multiple reporting districts
LMLI-24	Intersections
LMLI-25	Block face addresses (zip codes)
LMLI-26	Commonplace names
LMLI-27	Map coordinates (latitude and longitude)
LMLI-28	Cautions/hazards/alerts
LMLI-29	Occupancy elevation (e.g., floor)
LMLI-30	Premise Type (e.g., single family residence, commercial, apartment building)
LMLI-31	Case references
LMLI-32	Residents
LMLI-33	Residence checks
LMLI-34	Emergency contact information
LMLI-35	Specific address searches
LMLI-36	Address range searches
LMLI-37	Selected persons (e.g., arrestees, suspects, witnesses, victim)
LMLI-38	Known associates
LMLI-39	Address inquiries
LMLI-40	Address recap to report on the total number of times that each address has been linked to incidents, arrests, and home addresses of individuals.
	The MLI will include the following data elements:
LMLI-41	Common place name
LMLI-42	Alarm permits
LMLI-43	Neighborhood
LMLI-44	Alerts
LMLI-45	Hazards
LMLI-46	The system will create valid address points and warn when a system does not have a valid address point.
LMLI-47	The MLI will link to a map layer using Esri ArcGis.
	Law Enforcement Crime Analysis

[redacted]

LCrmA-1	The system will utilize existing data previously entered or transferred into other integrated application modules for use in crime analysis reporting.
LCrmA-2	The system should be able to create static reports
LCrmA-3	The system should be able to create custom dashboards
	At a minimum, the following data will be extracted:
LCrmA-4	Date of Offense
LCrmA-5	Date Types, e.g., Report Date, Date Occurred, Arrest Date, etc.
LCrmA-6	Time of Offense
LCrmA-7	Time Types, e.g., Report Time, Time Occurred, Arrest Time, etc.
LCrmA-8	Location of Offense
LCrmA-9	Description of the Premises
LCrmA-10	Type of Offense
LCrmA-11	Method and Point of Entry
LCrmA-12	Description of Weapons Used
LCrmA-13	Description of Tools Used
LCrmA-14	Victim Data (Age/Relationship/Race/Sex/Gender Identity)
LCrmA-15	Type of Property Stolen
LCrmA-16	Suspect Vehicle Description
LCrmA-17	Suspect Description
LCrmA-18	M.O. Parameters
LCrmA-19	The data will be able to be reproduced in hard copy and used in map plotting
LCrmA-20	The system can generate any reports using a report wizard.
LCrmA-21	The system will allow authorized users access to access to the data warehouse to create custom reports.
LCrmA-22	The system has a built-in data assist capability that identifies in the user interface the table & field names for each data area of the software.
LCrmA-23	The system can generate a report that shows statistical data on crimes concerning the frequency and the distribution of crime throughout user-selected jurisdiction reporting districts/zone/beat/grid.
LCrmA-24	The system can generate a report that shows statistical data on crimes concerning the frequency and the distribution of crime throughout user-selected mapping layers available via the GIS maps (e.g., stations, sectors, grids, voting districts, etc.).
LCrmA-25	The system is able to retrieve cases with similar crime modus operandi to assist investigators in solving crimes.
LCrmA-26	The system is able to produce a solvability matrix
LCrmA-27	The system is able to identify the overall activity per crime type within a selected date range and reporting district.
	The system can create reports that target specific types of crimes based on the following:
LCrmA-28	Location (specific address) of Occurrence
LCrmA-29	User Selected Crime Type

[redacted]

LCrmA-30	Hate Bias Information
LCrmA-31	Geographical Groupings of Crimes
LCrmA-32	Similar Types of Victims
LCrmA-33	Common M.O. of Crime
LCrmA-34	Suspect Vehicle Description
LCrmA-35	Suspect Physical Description
LCrmA-36	Tools Used
LCrmA-37	Weapons Used
LCrmA-38	Property Targeted for Theft
LCrmA-39	Point and Method of Entry
LCrmA-40	Scene Category of Crime, e.g., Residence, Grocery/Supermarket
LCrmA-41	Theft Category of Crime (e.g., shoplifting from buildings, vehicles)
LCrmA-42	Crime Attempts
LCrmA-43	NIBRS offense codes
LCrmA-44	Description fields should be searchable via the use of wildcard characters, e.g. *.
LCrmA-45	The system allows the generation of ad hoc reports.
LCrmA-46	The system allows data to be sorted based on any field used to create the report.
LCrmA-47	The system is able to link related complaints together through associated case numbers.
LCrmA-48	The system allows report data to be exported in multiple file formats. For instance, ASCII, CSV, JSON, XML, Flat File, etc.
LCrmA-49	The system allows a report to be converted to PDF format.
LCrmA-50	The system provides the capability for data to be displayed as ESRI compliant GIS spatial data on a non-proprietary map, e.g., pin mapping, hot spots.
LCrmA-51	The system allows ESRI compliant data to be exported to a GIS module.
	The system can produce the following specific reports.
LCrmA-52	Records entry activity by user (user ID), to include cases, citations, and accidents.
LCrmA-53	Reports entered by officer (officer ID).
LCrmA-54	Missing reports (reports where a case number was issued but the report is not in the main LRMS case module).
LCrmA-55	Cases with invalid adresses.
LCrmA-56	Officer activity log (calls for service based on clearance codes/dispositions assigned to call, by officer and by shift).
LCrmA-57	Open cases requiring supplements.
	The system can retrieve suspect names based on:
LCrmA-58	Available photo
LCrmA-59	Known Offender Address

[redacted]

LCrmA-60	Past Criminal Contacts
LCrmA-61	Past Vehicle Relations
LCrmA-62	Pawn Transactions
LCrmA-63	Known Associates
	The system can retrieve suspect vehicle information based upon:
LCrmA-64	Year of Vehicle
LCrmA-65	Make of Vehicle
LCrmA-66	Model of Vehicle
LCrmA-67	Style of Vehicle
LCrmA-68	Top and Bottom Color of Vehicle
LCrmA-69	License Plate of Vehicle (including partial plates)
LCrmA-70	License Plate State of Vehicle
	The system can retrieve information on vehicles obtained through:
LCrmA-71	Field Interview Reports
LCrmA-72	Prior Contacts with the Department
LCrmA-73	Arrests
LCrmA-74	Case Reports
LCrmA-75	Citations/Moving Violations
LCrmA-76	Crash Reports
LCrmA-77	Want and Warrant Records
LCrmA-78	Suspect Vehicles Record
LCrmA-79	Impounded Vehicles
LCrmA-80	The system will retain Modus Operandi (M.O.) characteristics in agency specified coded fields.
LCrmA-81	The system is able to search for M.O. characteristics as selected parameters.
LCrmA-82	The system is able to generate reports with M.O. parameters and crime specialties.
	The system will retreive information on known offenders, such as:
LCrmA-83	Past Criminal Contact
LCrmA-84	Sex Offenders
LCrmA-85	Narcotics Offenders
LCrmA-86	Other Agency-defined Offender Types
	The system is able to capture and retrieve juvenile information, including:
LCrmA-87	Juvenile Demographic Information

[redacted]

LCrmA-88	Juvenile Personal Characteristics
LCrmA-89	Juvenile Guardian Information
LCrmA-90	The system is able to capture and retrieve crime analysis information from complaint records when information is included on a juvenile arrest.
LCrmA-91	The system should visually indicate when a subject is a juvenile
	Law Enforcement Gang Tracking
LGang-1	The system accepts and maintains information about gangs.
LGang-2	The system accepts and maintains information about individual gang members.
LGang-3	The system tracks gang activity.
LGang-4	The system tracks individual gang member activity.
LGang-5	The system will alert users to identified gang locations.
LGang-6	The system will alert users to identified gang members.
LGang-7	The system will alert users to identified gang/gang member vehicles.
LGang-8	The system allows gang tracking data to be secured from unauthorized users.
LGang-9	They system will have specific read-only rights for Gang information.
LGang-10	The system allows gang case data (that does not include IBR and/or UCR reporting elements) to be maintained separately from other agency case information.
LGang-11	The system allows gang case data to be approved for general viewing based on approval of authorized user.
LGang-12	The module is compliant with 28 Code of Federal Regulations Part 23 (28 CFR Part 23), which is considered the national standard for criminal intelligence information under the National Criminal Intelligence Sharing Plan.
	The system accepts and maintains the following basic gang related information:
LGang-13	Gang name
LGang-14	Gang type
LGang-15	Location/Address/general area/Beat
LGang-16	Number of members
LGang-17	Alliances/origin
LGang-18	Date of Alliances
LGang-19	Ethnicity
LGang-20	Race
LGang-21	Dress/colors
LGang-22	Any other symbols, graffiti, hand signs
LGang-23	Number of sub-groups
LGang-24	Name of sub-groups
LGang-25	Reporting district
LGang-26	General description (free-from text narrative)

[redacted]

LGang-27	Modus operandi
LGang-28	Weapons
LGang-29	Vehicles
LGang-30	Associated gangs
LGang-31	Rivals
LGang-32	The system accepts and tracks gang-related activities.
	The system accepts and maintains records on individual members of a gang, including, at a minimum:
LGang-33	Start/first contact date
LGang-34	Gang relationship
LGang-35	Known vehicles
LGang-36	The system has the capability of attaching multiple supporting documents of various types to a gang record.
	The system is able to search for gang information using the following criteria:
LGang-37	Gang name
LGang-38	Gang type
LGang-39	Location
LGang-40	Unique Number (e.g. agency system number, corrections number)
LGang-41	Alliance/origin
LGang-42	Ethnicity
LGang-43	Dress/colors
LGang-44	Modus operandi
LGang-45	Gang member
LGang-46	Gang associate - non-member
LGang-47	Reporting district
LGang-48	The system will accept and maintain multiple contact numbers associated with gangs.
LGang-49	The system will accept and maintain multiple contact numbers associated with individual gang members.
LGang-50	The module must require date, time, code, type and officer name to create an activity record.
LGang-51	The system will accept, maintain, and track intelligence records, i.e., information received from various informants about a gang or gang member.
LGang-52	The system can generate gang related reports.
	Law Enforcement Crime Reporting
	The system satisfies the requirements for electronic submission to State UCR/NIBRS repository
LCrmR-1	Uniform Crime Reporting (UCR) including specific requirements (family violence, sexual assault, drug seizure)

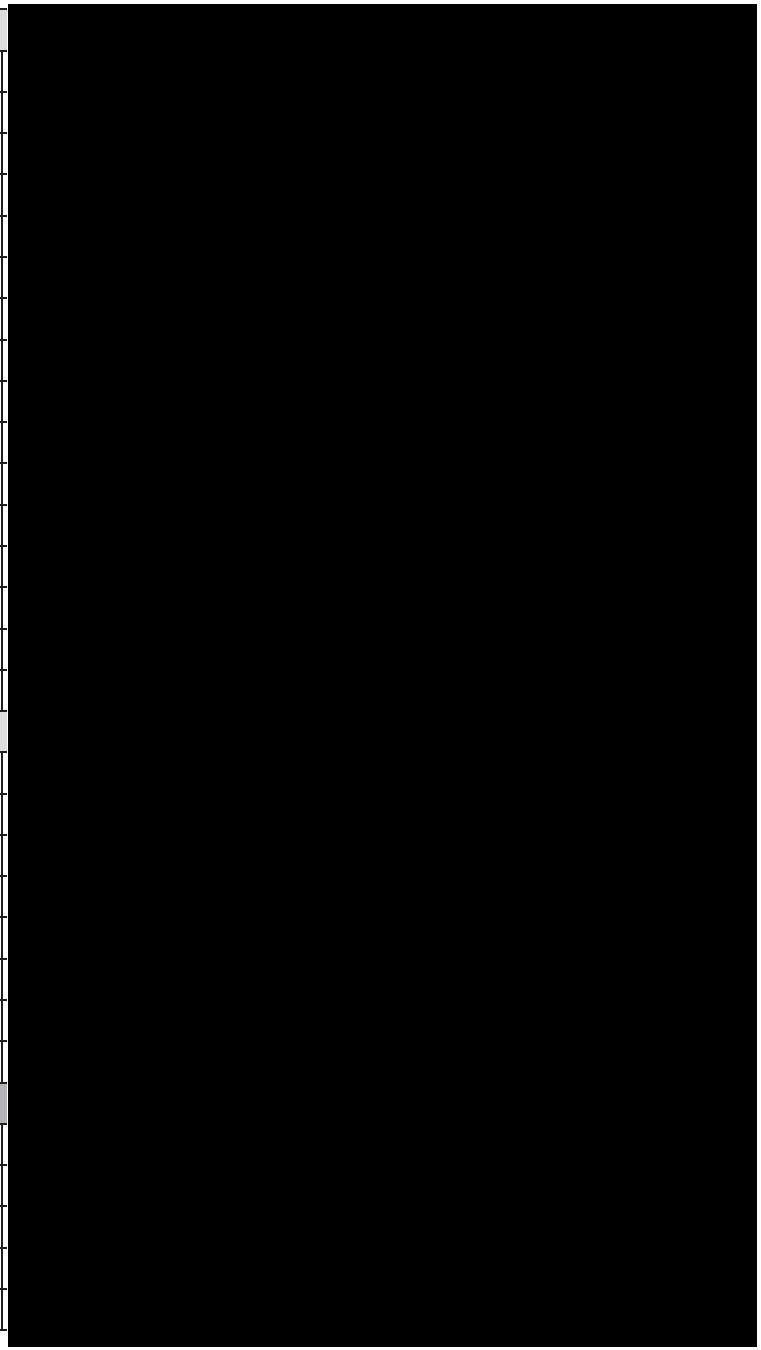
[redacted]

LCrmR-2	National Incident Based Reporting System (NIBRS)
LCrmR-3	The ability to track additions/modifications/deletions to already submitted data for reporting to the state, as required by State Reporting guidelines.
LCrmR-4	The system has the ability to transmit changed and updated records as well as original records within the reported month.
LCrmR-5	The system provides the required NIBRS data elements in the appropriate formats.
LCrmR-6	The system provides the required UCR data elements in the appropriate formats.
LCrmR-7	The system has the ability to validate UCR and/or NIBRS information and identify errors prior to submission.
LCrmR-8	The system has the ability to edit the monthly NIBRS information and identify errors before submission.
LCrmR-9	The system has the ability to update previously submitted records with revised information.
LCrmR-10	The system will provide the ability to submit monthly reports electronically
	Law Enforcement Investigations
	Basic Capabilities
LInv-1	The system can track Law Enforcement investigations.
LInv-2	The system can restrict access to data pertaining to juvenile offenders to authorized users only.
LInv-3	The juvenile offenders section within the investigations module can have separate security settings.
LInv-4	The system supports the ability to create multiple investigation types.
LInv-5	The system upholds strict security allowing only authorized user(s) access to investigation records.
LInv-6	For NIBRS reporting, the system allows the designation of an incident as a potential arson, with ability to record additional fields of associated information.
LInv-7	The system is able to secure investigative records to limit individual and group access to individual or multiple records.
	Investigation data includes, but is not limited to:
LInv-8	Investigator name and/or ID number
LInv-9	PD investigator assigned
LInv-10	Call for Service/RMS case number
LInv-11	Date case begun
LInv-12	Date case closed
LInv-13	Investigation location / address
LInv-14	Witness information/statements (unlimited)
LInv-15	Victim information/statements (unlimited)
LInv-16	Property Occupant
LInv-17	Property owner address
LInv-18	Individual collecting evidence
LInv-19	Property Type (i.e. evidence, property, sample, etc.)
LInv-20	Track Chain-of-Evidence

[redacted]

LInv-21	Characteristics of modus operandi	[redacted]
LInv-22	Narrative	
LInv-23	The system is able to attach graphic file(s) to an investigation record (e.g., scene diagram).	
LInv-24	The system interfaces with third-party diagraming software to import scene diagram graphic file(s) into investigative records.	
LInv-25	The system is able to restrict assigned investigator to certain information.	
LInv-26	The system is able to assign investigator(s) to case.	
LInv-27	The system is able to relate multiple incidents to one case.	
LInv-28	The system is able to attach any Windows-compliant file(s) to an investigation record.	
LInv-29	The system allows case status to be updated with ongoing activities and notes.	
LInv-30	The system is able to import, link, or attach initial reports into the investigation record.	
Linv-31	The system has the capability to lock down a Case to authorized users only.	
	Investigative Case Management	
	The system tracks, at a minimum, the following for each case:	
LInv-32	Assigned to	
LInv-33	Assigned date	
LInv-34	Status	
LInv-35	Status date	
LInv-36	Initial narrative	
LInv-37	Supplemental narratives (unlimited)	
LInv-38	Solvability factors	
LInv-39	Calculated solvability rating	
LInv-40	Hours of activity	
	The system provides case investigation summaries for each detective including at a minimum, the following:	
LInv-41	Number of active cases	
LInv-42	Case type breakdown	
LInv-43	Assignment date	
LInv-44	Activity log	
LInv-45	The system is capable of assigning "split" case management. Case management assigned to more than one division or administrative units. (e.g., Narcotics and Crimes Against Persons)	
LInv-46	An authorized user is able to assign (or reassign) cases to any detective.	
LInv-47	The system is able to view and print entire case report.	

	An authorized user can locate subjects using a single criterion or multiple criteria, including, but not limited to:
LInv-48	Physical characteristics
LInv-49	Fingerprints
LInv-50	Charges
LInv-51	Scars
LInv-52	Marks
LInv-53	Tattoos
LInv-54	Race
LInv-55	MO
LInv-56	Handicaps
LInv-57	User defined fields
LInv-58	An authorized user is able create random lineups of subjects drawn from search results.
LInv-59	An authorized user is able to create random lineups with user defined search criteria and in compliance with agency standards. (e.g. sequential photo lineup)
LInv-60	Searches can be limited to a single jurisdiction or search all jurisdictions.
LInv-61	Searches include master names.
LInv-62	Searches include businesses.
LInv-63	Searches include property type.
	The system can generate a crime analysis reports based on user-defined report criteria, such as, but not limited to:
LInv-64	Specific criminal activity
LInv-65	Offenses
LInv-66	MO
LInv-67	Entry/exit methods
LInv-68	Evidence collected
LInv-69	Location/scene
LInv-70	Hate/bias
LInv-71	Weapon used
	Law Enforcement Case Entry
LCseE-1	The system will apply user security to case entry, search and all incident related reports.
LCseE-2	The system can pull data from an existing incident record.
LCseE-3	The system will generate a notification or some other reference to any case number that is issued in the CAD module that requires a report (via Mobile upload or manual RMS entry).
LCseE-4	The system has the ability to flag a case as 'domestic related'.
LCseE-5	When a case is flagged as 'domestic related' the system will require specific mandatory domestic-related fields be completed by the user.



	The system links the case to:
LCseE-6	CAD incident
LCseE-7	Master name index
LCseE-8	Arrest data
LCseE-9	Property data
LCseE-10	Master vehicle index
LCseE-11	The system is able to accept entry of supplemental reports.
LCseE-12	The system is able to index case records by case number, which may be the same as the originating event (CFS) number.
LCseE-13	The system is able to accept and maintain case records on any type of incident or criminal activity.
LCseE-14	The system tracks multiple crimes within a single master case record.
LCseE-15	When name related information is entered into the module, it is updated in the master name file in RMS and triggers a notification to the system manager and/or records custodian.
LCseE-16	The system will cross-reference and link multiple related offenses to a specific case record via its case number.
LCseE-17	The system will cross-reference and link multiple related incident records to a specific case record via its case number.
LCseE-18	The system will allow direct access to any related incident via hyperlink or other direct access method from within the case and/or any related case record.
LCseE-19	The system will create a case record upon entry of the crime report data.
LCseE-20	The system allows the generation of year-based case numbers.
LCseE-21	The system has the ability for an authorized user to correct previously entered incident data in the case data entry screen.
	The system will accept and maintain the following case record data elements:
LCseE-22	Incident Type
LCseE-23	Occurred Location
LCseE-24	Hate Bias Information
LCseE-25	Criminal Activity
LCseE-26	Entry and Exit Methods/Points
LCseE-27	Date/Time of Occurrence
LCseE-28	Date of Reported Occurrence
LCseE-29	Multiple Crime/Offense Codes
LCseE-30	Type of Arson Reported
LCseE-31	Type of Theft Reported
LCseE-32	Status of the Complaint
LCseE-33	Disposition/Date of the Complaint
LCseE-34	Multiple MOs of the Crime
LCseE-35	Attempted Crime

[redacted]

LCseE-36	Type of Weapon	
LCseE-37	Type of Tool	
LCseE-38	Codes for the Type of Scene of the Crime	
LCseE-39	Officer's Bureau Assignment	
LCseE-40	Type of Stolen/Recovered Vehicle	
LCseE-41	Estimated Dollar Amount of Property Involved	
LCseE-42	Property Involved	
LCseE-43	Solvability Factors Associated with Complaint	
	The system will accept and maintain, at a minimum, the following domestic violence data elements associated with a case:	
LCseE-44	Injury type	
LCseE-45	Extent of injury	
LCseE-46	Sobriety of victim	
LCseE-47	Demeanor of victim	
LCseE-48	Length of relationship	
LCseE-49	Date relationship ended (if applicable)	
LCseE-50	Prior domestic violence victim	
LCseE-51	Number of calls to law enforcement	
LCseE-52	If Protective Order is in effect	
LCseE-53	Protective Order expired	
LCseE-54	Court issuing protective order	
LCseE-55	Order/Docket number	
LCseE-56	The system will accept and maintain detailed information about all offenses associated with a case.	
LCseE-57	The system will accept and maintain detailed information about all subjects associated with a case (e.g., arrested adults, juveniles, witnesses, complainants, missing persons, reporting party, victims).	
LCseE-58	The system will accept and maintain information about all arrests associated with a case.	
LCseE-59	The system will accept and maintain information about all field investigations associated with a case.	
LCseE-60	The system will automatically link all information from a field reporting record to the original case report.	
LCseE-61	The system will accept and maintain information about all vehicles associated with a case.	
LCseE-62	The system supports unlimited narrative input and editing capabilities for the original case report.	
LCseE-63	The system supports unlimited narrative input and editing capabilities for any type of supplemental report.	
LCseE-64	The system will capture crime analysis related information during case processing.	
LCseE-65	The system has the ability to expunge a subject from a case record.	
LCseE-66	Information from an incident record is automatically pulled into an associated case record to eliminate the need to enter the same data twice.	

[redacted]

LCseE-67	The system is able print hard copies of case records and supplemental reports, depending on security.
LCseE-68	The system is able to print a redacted version of a case record for public use.
LCseE-69	All entry information can be built into a report, which will plot on a map or generate a printable report.
LCseE-70	The system has the ability to generate multiple case related reports for statistical crime analysis.
LCseE-71	The system will support batch uploads and provide the ability to attach multiple supporting documents/files of various types (e.g., Word, Excel, PDF, WMA, JPG, MPG, WAV) to a case record. (The vendor will provide a list of file types supported for attachment by the system).
LCseE-72	A user defined description can be associated with each attached file.
LCseE-73	Case entry provides a mechanism to complete an NIBRS edit check from within the record at any time.
LCseE-74	Updates to case data update IBR-related information when applicable, and generates any updates that are required for NIBRS submissions.
LCseE-75	The system can generate a NIBRS edit list at any time.
LCseE-76	IBR edit lists reference the applicable case number and correction required based on imbedded NIBRS logic.
LCseE-77	The system will generate a report that references case numbers that have been issued via CAD and Field Reporting that do not have a corresponding report (i.e. still resident within field reporting or officer has not completed via the RMS system.)
LCseE-78	System security allows narrative access to be assigned to only specific individual users.
LCseE-79	System security allows narrative access to be assigned to only a specific group of users.
LCseE-80	The system shall allow any individual case report to be closed, where the report will then be visible only to those users who have authority to see closed records based on security settings.
LCseE-81	The system shall allow individual case elements to be marked "closed", where those elements are only visible to users who have authority to see closed records based on security settings.
LCseE-82	Relationship of victim to offender(s)
	Law Enforcement Case Management
LCseM-1	The system maintains a database of current cases and statuses.
LCseM-2	The system is able to use the module as a supervisory tool.
LCseM-3	The system allows an authorized user to assign or reassign officers to cases.
LCseM-4	The system provides edit check capabilities to ensure each case meets all entry requirements as defined by the agency.
	Items checked, at a minimum:
LCseM-5	Subject information
LCseM-6	Property information
LCseM-7	Offense information
LCseM-8	Arrest information
LCseM-9	The system will notify the user what edit check items are not met.
LCseM-10	At a minimum, the edit checks will meet the minimum requirements for submission to the State and Federal authorities, specifically, UCR or NIBRS data elements.
LCseM-11	At a minimum, the edit checks will meet the minimum requirements for submission to the State and Federal authorities, specifically NIBRS data elements.
LCseM-12	The system allows for agency-defined case activities (e.g., table driven coding).
LCseM-13	The system will have the ability to integrate case activities with commercial calendar applications (e.g., Microsoft Outlook).
	Case activity shall include, but not be limited to:

[redacted]

LCseM-14	Assigned Officer/investigator
LCseM-15	Activity type
LCseM-16	Activity date
LCseM-17	Activity time
LCseM-18	Free text narrative
LCseM-19	Status
LCseM-20	Status date
LCseM-21	The system accepts and maintains solvability factors.
LCseM-22	The system allows an authorized user to assign case activities to various personnel as required (e.g., property clerk, other investigator, supervisor).
LCseM-23	The system allows personnel to see all cases assigned to them based on log in.
LCseM-24	The system tracks case status history.
LCseM-25	The system tracks case disposition history.
LCseM-26	Case Management integrates with Crime Analysis module to produce comprehensive statistical reports.
LCseM-27	The system tracks assigned and unassigned cases.
	The system tracks cases by:
LCseM-28	Officer
LCseM-29	Squad
LCseM-30	Assigned bureau
LCseM-31	Activity type
LCseM-32	Activity officer
LCseM-33	Status
LCseM-34	Disposition
LCseM-35	The system provides case load reports by officer, supervisor, case status and activities.
LCseM-36	The sysem has the ability to sort cases by Type and/or Felony or Misdemeanor.
LCseM-37	The system allows personnel to assign activities to other officers/investigators.
	The system allows personnel to assign activities to others, including but not limited to:
LCseM-38	Domestic violence investigator
LCseM-39	Domestic violence unit
LCseM-40	The system can enable automatic e-mail notifications to appropriate personnel whenever a case is updated or a report is added to a case.
LCseM-41	The system can enable automatic e-mail notifications to appropriate personnel whenever the are assigned a case.
LCseM-42	The system can enable automatic e-mail notifications to appropriate personnel whenever the are assigned a case activity.
LCseM-43	The system provides a methodology that allows supervisors to review open, unassigned cases to make Officer/personnel assignments.

[redacted]

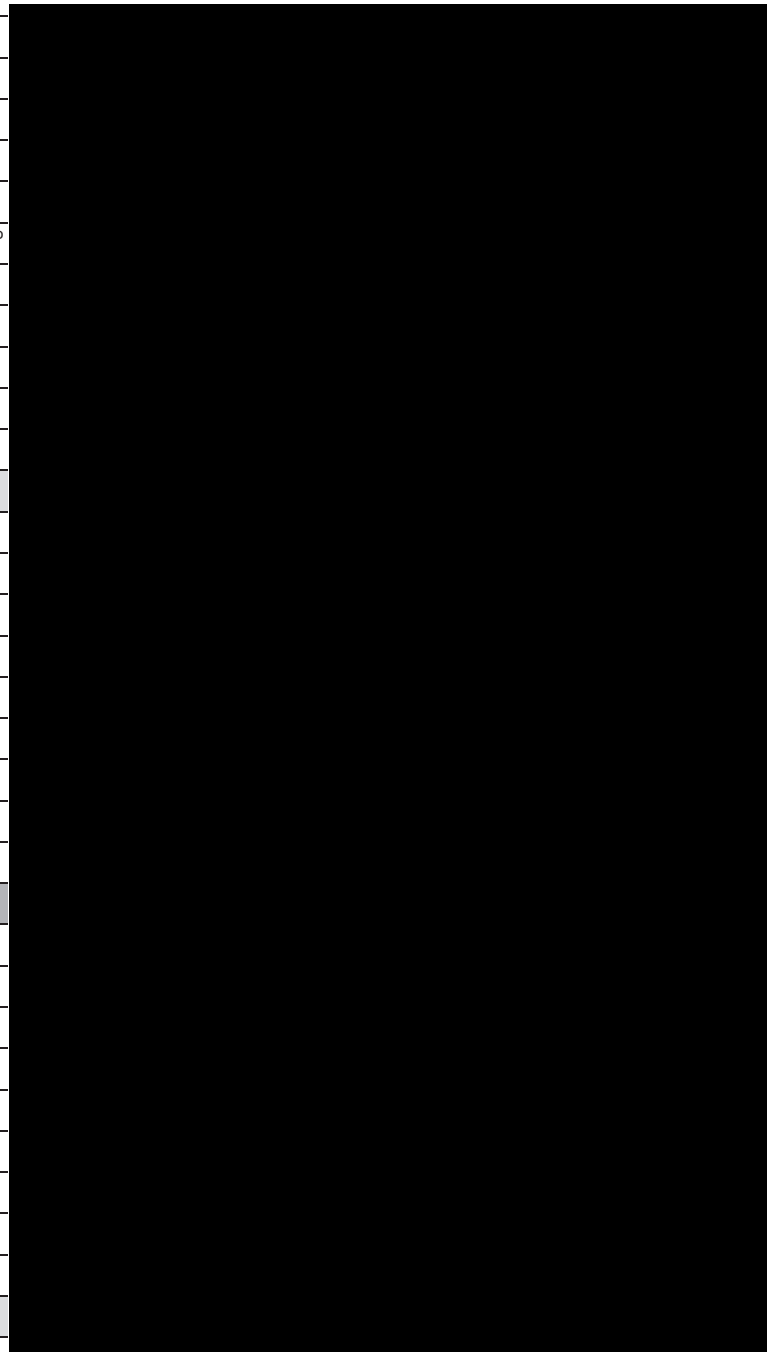
LCseM-44	The system allows a user to assign multiple dispositions to a single case.
	Law Enforcement Narcotics
LNarc-1	Authorized user access to the narcotics module and records are based on active directory permissions .
	Access to the narcotics module is logged, including at a minimum the following:
LNarc-2	Date
LNarc-3	Time
LNarc-4	Accessing User Information
LNarc-5	An authorized user has the ability to create and maintain agency-defined investigation types.
LNarc-6	An authorized user has the ability to create agency-defined investigation statuses.
LNarc-7	Investigation records are tied to a location and provide full access to location history.
LNarc-8	The system is able to tie an investigation to a case number and case ORI.
LNarc-9	The system manages associated assignments within the investigation record.
LNarc-10	The system tracks all investigation activities within the investigation record.
LNarc-11	The system is able to tie to associated intelligence records and other investigation numbers.
LNarc-12	The system is able to track an unlimited number of subjects with full access to their master name files and agency histories.
LNarc-13	The system is able to track subject activities.
LNarc-14	The system is able to tie an unlimited number of confidential informants to an investigation record.
LNarc-15	The system is able to track an unlimited number of associated vehicles.
LNarc-16	The system tracks all charges (pending or otherwise) associated with an investigation.
LNarc-17	The system tracks court information associated with a charge.
LNarc-18	The system tracks all drug buys, i.e., narcotics purchased during the course of the investigation.
LNarc-19	The system tracks all drug purchasing locations.
LNarc-20	The system tracks all monies used in drug buys.
LNarc-21	The system tracks all charges associated with a particular drug buy.
LNarc-22	The system documents all laboratory results tied to a drug buy.
LNarc-23	An authorized user can attach multiple supporting documents of various types to a drug buy record.
LNarc-24	The system tracks property associated with the investigation.
LNarc-25	An authorized user can attach unlimited supporting documents of various types to an investigation record.
LNarc-26	An authorized user is able to determine numbering system for investigation records, including optional auto-incrementing.
LNarc-27	The system is able to generate a variety of narcotics related reports to facilitate statistical analysis.
LNarc-28	An authorized user is able to create, maintain and track intelligence records associated with narcotics investigations.
LNarc-29	The system is able to tie a confidential informant to an intelligence record.

[redacted]

LNarc-30	The system can secure intelligence records and make them accessible to only those users with the proper Narcotics Management security permissions.
LNarc-31	The system has the capability for entry and maintenance of information about intelligence related payments.
	The system has the capability to tie intelligence to and define roles for the following:
LNarc-32	Person
LNarc-33	Location
LNarc-34	Vehicle
LNarc-35	Ensuing investigation
LNarc-36	An authorized user can attach unlimited supporting documents of various types to an intelligence record.
LNarc-37	The system has the capability to create, maintain and track separate records about confidential informants.
LNarc-38	The system has the capability to track all confidential informant activities.
LNarc-39	The system has the capability to document current confidential informant status.
LNarc-40	The system has the capability to document and track confidential informant reliability.
LNarc-41	The system has the capability to track all monies paid to a confidential informant.
LNarc-42	The system has the capability to attach multiple supporting documents of various types to a confidential informant record.
LNarc-43	The system is able to track all narcotics-related funds and transactions.
LNarc-44	The system is able to set user security permissions for all narcotics applications and reports.
LNarc-45	The system is able to share department-specific and designed information when approved by an authorized user.
	Law Enforcement Lineup / Mug Shot
	The image can be uploaded and stored from:
LMug-1	Direct connect with a digital camera
LMug-2	Computer hard drive
LMug-3	Standard scanned image file format (e.g., PDF, JPG)
LMug-4	USB drive
LMug-5	Other RMS modules
LMug-6	The Lineup / Mug Shot module is able to create photo lineups based on selected personal characteristics determined by the user, e.g., age, DOB, weight, DL number, SSN.
LMug-7	The Lineup / Mug Shot module is able to create photo lineups based on selected personal characteristics ranges as determined by the user.
LMug-8	The Lineup / Mug Shot module is able to generate photo lineups based on individuals selected by the user and in compliance with agency standards. (e.g., sequential photo lineup) .
LMug-9	The system provided the ability to save a photo lineup.
LMug-10	The system provides the ability to save the list of individuals used in the photo lineup.
LMug-11	The photo lineup can be attached to an incident record.
LMug-12	The system has the ability to store name information with each saved lineup image that originates from outside the RMS.
LMug-13	The system has the ability to print a lineup record to a hard copy.

[redacted]

LMug-14	The system has the ability to lock a lineup record for use in an investigation to only allow access by authorized user(s).
LMug-15	The system can produce a lineup using individual photographs to be presented to a witness for identification.
LMug-16	The system can build a six and eight image lineup.
LMug-17	The system can randomize the order of the images in the lineup, each time it is displayed.
LMug-18	The Lineup / Mugshot module does not allow multiple pictures of the same individual (historic photos) to be entered into a lineup.
LMug-19	The Lineup / Mugshot lineup utility enables a user to enter multiple search criteria at the same time, rather than only enabling them to search one field at a time.
LMug-20	The Lineup / Mugshot lineup utility fills the lineup with a randomly selected set of photos from the search, user-selected photos, or a combination of random and user selected.
LMug-21	The Lineup / Mugshot lineup utility allows the user to ensure a specific photo is included in the lineup.
LMug-22	The Lineup / Mugshot lineup utility is capable of exporting the line up images in common image formats.
LMug-23	An authorized user can specify the format for export of the line up image.
LMug-24	The system provides a list of photograph sizes where the photograph size can be selected by the user (selection is enabled by a button).
	Advanced Image Search capabilities include the ability to search on:
LMug-25	Partial information
LMug-26	Ranges
LMug-27	Field content
LMug-28	Like values
LMug-29	Greater than
LMug-30	Less than
LMug-31	Equal to
LMug-32	The search criteria includes: the description of the Lineup record; a range of dates; an Incident record to which the Lineup record is attached; created by and/or updated by.
LMug-33	The user is capable of flagging a Master Name and image from being displayed in the Lineup Search by selecting a remove image feature. The name and the image are no longer provided as an option for the search return of available candidates.
	Law Enforcement Property Processing
LProp-1	The Property Processing module is associated with all other modules of the system involving the reporting, custody and analysis of property.
LProp-2	The system has the ability to enter property/evidence into the property and evidence module without the need to complete the report first and then allows the import of that property into the report.
LProp-3	The system allows for property tag numbers to be an auto-incremented number generated by the system.
LProp-4	The ability to have the property tag number auto increment or be entered manually is agency-specific.
LProp-5	The system allows for agency defined tag number format (e.g., 123, 1A, 2A, case number-1, case number-2)
LProp-6	All transactions should have audit records as outlined under the Law RMS General tab.
LProp-7	The system needs to be able to complete analysis and audits within the system.
LProp-8	The system has the capability to capture electronic signatures.
LProp-9	The system has the capability to attach images of items to property records.
	The system is able to enter and maintain the following property data:



LProp-10	Item Number
LProp-11	Piece Number
LProp-12	Serial Number
LProp-13	Associated case number
LProp-14	Officer of initial custody
LProp-15	Property Code (e.g., stolen, pawned, evidence)
LProp-16	Property Tag Number
LProp-17	Owner Applied Number
LProp-18	Storage Location
LProp-19	Quantity
LProp-20	Value – Nearest Dollar
LProp-21	Property Owner
LProp-22	Date Property Received
LProp-23	Item Category (firearms, tools, vehicles, bicycles)
LProp-24	Lab Report Cross-Reference
LProp-25	Date of Disposal/Release
LProp-26	Employee Authorizing Release
LProp-27	Date Scheduled for Disposal/Destruction
LProp-28	Item Class (UCR)
LProp-29	Free-form Descriptions
LProp-30	Color
LProp-31	Recovered for other Jurisdiction Flag

The system is able to enter and maintain the following additional elements for firearms:

LProp-32	Firearm Serial Number
LProp-33	Firearm Type
LProp-34	Firearm Manufacturer (drop-down list)
LProp-35	Action (automatic, bolt action, carbine, pump)
LProp-36	Caliber
LProp-37	Shot Capacity
LProp-38	Barrel Length
LProp-39	Finish
LProp-40	Make/Model

[redacted]

LProp-41	Condition	
LProp-42	Year Made	
	The system is able to enter and maintain the following additional elements for boats:	
LProp-43	Boat Name	
LProp-44	Registration Number	
LProp-45	Registration State	
LProp-46	Registration Year	
LProp-47	Boat Manufacturer	
LProp-48	Hull Number	
LProp-49	Hull Shape	
LProp-50	Hull Type	
LProp-51	Hull Material	
LProp-52	Color	
LProp-53	Propulsion	
LProp-54	Boat Length	
LProp-55	Year of Manufacture	
LProp-56	Free-form Descriptions	
	The system is able to enter and maintain the following additional elements for vehicles:	
LProp-57	Vehicle Type	
LProp-58	Color (top, bottom, interior)	
LProp-59	Vehicle Year	
LProp-60	Vehicle Make	
LProp-61	Model	
LProp-62	License Plate/VIN	
LProp-63	License Plate State	
LProp-64	Plate Year	
	The system is able to enter and maintain the following information for bicycles:	
LProp-65	Bicycle Make	
LProp-66	Model (boys, girls, tandem)	
LProp-67	Serial Number	
LProp-68	Owner applied number (OAN)	
LProp-69	Wheel Size	

[redacted]

LProp-70	Speed
LProp-71	Color
LProp-72	The system can tie a property item to a case.
	The system is able to enter and maintain the following information for bank cards:
LProp-73	Banking/Institution that issued the card
LProp-74	Account number
LProp-75	Owner of the bank card
LProp-76	Expiration of the bank card
LProp-77	Disposition of the bank card (e.g., lost, stolen, etc.)
	Law Enforcement Property Room
LProp-78	The property room module will interface to bar coding (see bar code interface).
LProp-79	The system tracks items from receipt to disposal.
LProp-80	The system maintains complete evidence tracking (chain of custody) audit trail of property until final disposition of the item.
LProp-81	The system has an audit feature for the property room.
LProp-82	The system has an audit feature which includes an audit scan of items and will match the scan to data stored in the database.
LProp-83	The system is capable of printing the chain of custody audit trail for any/all items.
LProp-84	The system supports creation of multiple property rooms.
LProp-85	The system property room capabilities allow agency to define a minimum of four (4) levels of location definitions (i.e., Room 1, row 2, shelf 1, bin 5).
LProp-86	The system property room capabilities allow agency to define greater than four (4) levels of location definitions (i.e., Room 1, row 2, shelf 1, bin 5) to accommodate future growth and expansion.
LProp-87	Defined property locations become table driven (or drop down) values that are co-dependent of each other (i.e., When Room 1 is selected, second choice is only those rows that are defined for Room 1).
LProp-88	The system supports the creation of multiple property rooms for multiple jurisdictions.
	Additional chain of custody information will be maintained for each property item each time the item is moved or changes custody:
LProp-89	Current officer responsible for custody
LProp-90	Property location
LProp-91	Date / time of custody record update
LProp-92	Officer turning over custody
LProp-93	Date / time of item entry into State/NCIC
LProp-94	Date / time of item removed from State/NCIC
LProp-95	The system maintains details of all evidence retained in the property room for an indefinite amount of time.
LProp-96	The system maintains a disposition status for all evidence items after each item has been released.
LProp-97	The system has the capability to track batch moves and destruction of property.
LProp-98	The system has the capability to track batch moves and destruction of property for multiple cases.

LProp-99	The system maintains lab reports on fingerprint analysis
LProp-100	An operator can enter and maintain information about the individual or organization to which the property was released.
LProp-101	An operator can print an evidence inventory report by case number.
LProp-102	An operator can print a property disposition report for all disposed items.
LProp-103	An operator can generate a report of property scheduled to be disposed.
LProp-104	An operator can print a property purge reminder list of items to be released within a user-selected date range.
LProp-105	An operator can print a property purge reminder list of items to be released within a user-selected case disposition.
LProp-106	An operator can print a report displaying all items of property/evidence pertaining to a single report.
LProp-107	The system restricts inquiry access to property/evidence records based on assigned user rights.
LProp-108	At the time of entry, the system compares property records with previously entered property records (i.e., pawned, impounded, stolen, etc.).
	The system allows users to search for property based on the following search criteria:
LProp-109	Serial Number
LProp-110	Owner's Name
LProp-111	Property Tag Number
LProp-112	Case Number
LProp-113	Owner Applied Number
LProp-114	Make/Brand Name
LProp-115	Property Type/Kind
LProp-116	UCR Property Class
LProp-117	IBR Property Class
LProp-118	Vehicle Identification Number
LProp-119	Date range
LProp-120	Vehicle License Plate / Registration
	An operator can print barcodes for the following:
LProp-121	ORI
LProp-122	Officer
LProp-123	Disposition
LProp-124	Receiving and Release Status
LProp-125	Locations
LProp-126	An operator can print location labels by specific location or range.
LProp-127	An authorized user can set agency-defined label height, width and font size.

[redacted]

LProp-128	The system can print labels individually.
LProp-129	The system automatically generates property tag numbers.
	Evidence Lockers
LProp-130	The system shall have the ability for authorized users to enter property items into the system when they deliver those items to evidence lockers at various locations/substations.
LProp-131	The system should generate receipts for property entered at evidence locker locations.
LProp-132	The system should allow property room personnel to query what lockers/stations have property logged in for pick up from main RMS application (to allow property personnel to know what stations they need to go to for property/evidence pick up).
LProp-133	The system provides the ability to apply bar codes to the property being placed in the evidence locker.
	Lab Tracking
	The ability to track lab information on evidence submitted to labs, to include:
LProp-134	Chain of custody
LProp-135	Lab name
LProp-136	Lab Number (lab assigned number)
LProp-137	Date sent
LProp-138	Date returned
LProp-139	Results
LProp-140	Status
LProp-141	Status date
LProp-142	Attached narrative and other PC-based media (such as Word documents, images, scanned documents, PDF's etc.)
	Law Enforcement Impounded Vehicle Processing
	An authorized users is able to enter and maintain the details of an impounded vehicle, including the following general information:
LImpV-1	Impound Date/Time
LImpV-2	Impound Lot
LImpV-3	Reason for Impounding
LImpV-4	Place of Storage
LImpV-5	Location Impounded From
LImpV-6	Towing Service
LImpV-7	Impounding Officers
LImpV-8	Vehicle Information (e.g., make, model, color)
LImpV-9	Vehicle hold
LImpV-10	An authorized user can enter owner information based on master name file selection, if name is available.
LImpV-11	The system indicates owner notification date/time.
LImpV-12	The system accepts and maintains disposition information.

[redacted]

LImpV-13	The system accepts and maintains vehicle release information.
LImpV-14	The system tracks the time from the vehicle being impounding.
LImpV-15	The system will report the number of days that a vehicle has been impounded.
LImpV-16	The system will display vehicles with holds associated with them.
LImpV-17	The system accepts and maintains associated incident, case, arrest, warrant, and booking information.
LImpV-18	The system tracks associated fees.
LImpV-19	The system has the capability of attaching multiple supporting documents of various types to an impounded vehicle record.
	Law Enforcement Wants and Warrants
	The system has the ability to enter and maintain detailed information about want and warrant records, including (but not limited to) the following data elements:
LWant-1	File Transaction Number (internal warrant number)
LWant-2	Court Warrant Number
LWant-3	Court Case Number
LWant-4	User Defined Number
LWant-5	Subject name
LWant-6	Subject address
LWant-7	Subject alias(s)
LWant-8	Subject DOB
LWant-9	Subject Sex
LWant-10	Subject Race (drop down)
LWant-11	Subject Driver's License number
LWant-12	Subject Driver's License state
LWant-13	Subject telephone number(s)
LWant-14	Subject Social Security Number
LWant-15	Subject Employer
LWant-16	Subject vehicle make / model / color
LWant-17	Subject vehicle license plate / state / year
LWant-18	Issuing Court
LWant-19	Issuing Judge
LWant-20	Charges
LWant-21	Warrant Type (e.g., felony, misdemeanor)
LWant-22	Location of Warrant (original)
LWant-23	Bond amount

[redacted]

LWant-24	Disposition (e.g., served, returned un-served)
LWant-25	Agency defineable status (e.g., active, inactive, unservable)
LWant-26	Status History
	All service activity (e.g., service attempts), including but not limited to:
LWant-27	Date
LWant-28	Time
LWant-29	Officer ID
LWant-30	Activity type
LWant-31	Free text narrative
LWant-32	Warning remarks
LWant-33	Background narrative, if applicable
LWant-34	Beat/zone/section within warrant venue
LWant-35	Reason for change on warrant, if applies
LWant-36	Extradition approved
LWant-37	Distance of pickup
LWant-38	The system displays a photo of the subject within the want/warrant record, if available.
LWant-39	A photo image can be loaded and stored via direct connect with a digital camera.
	The photo image can be uploaded from:
LWant-40	Digital camera (TWAIN compliant)
LWant-41	Computer disk
LWant-42	TWAIN complaint standard scanned image file format (e.g., JPG)
LWant-43	USB drive
LWant-44	Embedded email
LWant-45	Embedded text message
LWant-46	The system can display an alert whenever the name of a subject with an outstanding warrant is entered anywhere in the system.
LWant-47	Authorized users are able to update the status of a warrant record whenever necessary.
LWant-48	The system is able to assign an incremental warrant transaction numbers automatically.
LWant-49	A printed report can be generated displaying a log of all warrants within a specified date range.
LWant-50	Authorized users have the ability to cancel outstanding warrant records. Authorization is based on user security profiles (ID, password, security permissions) for example, warrants served.
	Outstanding warrants may be cancelled for the following reasons:
LWant-51	Recalled by Court or other jurisdiction
LWant-52	Served on the person

[redacted]

LWant-53	Cleared of the charge
LWant-54	Beyond statutory limits
LWant-55	Received/transferred to
LWant-56	Records on canceled warrants can be maintained for an unlimited amount of time.
LWant-57	Records on canceled warrants include reason for cancellation and date of cancellation.
	The system allows warrants to be automatically searched from CAD based on the entry of matching name and/or matching address and display, at a minimum:
LWant-58	Warrant status
LWant-59	Wanted person demographics
LWant-60	Location of Warrant (original)
LWant-61	Warnings
LWant-62	In CAD, when warrants are automatically searched based on the entry of matching name and/or matching address, a resulting match on either of these search criteria will display a message for the user.
LWant-63	A printed report can be generated that lists all canceled warrants within a specified date range.
LWant-64	A printed warrant summary report can be generated that lists all warrant types and totals within a specified date range.
LWant-65	Ability to update a warrant's status from the mobile data.
	Law Enforcement Arrest Records
	The system accepts and maintains the following arrest information:
LArst-1	Arrest Number
LArst-2	Date/Time of Arrest
LArst-3	Arrest Type
LArst-4	Charge(s)
LArst-5	Associated Case Number
LArst-6	Location of Arrest
LArst-7	Name of Arrested Person
LArst-8	Alias (unlimited)
LArst-9	Scars, Marks and Tattoos (unlimited descriptions)
LArst-10	Arresting Officer (multiple possible)
LArst-11	Arresting Officer's unit/team
LArst-12	Reporting Districts of the Arrest
LArst-13	Assisting Arrest Officer
LArst-14	Disposition of the Arrest

[redacted]

LArst-15	Disposition Date
LArst-16	On data entry, prior to assigning an arrest number, the system will search existing arrest records using the Master Name dataset for existing arrest records. If existing records are found, the system will message the operator to use either the prior arrest number for that arrestee, or generate a new arrest number
LArst-17	The system accepts and maintains information about all charges associated with the arrest.
LArst-18	The system accepts and maintains data on arrest and court dispositions.
LArst-19	The system links arrests to cases.
LArst-20	The system can link multiple arrests to a single case.
LArst-21	The system can link an arrest to multiple cases.
LArst-22	The system accepts and maintains information about injuries the arrestee may have sustained while being apprehended within the Use of Force module/report.
LArst-23	The system accepts and maintains information about weapons involved in the arrest.
LArst-24	The system is integrated with Booking module, allowing subject data to be transferred into the Booking module from a related arrest.
LArst-25	The system is integrated with Booking module, allowing offense data to be transferred into the Booking module from a related arrest for use with Booking charges.
	The system accepts and maintains information about identification numbers associated with the arrest, including, not limited to:
LArst-26	Booking number
LArst-27	Case number
LArst-28	Warrant number
LArst-29	Offender-based tracking system number
LArst-30	The system maintains and reports information per NIBRS requirements.
LArst-31	The system maintains and is able to report information in the legacy UCR Summary format.
LArst-32	The system links newly arrested individuals to previous arrests, if applicable.
LArst-33	If one does not already exist, the system automatically create a master name record at the time of the arrest processing.
LArst-34	The system has access to an arrest register within a selected date range.
LArst-35	An arrest record can be added at the time of the original case report.
LArst-36	An arrest record can be added at any time after the original case report.
LArst-37	In the event of an arrest at a later date, the system is able to add additional supplemental narrative to the original case report.
LArst-38	The system has the ability to flag or otherwise indicate that an arrest is a 'juvenile'.
LArst-39	When a juvenile record is accessed, the system triggers an alert to the user.
LArst-40	The system has the ability to flag an arrest as 'domestic related'.
	The system can search for arrest records based on the following criteria:
LArst-41	Arrestee's Name
LArst-42	Arrest Location
LArst-43	Arrest Area (District, Beat, Reporting Area)
LArst-44	Arrest Date/Range

[redacted]

LArst-45	Complaint Incident Number
LArst-46	Complaint Case Number
LArst-47	Complaint Offense Type
LArst-48	Arresting Officer ID
LArst-49	Arrest Tracking Number
LArst-50	Scars, Marks and Tattoos
LArst-51	Aliases
	The system can print a variety of arrest related reports to facilitate the statistical analysis or arrest data, including the following:
LArst-52	Arrest by Court Disposition Date Report
LArst-53	Arrest by Location Report
LArst-54	Arrest by Officer Report
LArst-55	Arrest Charge Summary Report
LArst-56	Arrest Detail Report
LArst-57	Arrest Register Report
LArst-58	Arrest Status Summary Report
LArst-59	The system provides equivalent reports for both juvenile and adult arrest records.

Law Enforcement Field Interview

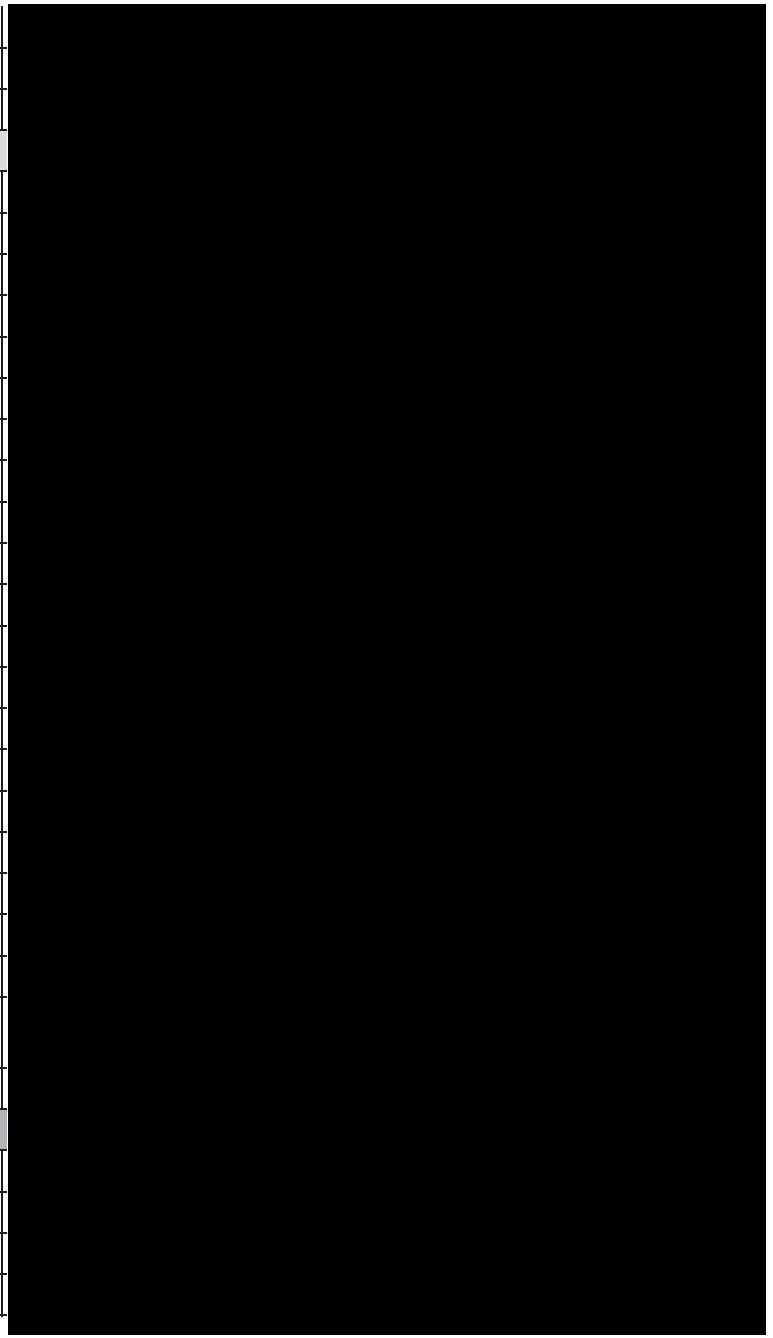
LFIdI-1	The Field Interview module can be accessed and updated from a mobile data device.
LFIdI-2	The system is capable of associating an investigation to a specific case.
LFIdI-3	The system is capable of an interface with a third-party Field Interview module (e.g., Delta Plus).
	The system maintains the following basic contact information:
LFIdI-4	Contact date/time
LFIdI-5	Contact type
LFIdI-6	Subject Name
LFIdI-7	Contact reason
LFIdI-8	Location
LFIdI-9	Ability to add multiple contacts
LFIdI-10	Ability to add subject vehicle
LFIdI-11	Ability to add multiple subject vehicles
LFIdI-12	The system accepts and maintains information sources (e.g., rumors, anonymous tips, confidential informants, first-hand accounts from a law enforcement personnel).
	The system will accept and maintain data from an external source, at a minimum:
LFIdI-13	Subject Name

[redacted]

LFldI-14	Location of encounter
LFldI-15	Narrative
LFldI-16	Images
LFldI-17	Videos
	Documents that were received as attachments, such as:
LFldI-18	Text (e.g., Rich Text)
LFldI-19	MS Word
LFldI-20	PDF
LFldI-21	The system has the ability to close any investigation record to allow access only to specified authorized users.
LFldI-22	The system will associate an investigation with a specific bureau.
LFldI-23	The system will associate an investigation with a specific reporting district.
LFldI-24	The system can identify a contact by master name.
LFldI-25	The system can identify a contact by associated case subject.
LFldI-26	The system will accept and maintain contact vehicle information.
LFldI-27	The system will accept maintain all officers associated with the investigation.
LFldI-28	The system is able to attach multiple document of various types to an investigation record.
LFldI-29	The system is able to link or group all known associates at a given criminal location.
LFldI-30	The Field Investigations record can be searched and sorted by any field of the record.
LFldI-31	The system can generate any report using a report wizard.
LFldI-32	The system allows report data to be exported in ASCII, delimited format.
LFldI-33	The system allows a report to be converted to PDF format.
	The system is able to track field investigations by:
LFldI-34	Contact type
LFldI-35	Case number
LFldI-36	Vehicle
LFldI-37	Contact reason
LFldI-38	Date/date range
LFldI-39	Field investigation number
LFldI-40	Investigating officer
LFldI-41	Contact name
LFldI-42	Location
Law Enforcement Orders of Protection	

[redacted]

LOrProt-1	The system has the ability to create, maintain and track Orders of Protection records.
LOrProt-2	The system has the ability to automatically generate system-wide alerts when a defendant is defined and the order record saved.
LOrProt-3	The system provides CAD alert information when location for an event is a location that is part of an Order of Protection.
	The system tracks the following basic order of protection details:
LOrProt-4	Issued date
LOrProt-5	Expiration date
LOrProt-6	Court date
LOrProt-7	NCIC number
LOrProt-8	Status (e.g. active, expired, served)
LOrProt-9	Date served
LOrProt-10	Type (agency defineable table)
LOrProt-11	Narrative
LOrProt-12	The system has the ability to create and maintain information on all subjects associated with an order, including each subject's role and relationship to the complainant or petitioner.
LOrProt-13	The system has the ability to generate a report of activity related to the serving of reports for a time period determined by an authorized user, which include:
LOrProt-14	Names of Subjects served
LOrProt-15	Names of Subjects yet to be served
LOrProt-16	The system has the ability to access the department history of all involved parties from the master name index.
LOrProt-17	The system has the ability to accept and maintain information about all the locations from which defendants are restricted.
LOrProt-18	The system documents associated agency and court case numbers.
LOrProt-19	The software provides the ability to document issuing judge.
LOrProt-20	The system has the ability to accept and maintain the terms of orders of protection.
LOrProt-21	The system has the ability to enter and maintain information about the cancellation of orders of protection.
LOrProt-22	The system has the ability to enter and maintain information about all activities associated with an order.
LOrProt-23	The system has the ability to enter and maintain information about court ordered remedies.
LOrProt-24	An authorized user can generate NCIC queries and display query responses from within the Orders of Protection module.
LOrProt-25	The system has the ability generate department-specific reports on any captured table/data field.
	Law Enforcement License, Permits and Billing
LPerm-1	The License and Permit module can be accessed from CAD.
LPerm-2	The License and Permit module can be accessed from a mobile device.
LPerm-3	Names entered through the License and Permits module will associate the names into the Master Name Index.
LPerm-4	The License and Permit module can be accessed from the RMS module.



LPerm-5	The locations maintained in the License and Permit module can be displayed using a GIS mapping capability.	
LPerm-6	The License and Permit module will interface with the permitting system.	
	Permits	
LPerm-7	The system is able to track and issue permits.	
	The system can capture and maintain the following permit information, including:	
LPerm-8	Permit number	
LPerm-9	Permit type	
LPerm-10	Permit status	
LPerm-11	Permit status date/time	
LPerm-12	Application date	
LPerm-13	Permit issue date	
LPerm-14	Permit expiration date	
LPerm-15	Permit holder name	
LPerm-16	Permit holder address	
LPerm-17	Permit holder telephone number	
LPerm-18	Business name	
LPerm-19	Business address or location	
LPerm-20	Event name	
LPerm-21	Event type	
LPerm-22	Permit rejection / revocation date	
LPerm-23	Permit rejection / revocation reason	
LPerm-24	Permit rejection / revocation resolution	
LPerm-25	Date reapplied	
LPerm-26	Fee date	
LPerm-27	Fee (dollar value collected)	
LPerm-28	The system has the ability to view permit status history.	
LPerm-29	The system allows the agency to create and maintain permit types, e.g., burning permit, solicitation permit.	
LPerm-30	The system allows the permit to be associated with a person or a business.	
LPerm-31	The system allows the permit to be associated with a business address or business location.	
LPerm-32	The system is able to attach multiple supporting documents of various types to a permit record.	
LPerm-33	The system has the ability to print the permit in a format determined by the agency.	

LPerm-34	The system has the ability to print a photo on the permit		[redacted]
LPerm-35	The system has the ability to print permits using various, selectable formats.		
	Licenses		
LPerm-36	The system is able to track and issue licenses.		
	The system can capture and maintain the following license information, including:		
LPerm-37	License number		
LPerm-38	License type		
LPerm-39	License status		
LPerm-40	License status date/time		
LPerm-41	License application date		
LPerm-42	License issue date		
LPerm-43	License expiration date		
LPerm-44	Business name		
LPerm-45	Business address or location		
LPerm-46	License holder name		
LPerm-47	License holder address		
LPerm-48	License holder telephone number		
LPerm-49	License holder photograph		
LPerm-50	Permit rejection / revocation date		
LPerm-51	Permit rejection / revocation reason		
LPerm-52	Permit rejection / revocation resolution		
LPerm-53	Date reapplied		
LPerm-54	Fee date		
LPerm-55	Fee (dollar value collected)		
LPerm-56	The system has the ability to view license status history.		
LPerm-57	The system is able to attach a picture of the license holder to the license record.		
LPerm-58	The system is able to attach multiple supporting documents of various types to a license record.		
LPerm-59	The system has the ability to print the license in a format determined by the agency.		
LPerm-60	The system has the ability to print a License ID in the form of an ID badge incorporating the photo and license record information.		

LPerm-61	Ability to capture electronic signatures.
	Law Enforcement Bar-Coding Interface
LBarC-1	System is capable of expansion to accommodate potential for future additional scanners, printers, property intake locations, etc.
LBarC-2	The system will allow a user profile to recognize/assign more than one peripheral device.
LBarC-3	The system utilizes bar code interface with the Fixed Asset, distributed property, and inventory modules of the selected LERMS system.
LBarC-4	The system generates bar code labels when checking in evidence/property.
LBarC-5	The system is able to use portable/wireless bar code scanner to update evidence/property locations and upload results into main database.
LBarC-6	The system is able to upload data from hand-held scanner via cradle mechanism.
LBarC-7	The system is able to upload data from hand-held scanner via wireless system access.
LBarC-8	The system is able to generate bar code labels in the field.
LBarC-9	The system is able to complete/maintain inventory with bar code system.
LBarC-10	Bar code labels recommended are smear-proof.
LBarC-11	Bar code labels recommended are of significant strength as to resist wear, ripping, fading, tearing and is tamper proof.
LBarC-12	The system is able to print page(s) of bar code labels to apply in the field.
LBarC-13	The system is able to use paper (or equivalent) bar code labels.
LBarC-14	The system is able to use 3 dimensional bar code tags.
	The barcode module is able to print barcodes for:
LBarC-15	ORI or Agency Code
LBarC-16	Officer
LBarC-17	Disposition
LBarC-18	Receiving and Release Status
LBarC-19	Locations
LBarC-20	The barcode module prints location labels by specific location or by range.
LBarC-21	The barcode module is able to produce labels in agency-defined label height, width and font size.
LBarC-22	The barcode module is able to differentiate between evidence and assets.
LBarC-23	The system provides a means to print a bicycle registration bar code label.
LBarC-24	The system provides a means to print a bicycle inspection bar code label.
LBarC-25	The barcode module is able to print single/individual labels.
LBarC-26	The barcode module is able to automatically generate tag numbers.
LBarC-27	The barcode module can automatically enter a transaction when a tag is scanned.
	Law Enforcement Fleet Maintenance
LFM-1	The system tracks department vehicles by department-specific vehicle type.

[redacted]

LFM-2	The system tracks department vehicles by department-issued unit number.
LFM-3	The system associates a vehicle with an inventory number.
	The system accepts and maintains purchase information, including the following:
LFM-4	Purchase date
LFM-5	Individual or business from whom the vehicle was purchased
LFM-6	Original cost
LFM-7	Received date
LFM-8	First in service date
LFM-9	Scheduled replacement date
LFM-10	The system indicates the vehicle's current status and the date the status was set.
LFM-11	The system flags a vehicle as in/out of service.
	The system accepts and maintains the following basic vehicle information:
LFM-12	Make and model (model ties make)
LFM-13	Model year
LFM-14	Color
LFM-15	VIN
LFM-16	License plate
LFM-17	License plate state
LFM-18	Vehicle style
LFM-19	Description (free-form narrative)
LFM-20	Special Equipment (user defineable drop-down list).
	The system can assign a vehicle to a:
LFM-21	Station
LFM-22	Division
LFM-23	Unit number
LFM-24	Location
	The system is able to document the following information about vehicle size:
LFM-25	Height
LFM-26	Width
LFM-27	Length
LFM-28	Gross Vehicle Weight Rating (GVWR)
LFM-29	Wheel base

[redacted]

	The system tracks the following information about operation specifications:
LFM-30	Turn radius
LFM-31	Maximum altitude
LFM-32	Maximum grade
LFM-33	The system tracks information about air temperature range.
	The system tracks the following engine information:
LFM-34	Manufacturer
LFM-35	Model
LFM-36	Serial number
LFM-37	Oil type
LFM-38	Fuel type
LFM-39	Fuel tank capacity
LFM-40	Misc. Engine Size (e.g. 3.8L)
LFM-41	Number of cylinders
LFM-42	Horsepower
LFM-43	Transmission Type
	The system tracks the following battery information:
LFM-44	Manufacturer
LFM-45	Model
LFM-46	Capacity
LFM-47	Installation date
	The system tracks the following vehicle electrical system requirements:
LFM-48	Number of volts
LFM-49	Output in amperes
LFM-50	The system tracks any tanks the vehicle may contain.
	The system tracks the following vehicle tank information:
LFM-51	Type
LFM-52	Capacity
LFM-53	Installation date
LFM-54	The system tracks tire information.
	The system tracks the following tire information:
LFM-55	Make

[redacted]

LFM-56	Model
LFM-57	Type
LFM-58	Size
LFM-59	Pressure
LFM-60	Installation date
LFM-61	The system tracks department-specific vehicle activities.
LFM-62	The system will schedule a vehicle for any type of maintenance.
LFM-63	The system tracks a vehicle's maintenance history.
LFM-64	The system tracks vendors that have performed maintenance on a vehicle.
LFM-65	The system tracks vehicle maintenance costs.
LFM-66	The system records a vehicle's fuel and oil usage.
	The system will generate the following vehicle related reports:
LFM-67	Vehicle Detail Report
LFM-68	Vehicle Fuel/Oil Usage
LFM-69	Vehicle Listing
LFM-70	Vehicle Maintenance Schedule Report
LFM-71	The system has the ability to attach supporting documents to a vehicle record.
	Law Enforcement Personnel and Training
LPT-1	The system has the ability to display, store and print a photograph of an employee within the personnel record.
LPT-2	The system has the ability to capture an image with a digital camera for the purpose of storage with an employee record.
LPT-3	The system has the ability upload an image from a camera, computer disk or any standard scanned image file format (e.g., PDF, JPG)
LPT-4	The system supports Personnel and Training module access security at the user level.
LPT-5	The system has the ability to interface to a third-party personnel/training product (e.g., Skills Manager).
	The system has the ability, at a minimum, to enter and maintain the following general personnel information on every employee:
LPT-6	Employee Full Name
LPT-7	Employee Address
LPT-8	Employee Badge and/or ID Number
LPT-9	Jurisdiction
LPT-10	Home Phone Number

[redacted]

LPT-11	Cell Phone Number	
LPT-12	E-mail addresses	
LPT-13	Department Number and Extension	
LPT-14	Date of Birth	
LPT-15	Place of Birth	
LPT-16	Current Rank	
LPT-17	Rank History	
LPT-18	Hire Date	
LPT-19	Termination Date	
LPT-20	Education, including Degrees, Certifications	
LPT-21	Payroll information	
LPT-22	Special Skills	
LPT-23	Department Injuries	
LPT-24	Blood Type	
LPT-25	Emergency Notification Information	
LPT-26	Employee Status or Promotions	
LPT-27	Reprimands	
LPT-28	Commendations	
LPT-29	Spouse’s Name	
LPT-30	Driver’s License Number	
LPT-31	Employee Demographic Information	
LPT-32	Disciplinary Actions	
LPT-33	Contact Information	
LPT-34	The system has the ability to associate additional security with stored fields of the personnel information, which include, at a minimum	
LPT-35	Reprimands	
LPT-36	Disciplinary Actions	
LPT-37	The data fields assigned additional security will be visible and accessible by authorized personnel only.	
LPT-38	The system has the ability to enter and maintain information about an employee's current assignment.	
LPT-39	The system has the ability to enter and maintain history of an employee's assignments.	
LPT-40	The system has the ability to upload and maintain copies of employee certificates.	
	The system provides the ability to export data contained in the personnel file to one of the following supported formats:	

LPT-41	Excel
LPT-42	XML
LPT-43	CSV
LPT-44	PDF
LPT-45	Text
	The system has the ability to track information about the equipment issued to each employee, including the following:
LPT-46	Item Type
LPT-47	Quantity
LPT-48	Inventory Number
LPT-49	Date Issued
LPT-50	Condition of Item
LPT-51	Returned Date
LPT-52	Condition Returned
LPT-53	Ability to capture electronic signatures.
	The system has the ability to track information about the training/certifications of personnel, including the following:
LPT-54	Courses (e.g., Firearms Training, Hazmat Technician Training)
LPT-55	In-house training courses
LPT-56	Programs
LPT-57	Certifications
LPT-58	Automatically Re-Schedules Re-Certification Classes
LPT-59	Basic Academy Training
LPT-60	Military Training
LPT-61	College Classes
	The system maintains the following training related data elements:
LPT-62	Employee ID Number
LPT-63	Training Course Title
LPT-64	Training Location

[redacted]

LPT-65	Re-certification Date
LPT-66	Length of the Course
LPT-67	Course Completion Date
LPT-68	Course Comments
LPT-69	Course Expenses
LPT-70	College Credit Hours
	Ability to enter and maintain information about any special skills an employee may have, including, but not limited to:
LPT-71	Foreign Language
LPT-72	Public Relations Training
LPT-73	Bomb Disposal Training
LPT-74	First Aid Training
LPT-75	SWAT Training
LPT-76	Breathalyzer Training
LPT-77	Other Agency-defined skills
LPT-78	The system provides the ability to schedule training by individual or group
LPT-79	The system provides the ability to print a summary report detailing all employees and all training conducted within a specified date range.
LPT-80	The system provides the ability to print a summary report detailing the certification level of each officer (i.e., intermediate, advanced, master)
LPT-81	The system provides the ability to print a summary report of all training received by an employee during his/her course of employment
LPT-82	The system provides the ability to print a detailed employee report with all fields of data in the personnel record.
LPT-83	The system provides the ability to print a summary department personnel listing sorted by Employee Name.
LPT-84	The system provides the ability to print a detailed department personnel listing sorted by Employee Name.
	Training
LPT-85	The system has the ability to create and maintain records on all the training courses for which personnel can register.
LPT-86	The system displays and prints a summary report of individual instructor hours by class, for a user-defined date range.

[redacted]

LPT-87	The system displays and prints the personnel that are currently scheduled for classes.
LPT-88	The system displays and prints the personnel that have completed the selected training.
LPT-89	The system displays and prints a summary report of individual instructor hours by class type (e.g. Use of Force) for a user-defined date range.
LPT-90	The system will have the ability to display and print class rosters.
	Ability to display and print class roster information including:
LPT-91	Date for each class/program
LPT-92	List of all participants, station/shift
LPT-93	Grade information
LPT-94	Instructor name
	Ability to print and display rosters for:
LPT-95	Certified classes
LPT-96	College unit classes for credit
LPT-97	Firearm certification with weapon type (e.g., handgun, rifle, shotgun)
LPT-98	SWAT certification
LPT-99	State or national academy classes
LPT-100	Seminars
LPT-101	FBI certification
LPT-102	The system will have the ability to print a summary of training.
LPT-103	The system automatically updates individual training record based on recorded course results.
LPT-104	The system alerts supervisors of training deficiencies (e.g., failed or missed class).
LPT-105	An authorized user can manually add previously attended training courses.
LPT-106	An authorized user can manually add previously attained certifications.
LPT-107	An authorized user can manually add previously attained qualifications.
LPT-108	The system links the course / certification / program information and each individual personnel / training record.
	The system has the ability to enter and maintain the following basic information for each course:
LPT-109	Course Title
LPT-110	Category
LPT-111	Keyword

[redacted]

LPT-112	Description
LPT-113	Active/Inactive
LPT-114	Instructor
LPT-115	Certification achieved
LPT-116	Recertification Period
LPT-117	Recertification Units (e.g.,Mandatory In-service Retraining)
LPT-118	Equivalent Courses
	The system has the ability to enter and maintain course information regarding hours and default provider, including the following:
LPT-119	Duration
LPT-120	Units
LPT-121	Number of Days
LPT-122	Credit Hours
LPT-123	Other
LPT-124	Default Provider Name, Address and Phone
	The system has the ability to enter and maintain course information regarding default costs, including the following detail:
LPT-125	Expense Type
LPT-126	Amount
LPT-127	General Ledger Account
LPT-128	Percentage
	The system has the ability to view course history and the scheduling of a given course, including the following information:
LPT-129	Course Title
LPT-130	Category
LPT-131	Start Date/Time
LPT-132	End Date/Time
LPT-133	Provider
LPT-134	Address
LPT-135	Location
LPT-136	Phone Number
LPT-137	The system has the ability to create and maintain course objectives.
LPT-138	The system has the ability to attach multiple supporting documents of various types to each course record.
LPT-139	The system has the ability to upload supporting documents and attach to each course record.
	The system has the ability to search for existing course records based on the following user-defined search criteria:

[redacted]

LPT-140	State Agency ID
LPT-141	Course Code
LPT-142	Title
LPT-143	Category
LPT-144	Keyword
LPT-145	Active/Inactive/All
LPT-146	Program
LPT-147	The system has the ability to create, maintain and track scheduled course records, i.e., schedules for individual courses.
	The system has the ability to enter and maintain the following basic information for each scheduled course record:
LPT-148	Start Date/Time
LPT-149	End Date/Time
LPT-150	Provider
LPT-151	Course Required/Not Required
LPT-152	Course
LPT-153	Course Location
LPT-154	Address
LPT-155	Phone Number
LPT-156	Activity Code
LPT-157	Days of the Week
LPT-158	Class Format
LPT-159	Training Type
LPT-160	Level of Training
LPT-161	Remarks (free-form narrative)
	The system has the ability to enter and maintain the following cost related information for each scheduled course record:
LPT-162	Expense Type
LPT-163	Amount
LPT-164	General Ledger Account
LPT-165	Percentage
LPT-166	The system has the ability to indicate all subjects associated with the scheduled course, including instructor and attendees.
	The system provides the ability to select scheduled course attendees by entering any of the following:
LPT-167	Employee ID
LPT-168	Individual personnel subjects

[redacted]

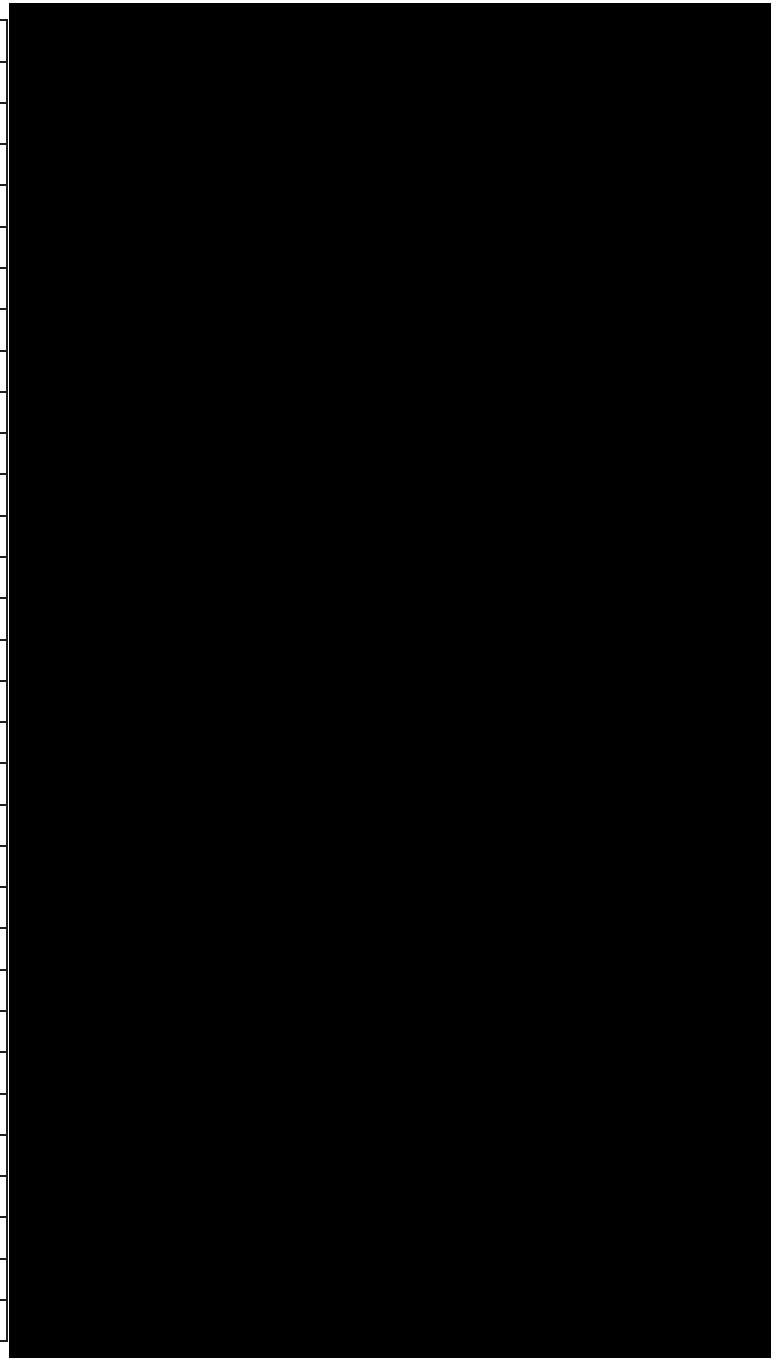
LPT-169	Linking to master name files
LPT-170	Entering names in free-form narrative
LPT-171	Group, e.g., station, shift, unit, employment classification, certification level.
LPT-172	Individuals from group lists can be selected for inclusion or exclusion.
LPT-173	The system provides the ability to enter and maintain information about the registered attendees' course results (grade/score).
LPT-174	The system provides the ability to see at-a-glance all of the objectives associated with a current scheduled course.
LPT-175	The system provided the ability to track which objectives have been completed by which attendees.
LPT-176	The system has the ability to attach multiple supporting documents of mixed types to each scheduled course record.
	The system searches for existing scheduled course records based on the following user-defined search criteria:
LPT-177	Employee ID
LPT-178	Course Code
LPT-179	Course Number
LPT-180	Provider
LPT-181	Location
LPT-182	Instructor
LPT-183	Program
LPT-184	Course Start Date/Time Range
LPT-185	The system has the ability to create, maintain and track training program records.
LPT-186	The system can associate multiple required courses with a training program or certification program.
LPT-187	The system can perform a mass enrollment where multiple personnel can be assigned to a single class.
LPT-188	The system can perform a mass enrollment where a group can be assigned to a single class.
LPT-189	The system can print class rosters in a format determined by the agency.
LPT-190	The system can print a certification program status report in a format determined by the agency.
LPT-191	The system can print personnel recertification status reports in a format determined by the agency.
LPT-192	The system will send automatic alerts/reports on pending certification expirations via e-mail.
LPT-193	The system can print ad hoc reports as determined by the agency.
LPT-194	The system shall provide an automatic message to an applicant notifying acceptance or rejection into a class.
LPT-195	The system shall provide for an electronic web based class registration process for each employee, including sign off information by their supervisor.

[redacted]

LPT-196	The system allows for training requests to be submitted via mobile and uploaded to personnel record upon approval of supervisor.
LPT-197	The system integrates with commonly available calendar applications (e.g., Microsoft Outlook).
LPT-198	The system will interface with a Law Enforcement training tracking application.
	The system provides the ability to export data contained in the training file to one of the following supported formats:
LPT-199	Excel
LPT-200	XML
LPT-201	CSV
LPT-202	PDF
LPT-203	Text
	Law Enforcement Pursuit
LPur-0	The System will include the capability of generating a Pursuit report.
LPur-1	If a pursuit is indicated during data entry in other modules, automatic and mandatory completion of a Pursuit report should occur.
LPur-2	The system will generate a Pursuit report form using data entered.
	The system allows for the collection of the following information related to the Pursuit report:
LPur-3	Case number
LPur-4	Control number
LPur-5	Pursuit date
LPur-6	Pursuit day of the week
LPur-7	Pursuit time occurred
LPur-8	Primary pursuit unit
LPur-9	Secondary pursuit unit
LPur-10	Location pursuit engaged
LPur-11	Location pursuit terminated
LPur-12	Total length of pursuit (miles or blocks)
LPur-13	Duration of pursuit (minutes)
LPur-14	Weather conditions narrative
LPur-15	Road/surface conditions narrative
LPur-16	Vehicle speeds

[redacted]

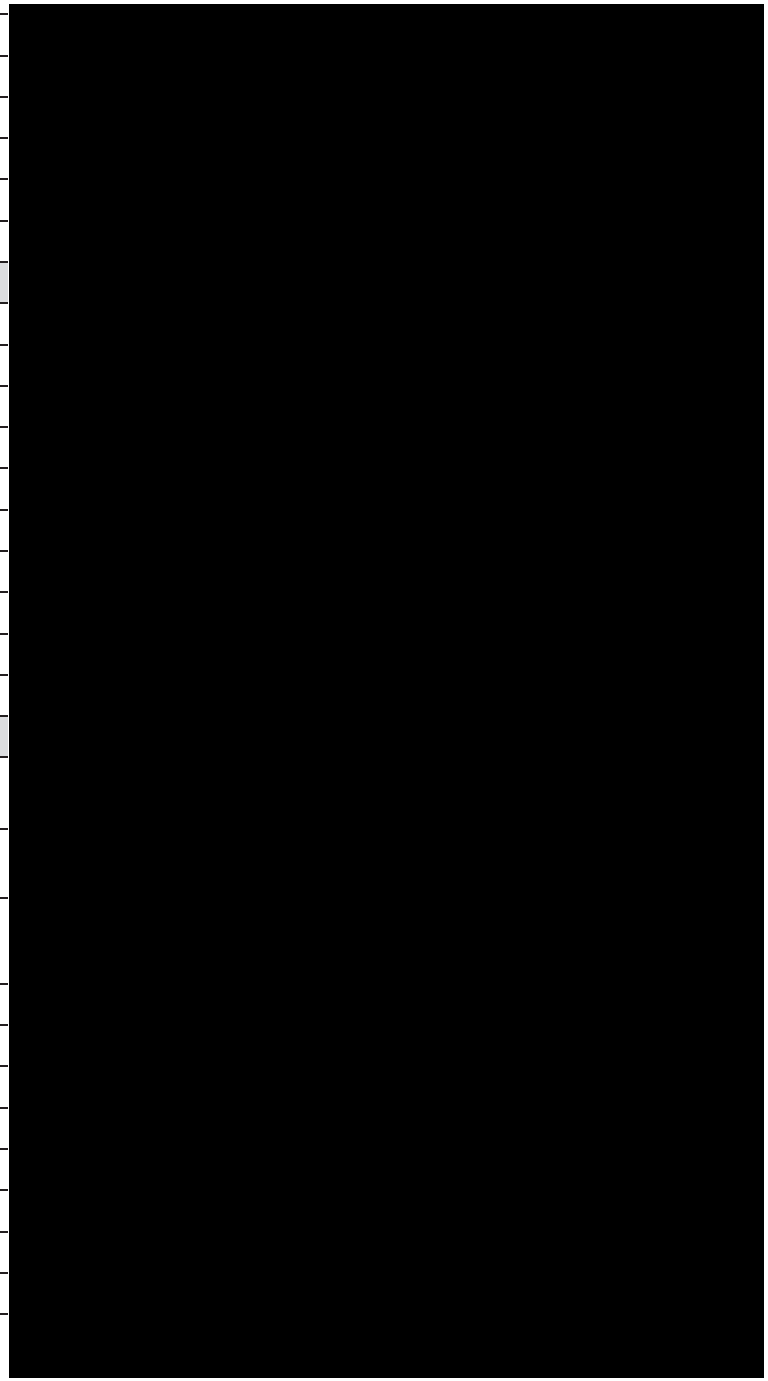
LPur-17	Police units involved (unlimited number of units)
LPur-18	Description of suspect vehicle narrative
LPur-19	Total number of occupants in suspect vehicle
LPur-20	Free text narrative
LPur-21	Terminating event
LPur-22	Arrested (Yes/No checkboxes)
LPur-23	Arrest number
LPur-24	Escaped (Yes/No checkboxes)
LPur-25	Details of arrest/escape narrative
LPur-26	Injuries to officers (Yes/No checkboxes)
LPur-27	Injured officers (unlimited)
LPur-28	Names of injured officers
LPur-29	Disposition of injured officers
LPur-30	Injuries to suspects (Yes/No checkboxes)
LPur-31	Injured suspects (unlimited)
LPur-32	Names of injured suspects
LPur-33	Disposition of injured suspects
LPur-34	Vehicle accident involved (Yes/No checkboxes)
LPur-35	Police unit involved (Yes/No checkboxes)
LPur-36	Third party involved (Yes/No checkboxes)
LPur-37	Third party injuries (unlimited)
LPur-38	Names of third parties injured
LPur-39	Treatment of injuries
LPur-40	Property damaged
LPur-41	Subject name
LPur-42	Subject race
LPur-43	Subject sex
LPur-44	Subject date of birth
LPur-45	Subject address
LPur-46	Subject charges (unlimited)
LPur-47	Passenger charges (unlimited)
LPur-48	Supervisor post pursuit critique narrative



LPur-49	Copy of Communications tape attached (Yes/No checkboxes)
LPur-50	Supervisor preparing report name
LPur-51	Supervisor preparing report ID number
LPur-52	Supervisor preparing report watch
LPur-53	System shall be capable of multiple agency defineable review levels. For each review, system shall capture at a minimum:
LPur-54	Date of review
LPur-55	Electronic signature
LPur-56	Narrative
LPur-57	Administrative Decision (user defineable table, e.g., sustain, not sustain, unfounded).
LPur-58	The report generated will reflect the most recent format of the Agency Police Department Pursuit form.
LPur-59	The report can be printed on any networked printer.
LPur-60	The printing of the report may only be performed by an authorized user.
LPur-61	Reason for initiating pursuit.
	Law Enforcement Data Analysis
LDAni-1	The system provides a report wizard that guides users through the steps of generating reports.
LDAni-2	The system will allow authorized users to run unrestricted custom queries against the database.
LDAni-3	Authorized users can run a query on every field in the RMS software to generate reports.
LDAni-4	The system will allow authorized users to create ad-hoc queries with multiple criteria levels.
LDAni-5	Ability to sort by any field used in a report query.
	The system tracks the following types of data:
LDAni-6	Statistical
LDAni-7	Operational
LDAni-8	Investigative
LDAni-9	Management
LDAni-10	Administrative
LDAni-11	The data analysis module is fully integrated with RMS and all optional modules.
	Once data is extracted from a query, the user is able to:
LDAni-12	Save and Edit the query at a later date

[redacted]

LDAni-13	Export to one of the supported formats (e.g., Excel, XML, CSV, ASCII delimited file, text)
LDAni-14	Use the data to construct a pie chart
LDAni-15	Use the data to construct a bar graph
LDAni-16	Plot data on a map
LDAni-17	Generate and Print the final report
LDAni-18	Users can only query data they are authorized to view within the system.
	The system allows users to customize the following report elements:
LDAni-19	Font
LDAni-20	Color
LDAni-21	Alignment
LDAni-22	Titles and Subtitles
LDAni-23	Graphics (e.g., agency logo)
LDAni-24	Addresses
LDAni-25	Phone numbers
LDAni-26	The system supports electronic transfer of reports.
LDAni-27	The system provides customizable pull-down menus that allow users to select data to query.
LDAni-28	The software supports pin-mapping.
	The software supports plotting incidents on a map to show:
LDAni-29	Incidents near specific businesses, such as liquor stores
LDAni-30	Incidents near specific streets, cross streets, stop lights, etc.
LDAni-31	Incidents near specific schools
LDAni-32	Incidents in specific regions
LDAni-33	Incidents by type
LDAni-34	Incidents by date/time
LDAni-35	The system is able to display detailed information about an incident by using mouse-over of the map icon.
LDAni-36	The system provides the ability to zoom and pan.
LDAni-37	The system is able to apply multiple map layers for more details.
LDAni-38	The system can generate a density map to display the results of inquiries.
LDAni-39	The system can generate a hot spot map to show high crime areas.
LDAni-40	The system is capable of exporting data to third party applications.



	The system is able to map crime trends by:
LDAni-41	Location
LDAni-42	Subject
LDAni-43	Weapon
	The software provides an agency-defined list of topics located in the drop down menus, including:
LDAni-44	Motor Vehicle Crash
LDAni-45	Incidents
LDAni-46	Cases
LDAni-47	Offenses
LDAni-48	Arrests
LDAni-49	Warrants
LDAni-50	Tickets/Citations
LDAni-51	Master Name Index
LDAni-52	Officer Initiated Calls
LDAni-53	Property
LDAni-54	Case Subjects
LDAni-55	Fire Incidents
LDAni-56	Bookings
LDAni-57	Field Investigations
	The system allows users to specify information such as, but not limited to, the following:
LDAni-58	Date and Date Ranges
LDAni-59	Date Types, e.g., Report Date, Date Occurred, Arrest Date, etc.
LDAni-60	Time and Time Ranges
LDAni-61	Time Types, e.g., Report Time, Time Occurred, Arrest Time, etc.
LDAni-62	Agency Name
LDAni-63	ORIs
LDAni-64	Address and Address Ranges
LDAni-65	Types
LDAni-66	Maps
LDAni-67	Specific Districts

[redacted]

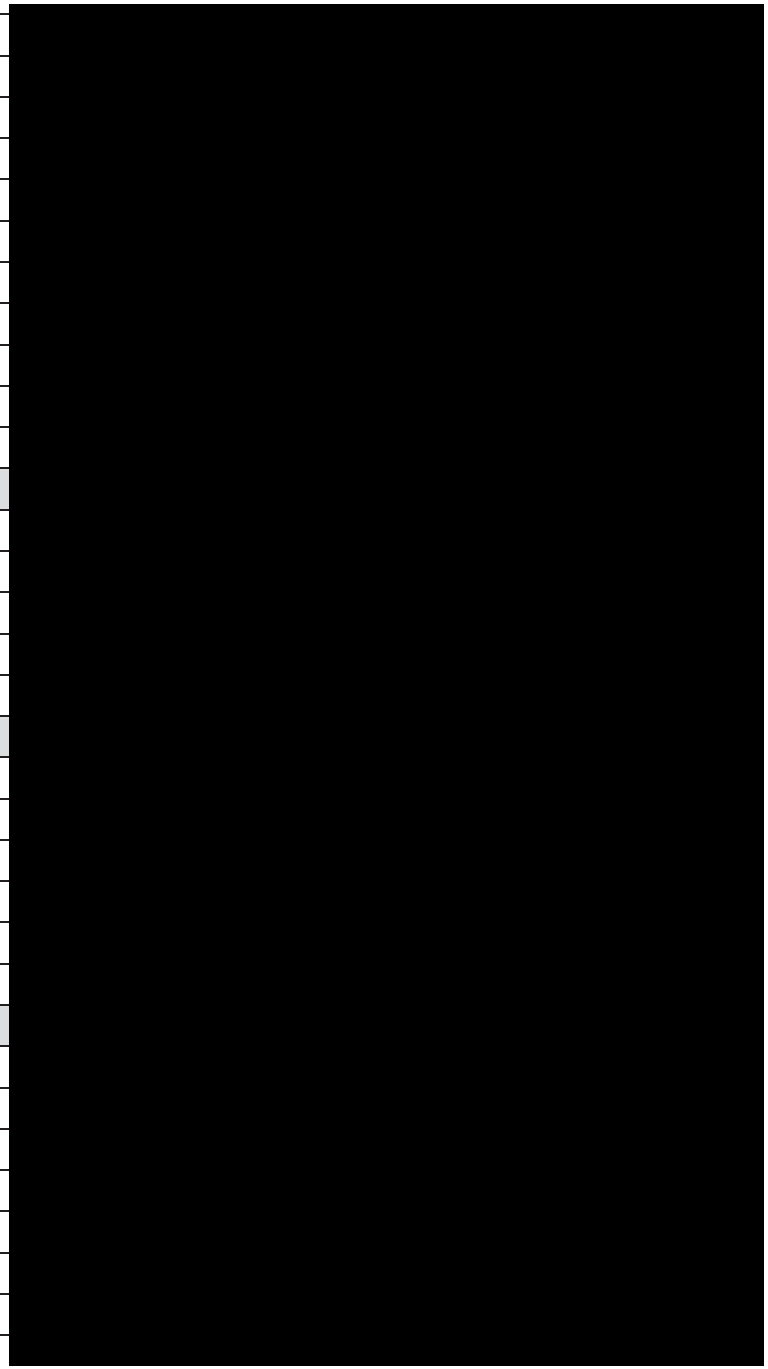
LDAni-68	The system has the ability to name and save a query.
LDAni-69	The system has the ability to access a saved query.
LDAni-70	The system allows authorized users to access any query created by another user.
LDAni-71	The system allows authorized users to create an ad hoc report useable by other authorized users.
LDAni-72	The system supports agency-defined icons in crime mapping to represent records from the query.
	Law Enforcement Field Reporting
LFldR-1	The software supports entry of field activity from a mobile device.
	Field activity includes the entry and update to:
LFldR-2	Arrests
LFldR-3	Cases
LFldR-4	Offenses
LFldR-5	Field Interview
LFldR-6	Civil process
LFldR-7	Field investigations
LFldR-8	Incidents
LFldR-9	Supplemental reports
LFldR-10	Citations
LFldR-11	User-defined forms
LFldR-12	Field investigations/contact cards are included in the supervisory review and upload/merge process.
LFldR-13	The forms and reports merge (into RMS) process is agency-defined.
LFldR-14	The system has the ability to include domestic-related fields outlined in case entry to be available for entry within the Field Reporting module.
LFldR-15	When an incident is flagged as "family violence" the system will require that specific mandatory fields be completed by the user.
LFldR-16	When an incident is flagged as "sexual assault" the system will require that specific mandatory fields be completed by the user.
LFldR-17	The software supports National Incident Based Reporting System (NIBRS) compliant data schema.
LFldR-18	The software supports the Uniform Crime Reporting (UCR) compliant data schema.
LFldR-19	The software has configurable form/field rules that will detect NIBRS errors at data entry time.
LFldR-20	The software has configurable form/field rules that will detect UCR errors at data entry time.
LFldR-21	The printed output from field report type is agency configurable.
LFldR-22	The software allows an officer to review the report for errors and warnings before submitting to a supervisor.
LFldR-23	The software supports supervisor review.

[redacted]

LFIdR-24	The software has the ability to add business logic to form entry. Business logic incorporates established rules and workflows to determine how the data is presented and stored.	
LFIdR-25	The system supports forms incorporating dynamic data entry user interface. For example, data entered in field of a form with a certain value will make other fields of that form mandatory entry fields.	
LFIdR-26	The system provides user maintainable workflow defined by report, by user and by department (agency), e.g., Report submitted -> Supervisor review -> Report returned to officer for correction if necessary -> Report resubmitted -> Supervisor approval.	
	The software allows for upload of officer reports using the following:	
LFIdR-27	Wireless (RF) over any protocol and network including, but not limited to:(i.e., private radio, commercial wireless network, mesh, etc.)	
LFIdR-28	Wireless (RF) over encrypted protocol and network including, but not limited to:(i.e., private radio, commercial wireless network, mesh, etc.)	
LFIdR-29	Secure on-line VPN connection to wireless router.	
LFIdR-30	The system can utilize third-party wireless connectivity/VPN software application to help manage connectivity to the wireless network.	
LFIdR-31	If connectivity is lost, data entered on forms is stored for later recall and upload once connectivity is restored.	
LFIdR-32	The software supports printing of a Field Report prior to being merged into the RMS database.	
LFIdR-33	The software provides a clipboard function that allows a user to enter and maintain notes as needed.	
LFIdR-34	The clipboard function stores data in folders as configured by the user.	
LFIdR-35	To comply with CJIS security requirements, temporary data in the clipboard is automatically deleted upon exit from the module.	
LFIdR-36	Data in the clipboard function can be deleted as desired by the user.	
LFIdR-37	Data in the clipboard function can be added to forms of system modules using cut-and-paste.	
LFIdR-38	The software has the capability of creating and archiving a .pdf version of the report.	
LFIdR-39	The software attaches a copy of all supplements into the RMS as a PDF.	
LFIdR-40	The software supports the retention of an exact copy of an officers report, as it existed when approved.	
LFIdR-41	The software supports the downloading of tables to all mobile devices, eliminating the need to update tables on individual devices.	
LFIdR-42	The software supports field reporting access security at the user level.	
LFIdR-43	The software supports field reporting access security at the device level (e.g. user supplied devices).	
LFIdR-44	Incomplete reports can be completed on any other device that has the field based reporting software installed.	
LFIdR-45	The software supports narrative text entry with spell checker.	
LFIdR-46	The software has automatic spell check.	
LFIdR-47	The software has the capability to permenantly enable automatic spell check.	
LFIdR-48	The software is table-driven.	
LFIdR-49	All field reporting drop down lists utilize common data from common fields in all applicable RMS modules and do not require separate entry.	
LFIdR-50	All field reporting drop down lists remain in sync with common data lists throughout the RMS application.	
LFIdR-51	The merge process supports merging one record at a time.	
LFIdR-52	The system automatically populates the fields in the RMS database during the merge process.	
LFIdR-53	An authorized user can configure default values and text that is available for use with any report field.	
LFIdR-54	The system supports agency-defined data entry screens for all field reports.	

LFldR-55	The system supports multiple report types for each incident allowing separate screens for specific report types.			
LFldR-56	The system supports text cut-and-paste between sections of a report.			
LFldR-57	The system supports text cut-and-paste between sections of different reports.			
LFldR-58	The system supports text cut-and-paste between modules of the application.			
LFldR-59	The system allows a user to create a new report based on the data of an existing report. This would copy the applicable data out of one report and into another.			
LFldR-60	The system supports batch upload of file attachments.			
LFldR-61	The system is capable of in-vehicle printing.			
LFldR-62	The system allows the entry of notations on every form and field as needed.			
LFldR-63	The system supports touch screen functionality.			
LFldR-64	The system allows the definition of business rules on any form.			
LFldR-65	The system allows for the use of client installed forms.			
LFldR-66	The system allows for the use of Web-based forms.			
LFldR-67	The software allows for a report to be transmitted to a supervisor and back to individual for review and editing over the wireless network.			
LFldR-68	The software supports encryption during all processes both on the local client and over the wireless network.			
LFldR-69	Any form that is built or scanned into the field reporting software is able to print with the appropriate data.			
	Law Enforcement Career Criminal			
LCCrm-1	The system has the ability to create and maintain agency defined categories, e.g., Sex offender, Violent Offender, DUI.			
LCCrm-2	The system allows an authorized user to determine if an offense is violent or non violent.			
LCCrm-3	The system is able to create agency-defined statuses.			
LCCrm-4	The system will identify parole/probation agents.			
LCCrm-5	The system will capture terms and conditions.			
LCCrm-6	The system will capture complete registrant history by police department.			
LCCrm-7	The system will indicate all (unlimited) offenses.			
LCCrm-8	The system will capture registration dates.			
LCCrm-9	The system will import and attach a variety of document/file types to career criminal records.			
LCCrm-10	The system is able to accept additional comments in free-form narrative format.			
LCCrm-11	The system is able to automatically create officer warnings throughout system (e.g. user adding subject to case or citation, would have indication the subject being added was a Career Criminal).			
LCCrm-12	The system displays the photo of the subject within the career criminal record.			
LCCrm-13	A photo image can be loaded and stored via direct connect with a digital camera and USB/SD Card transfer.			
LCCrm-14	The system can assign "career criminal" designations to subjects based on agency-defined criteria, such as 3 charges for violent crime, based on entered case data.			
LCCrm-15	The system can assign "career criminal" designations to subjects based on agency-defined criteria, such as being incarcerated four (4) times, based on entered Corrections Management information.			
LCCrm-16	The photo image can be uploaded from:			

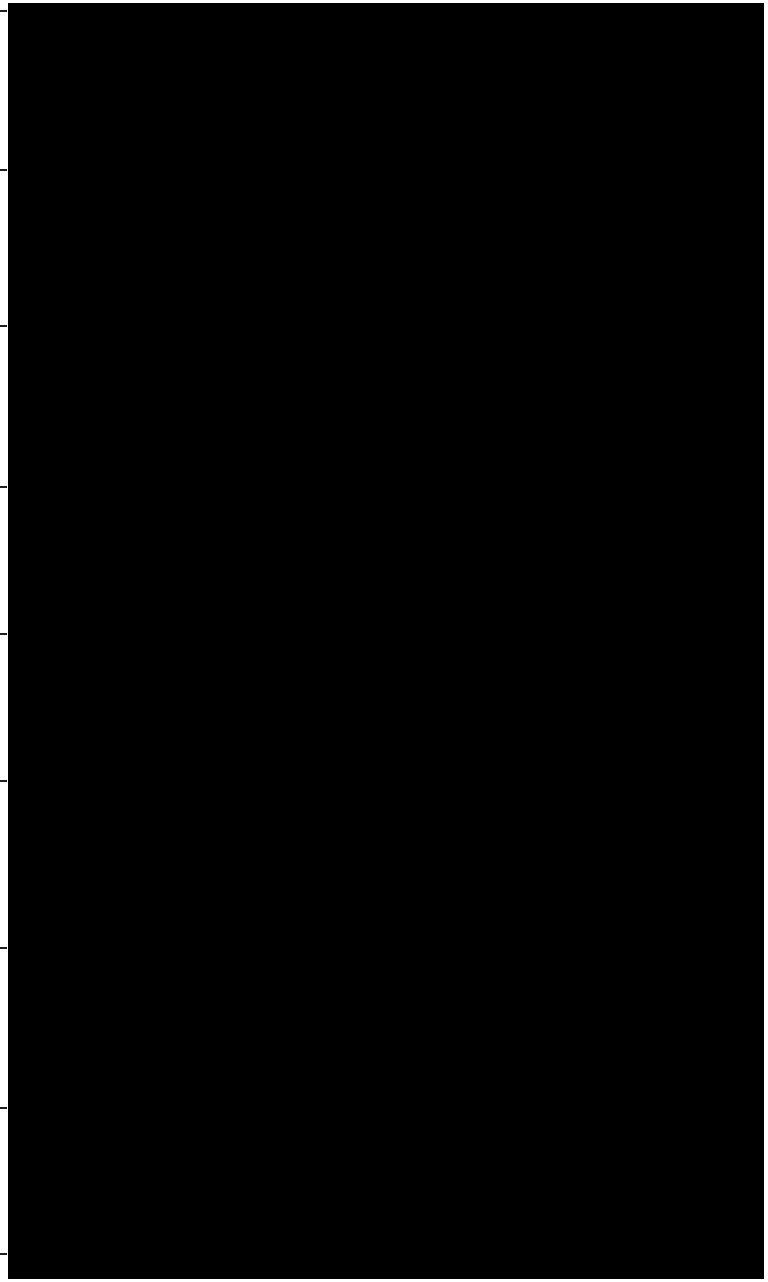
LCCrm-17	Digital camera (TWAIN compliant)
LCCrm-18	computer disk
LCCrm-19	TWAIN complaint standard scanned image file format (e.g., JPG)
LCCrm-20	USB drive
LCCrm-21	embedded email
LCCrm-22	embedded text message
LCCrm-23	The system is able to automatically create system wide alerts on all registrants.
LCCrm-24	The is able to generate department-specific reports from any captured fields.
LCCrm-25	The system is able to reference all activity of listed registrants.
LCCrm-26	The system is able to reference all registrants' department activity.
LCCrm-27	Career criminal module integrates with the Master Name Index (MNI).
	Law Enforcement Bicycle Registration
LBike-1	The system creates agency-defined registration types.
LBike-2	The system tracks registration by agency-defined status.
LBike-3	The system allows agency defined registration numbers, including auto-incrementing of registration numbers.
LBike-4	The system associates bicycle with registered owner.
LBike-5	The register owner is entered into Master Name Index.
	At a minimum, the following owner information is tracked:
LBike-6	Address
LBike-7	Race
LBike-8	Sex
LBike-9	The system tracks complete agency contact history of registered owner.
LBike-10	The system tracks complete agency contact history of bicycle.
LBike-11	The system is capable of searching all registered bicycles.
	The system tracks bicycle registration by:
LBike-12	Make
LBike-13	Model
LBike-14	Registered Owner
LBike-15	Wheel size
LBike-16	Frame size
LBike-17	Color
LBike-18	Serial number



LBike-19	The system can attach a variety of supporting documents (of various types) to the bicycle registration record.
LBike-20	The system generates agency specific reports on any or all captured fields.
LBike-21	The system references all bicycle owners' agency history.
LBike-22	The system provides a means to print a bicycle inspection or registration bar code label.
	Law Enforcement Racial Profiling
	The system is capable of capturing all the necessary data to complete a Racial Profiling report, as follows:
RacPrf-1	Sex/Gender (Selectable from drop down list)
RacPrf-2	Race/Ethnicity (Selectable from drop down list)
RacPrf-3	Officer knew the race/ethnicity of the individual before initiating the traffic stop
RacPrf-4	Garnishments
RacPrf-5	Individual stopped was resident of the Agency (Yes/No checkboxes)

[redacted]

RacPrf-6	Location of the traffic stop
RacPrf-7	Contact was related to a call for service, (provides ability to enter CFS number)
RacPrf-8	Citation or warning citation was issued, (selectable)
RacPrf-9	An individual was arrested as a result of the stop
RacPrf-10	Offense(s) charged, allows for multiple charges
RacPrf-11	The officer conducted a search
RacPrf-12	A consent to search was obtained
RacPrf-13	Search was conducted based upon probable cause



RacPrf-14	Contraband was discovered and seized as a result of the search	[redacted]
RacPrf-15	The officer used physical force that resulted in bodily injury (a positive response should result in officer being directed to complete the Use of Force Report)	
RacPrf-16	The contact was recorded (body worn and/or in car camera)	
RacPrf-17	The user can add customizable fields	
RacPrf-18	The system will produce the racial profiling report	
RacPrf-19	The system will be capable of submitting a report electronically to a federal, state, or third-party system.	
	The system should include the following modules:	
Mod-1	Sex Offender Registrations	
Mod-2	Police to civilain (P2C OSSI product) type public facing portal	
Mod-3	Field Training Officer (FTO)	
Mod-4	Criminal Trespass Log	
Mod-5	Auditing (audit CJIS, Car-to-Car, Car-to-dispatch messaging)	
	Law Enforcement Citations	
LCit-1	The system shall be capable of creating an upload file of citations.	

LCit-2	The system will interface to third-party citation software	[redacted]
LCit-3	The system will interface to Agency court system.	
LCit-4	A notification is provided to a user designated by the Agency if the upload fails.	
	All information pertaining to traffic tickets and citations can be entered and maintained, including:	
LCit-5	Ticket Book Distribution, by ticket number range	
LCit-6	Statistical Information by Department	
LCit-7	Statistical Information by Officer	
LCit-8	Ticket Deletions	
LCit-9	Status Changes	
	A history on each traffic ticket and citation can be produced, including (but not limited to) the following information:	
LCit-10	Violator name	
LCit-11	Violator address	
LCit-12	Violator DOB	
LCit-13	Violator DL number	
LCit-14	Violator telephone number	
LCit-15	Violator Employer	
LCit-16	Violation code, can be multiple violations	
LCit-17	Statute/Ticket type for each violation	
LCit-18	Violation location	
LCit-19	Vehicle license plate number	
LCit-20	Vehicle license plate state	
LCit-21	Vehicle owner name	
LCit-22	Owner personal information	
LCit-23	Vehicle make and model	
LCit-24	VIN	
LCit-25	Vehicle color	
LCit-26	Date/Time stamped	
LCit-27	Ticket number	
LCit-28	Weather and Traffic Conditions	
LCit-29	Court and Disposition Data	

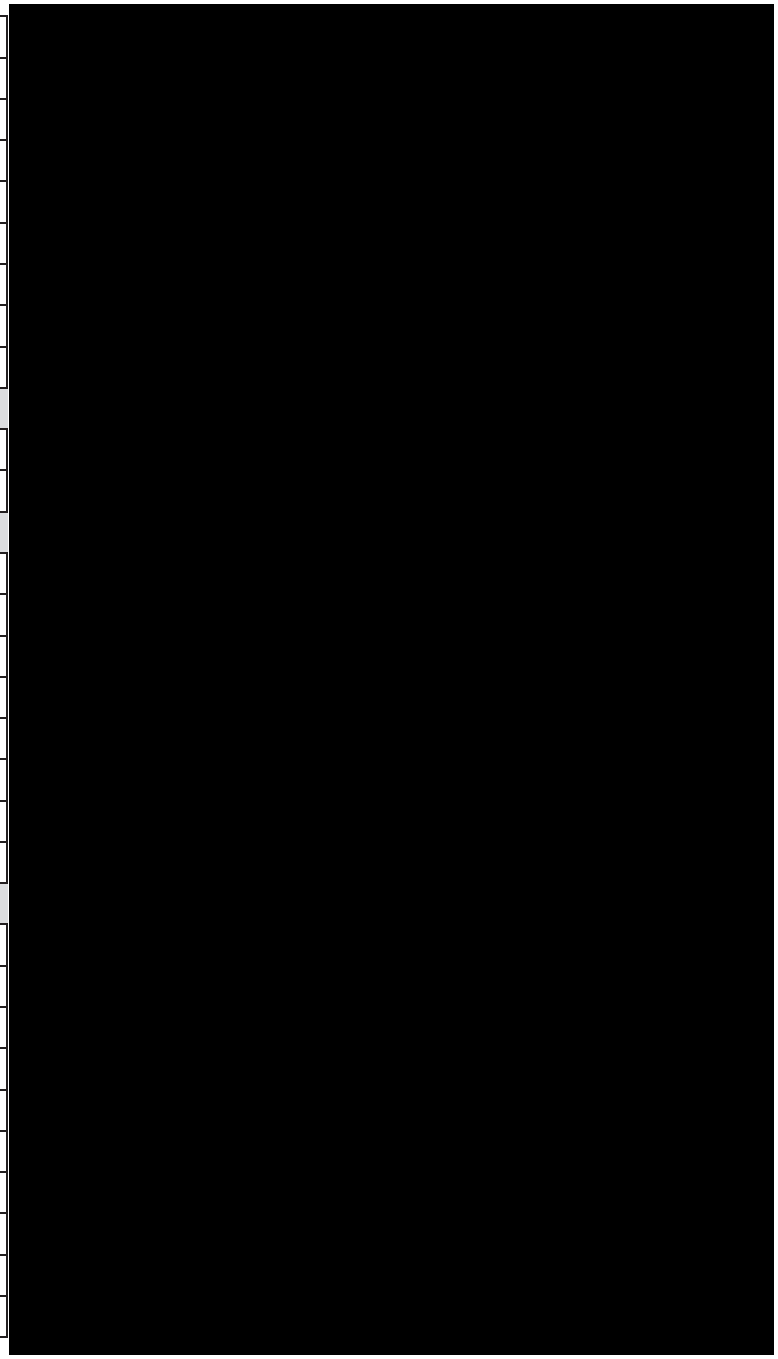
LCit-30	Fines and fees
LCit-31	Fines and fees payment tracking
LCit-32	Violator information will be included in MNI database.
LCit-33	Authorized personnel have the ability to void / delete tickets.
LCit-34	The system supports storing multiple violations under a single ticket number.
LCit-35	The system has the ability to search and report ticket / citation information.
	The system has the ability to search and report ticket / citation information using the following:
LCit-36	Violator name
LCit-37	Location
LCit-38	Geographic area
LCit-39	Jurisdiction / department
LCit-40	Officer ID
LCit-41	Officer name
LCit-42	Ticket type
LCit-43	Ticket book distribution
LCit-44	The system is able to generate failure to pay notices in a time frame determined by the agency.
LCit-45	The system is able to generate failure to pay notices in a format determined by the agency.
LCit-46	The system is able to interface with an e-ticketing mobile ticketing product with the mobile device.
LCit-47	The system is able to interface with a license barcode reader with the mobile device.
LCit-48	The system is able to interface with a license mag-stripe reader with the mobile device.
LCit-49	The system is able to interface with a electronic signature capture module with the mobile device.
LCit-50	The system is able to interface with mobile printing with the mobile device.
LCit-51	The system is able to associate with the CJIS and NCIC modules.
LCit-52	The system will provide the ability to import data from the citation software and when citations are entered manually.
	Law Enforcement Asset Management
LAMan-1	System is capable of expansion to accommodate potential for future additional scanners, printers, property intake locations, etc.
LAMan-2	The system manages equipment maintenance and repair functions.
LAMan-3	The system provides the ability to create maintenance schedules for equipment that requires regular maintenance.
LAMan-4	The system is able to attach multiple supporting documents/files of various types (e.g., Word, Excel, JPG, MPG, WAV) to a Asset record.
LAMan-5	Ability to capture electronic signatures.

[redacted]

	The system collects data to manage equipment maintenance and repair functions which includes, but is not limited to:
LAMan-6	Type
LAMan-7	Department
LAMan-8	Division
LAMan-9	Station
LAMan-10	General description
LAMan-11	Work order number
LAMan-12	Inspected/tested by (e.g., Officer ID, Name)
LAMan-13	Type of inspection/test (multiple occurrences)
LAMan-14	Date of inspection/test
LAMan-15	Status (e.g., pass/fail)
LAMan-16	Next action/inspection to be made
LAMan-17	Date of next action/inspection
LAMan-18	Unlimited Remarks (Free text)
LAMan-19	Date of repair
LAMan-20	Type of repair
LAMan-21	Cost of the repair
LAMan-22	Who made the repair
LAMan-23	Expected date to return to service
	Facility Repair / Work Order Tracking
LAMan-24	Any authorized user can submit work requests.
LAMan-25	The system is able to report and track requests for repair at facilities.
	The repair at facilities data tracked includes, but not limited to:
LAMan-26	Repair Type
LAMan-27	Repair Location
LAMan-28	Free-form text field for notes
LAMan-29	Requesting Facility
LAMan-30	General description
LAMan-31	Work order number
LAMan-32	Requesting Person
LAMan-33	Requesting Shift
LAMan-34	Reported Date

[redacted]

LAMan-35	Date Work Order Assigned
LAMan-36	Date of Action
LAMan-37	Action Type
LAMan-38	Date of Completion
LAMan-39	Assigned to (table based)
LAMan-40	Inspected / verified by (i.e. Personnel ID, Name)
LAMan-41	Date of inspection / verification
LAMan-42	Ability to associate / link work orders
LAMan-43	Unlimited Remarks (Free text)
	Issued Supplies and Equipment
LAMan-44	The system captures and tracks issued supplies and equipment data.
LAMan-45	The system has the ability to capture the proper authorization for the equipment, if necessary.
	Equipment may be assigned to, but is not limited to:
LAMan-46	Agency
LAMan-47	Division
LAMan-48	District
LAMan-49	Platoon
LAMan-50	Unit
LAMan-51	Group
LAMan-52	Physical location
LAMan-53	Individual
	The other issued equipment data includes, but is not limited to:
LAMan-54	System ID number
LAMan-55	Item description
LAMan-56	Equipment ID Number
LAMan-57	Agency ID number
LAMan-58	User-defined category
LAMan-59	User-defined sub-category
LAMan-60	Date of purchase
LAMan-61	Expiration Date
LAMan-62	Supplying vendor
LAMan-63	Purchase cost



LAMan-64	Manufacturer	
LAMan-65	Model number	
LAMan-66	Serial number	
LAMan-67	Last maintenance/inspection due	
LAMan-68	Personnel ID (Issued to)	
LAMan-69	Unit Number / Apparatus number (Issued to)	
LAMan-70	Free-form text field for notes	
LAMan-71	Repair records (including shipped/returned dates, shipped to, cost)	
LAMan-72	Maintenance records	
LAMan-73	Maintenance schedule	
LAMan-74	OSHA testing requirement ID	
LAMan-75	OSHA testing requirement due date	
LAMan-76	OSHA testing requirement completion date	
	Fixed Asset Tracking	
LAMan-77	The system is able to capture and track fixed-asset data.	
LAMan-78	The system has the ability to track equipment that is checked-in and checked-out basis (e.g. daily basis, for patrol)	
LAMan-79	The system has the ability to track equipment checked-out.	
LAMan-80	The system has the ability to track equipment checked-in.	
LAMan-81	The system provides a check-in and check-out log.	
LAMan-82	The system has the ability to print receipts.	
	The check-in and check-out log will include:	
LAMan-83	Date and time checked-out.	
LAMan-84	Date and time checked-in.	
LAMan-85	Unit	
LAMan-86	Individual	
LAMan-87	Equipment condition	
LAMan-88	The system must provide a log of all activity.	
	Ability to access the system via a mobile device:	
LAMan-89	Laptop Computer	
LAMan-90	Tablet	
LAMan-91	PDA	
LAMan-92	Other Type of Mobile Device	

	The fixed-asset related data includes, but not limited to:
LAMan-93	Item description
LAMan-94	System ID number
LAMan-95	Agency ID number
LAMan-96	User-defined category
LAMan-97	User-defined sub-category
LAMan-98	Date of purchase
LAMan-99	Supplying vendor
LAMan-100	Purchase cost
LAMan-101	Manufacturer
LAMan-102	Model number
LAMan-103	Serial number
LAMan-104	Last maintenance/inspection due
LAMan-105	Current location of item
LAMan-106	Free-form text field for notes
LAMan-107	Repair records (including shipped/returned dates, shipped to, cost)
LAMan-108	Maintenance records
LAMan-109	Maintenance schedule
LAMan-110	OSHA testing requirement ID
LAMan-111	OSHA testing requirement due date
LAMan-112	OSHA testing requirement completion date
	The system tracks, at a minimum, the following fixed-asset distribution data:
LAMan-113	System ID number
LAMan-114	Recipient
LAMan-115	Issuer
LAMan-116	Date distributed
LAMan-117	Date returned
LAMan-118	Date of loss or theft
LAMan-119	Police report number for theft or loss
LAMan-120	Police report date for theft or loss
	Inventory Tracking
LAMan-121	Inventory tracking system tracks all equipment sub-groups (e.g., vehicles, issued equipment, fixed assets)

[redacted]

LAMan-122	Inventory tracking is compatible with, can interface to, a bar-coding system.	[redacted]
LAMan-123	Ability to make inventory adjustments when doing annual inventory.	
	Ability to manage and track inventory using a bar code system including, but not limited to, the following functions:	
LAMan-124	Perform a mass update	
LAMan-125	Locate item by bar code	
LAMan-126	Generate bar code	
LAMan-127	Read bar code using remote, hand-held device	
LAMan-128	Track specific item information (e.g., description, quantity, status, etc.)	
LAMan-129	Ability to automatically update (e.g., download) inventory information into system.	
LAMan-130	Ability to print bar code labels.	
LAMan-131	Ability to provide inventory management using a bar code system.	
	Ability to record inventory of an item, including but not limited to:	
LAMan-132	Quantity in stock	
LAMan-133	Cost History	
LAMan-134	Minimum reorder points	
	Vendor information:	
LAMan-135	Name	
LAMan-136	Address	
LAMan-137	Phone	
LAMan-138	Contact	
LAMan-139	Ability to utilize a hand-held mobile inventory tracking scanner.	
	The system tracks, at a minimum, the following inventory-related data:	
LAMan-140	Quantity in stock	
LAMan-141	Re-order point	
LAMan-142	Vendor contact/ordering information	
LAMan-143	Order history	
LAMan-144	Pricing history	
LAMan-145	Last order information	
LAMan-146	Outstanding/pending order information	
LAMan-147	The system can generate and track internal purchase requests.	
LAMan-148	The system can generate and track purchase orders.	
	The system tracks, at a minimum, the following inventory distribution data:	

LAMan-149	Quantity distributed	[redacted]
LAMan-150	Recipient	
LAMan-151	Issuer	
LAMan-152	Condition at Issue	
LAMan-153	Condition at Return	
LAMan-154	Date of Issue	
LAMan-155	Date of Return	
	Supplies and Equipment Acquisition	
LAMan-156	Ability to generate automatic alerts to designated staff when inventory levels fall below a user defined level.	
	The system provides sufficient fields to record the receipt of an inventoried item, including, but not limited to, the following:	
LAMan-157	Item Type (bar code)	
LAMan-158	System ID Number	
LAMan-159	Agency ID	
LAMan-160	Station ID	
LAMan-161	Item Category	
LAMan-162	Item Sub-Category	
LAMan-163	Item Name	
LAMan-164	Item Description	
LAMan-165	Inventory or Asset Number (e.g. bar code)	
LAMan-166	Manufacturer	
LAMan-167	Model Number	
LAMan-168	Serial Number	
LAMan-169	Purchase Cost	
LAMan-170	Date of purchase	
LAMan-171	Vendor information	
LAMan-172	Current Location of Equipment	
LAMan-173	The system allows for user defined categories.	
LAMan-174	The system allows for user defined sub-categories.	
LAMan-175	The system allows for the tracking of equipment acquired via grant monies and attach any special notes/narrative specific to the grant	
	Ability to track vendor information:	
LAMan-176	Company Name	
LAMan-177	Point of Contact Name	

LAMan-178	Address	[redacted]
LAMan-179	Telephone Number	
LAMan-180	Email	
LAMan-181	Web Site	
LAMan-182	Order History	
LAMan-183	Notes/Narrative	
	Personal Equipment	
LAMan-184	The system provides the ability to develop a list of types of equipment that are issued to personnel.	
LAMan-185	The system provides the ability to define types of equipment (e.g., badges, IT equipment, cell phones, uniforms, etc.) included in personal equipment table.	
	The system provides the ability to track piece of equipment that has been assigned to personnel, including, but not limited to, the following:	
LAMan-186	Equipment Category	
LAMan-187	Equipment type	
LAMan-188	Quantity	
LAMan-189	Personnel ID	
LAMan-190	Personnel Name	
LAMan-191	Manufacturer	
LAMan-192	Serial number	
LAMan-193	Model	
LAMan-194	Description	
LAMan-195	Condition	
LAMan-196	Cost	
LAMan-197	Date of issuance	
LAMan-198	Date of purchase	
LAMan-199	Date of return	
LAMan-200	Disposal date	
LAMan-201	Inventory ID number (e.g., barcode)	
LAMan-202	Replacement date(s)	
LAMan-203	Service date	
LAMan-204	Calibration date	
LAMan-205	Size	
LAMan-206	Status (lost, decommissioned, etc.)	
LAMan-207	Comments	

LAMan-208	Ability to assign multiple pieces of the same type of equipment to an individual.	
LAMan-209	Ability to capture and track history of all equipment assigned to an individual.	
LAMan-210	Ability to track the daily assignment of items (e.g. weapons, vehicles, etc.).	
	Firearms and Ammunition	
LAMan-211	The system has the ability to capture, maintain and track firearms and ammunition assigned to personnel, including, but not limited to:	
LAMan-212	Agency	
LAMan-213	Division	
LAMan-214	Agency assigned ID number	
LAMan-215	Date issued	
LAMan-216	Employee ID	
LAMan-217	Employee Name	
LAMan-218	Inspected by	
LAMan-219	Inspected date	
LAMan-220	Issue by (name)	
LAMan-221	Maintenance requirements	
LAMan-222	Maintenance performed	
LAMan-223	Quantity issued	
LAMan-224	Received by	
	Ability to assign NCIC code identifiers:	
LAMan-225	Make	
LAMan-226	Model	
LAMan-227	Serial number	
LAMan-228	Caliber	
LAMan-229	Color/Finish	
	Station/Location Equipment	
LAMan-230	The system provides the ability to develop a list of types of equipment that are issued to stations/locations.	
LAMan-231	The system provides the ability to define the types of equipment that are issued to the stations/locations.	
	The system provides the ability to provide fields to track each piece of equipment assigned to a station including, but not limited to, the following:	
LAMan-232	Vehicles assigned to (e.g., Vehicle ID)	
LAMan-233	Asset tag number	
LAMan-234	Bar code number	
LAMan-235	Brand	

LAMan-236	Classification	[redacted]
LAMan-237	Cost	
LAMan-238	Date issued	
LAMan-239	Date acquired	
LAMan-240	Description	
LAMan-241	Equipment type	
LAMan-242	Location in station	
LAMan-243	Location on the vehicle (e.g. compartments)	
LAMan-244	Manufacturer	
LAMan-245	Model	
LAMan-246	Part number	
LAMan-247	Serial number	
LAMan-248	Agency/division/platoon assigned to	
LAMan-249	Warranty information	
LAMan-250	Individual receiving equipment	
LAMan-251	Size	
LAMan-252	Color	
LAMan-253	Ability to assign multiple pieces of the same type of equipment to an vehicle.	
LAMan-254	Ability to easily transfer equipment to a different vehicle/location without re-keying descriptive data (e.g. drag and drop or a quick transfer function).	
LAMan-255	The system is capable of logging and storing equipment location changes.	
LAMan-256	Ability to track loaned equipment.	
LAMan-257	Ability to generate alerts to individuals that loaned equipment is due back for return.	
LAMan-258	Ability to access a list of assigned equipment (including where/who assigned to) from the Mobile Data environment.	
LAMan-259	The system provides the ability when a piece of equipment is involved in an incident, the incident report and actions related to that incident are automatically linked to the equipment in the asset module.	
	Equipment Return	
LAMan-260	Ability to return or check equipment back into inventory.	
LAMan-261	Ability to document condition	
LAMan-262	Ability to unlink equipment from personnel upon check-in.	
	Ability to track replaced equipment:	
LAMan-263	Date replaced	
LAMan-264	Reason replaced (drop-down list)	
LAMan-265	Disposition of replaced equipment	

LAMan-266	Personnel ID replacing the equipment	[redacted]
	Equipment Maintenance and Replacement	
LAMan-267	Ability to create maintenance schedules for equipment requiring regular maintenance.	
LAMan-268	Ability to create maintenance schedules for equipment requiring regular inspection.	
LAMan-269	Ability to document maintenance for a piece of equipment.	
LAMan-270	Ability to document service test records for a piece of equipment.	
LAMan-271	Ability to create replacement schedules for equipment requiring replacement after a user defined period of time.	
	Ability to generate alerts to individuals that their equipment is due for:	
LAMan-272	Maintenance	
LAMan-273	Inspection	
LAMan-274	Replacement	
	Equipment Disposal	
LAMan-275	The system is able to track equipment that is disposed of.	
LAMan-276	When equipment is disposed of it changes the equipment status but does not remove the historical records associated with that item.	
LAMan-277	The system will track the date the equipment was taken out of service.	
LAMan-278	The system will track the person disposing the equipment.	
LAMan-279	The system will track the means of disposal.	
	Asset Management Reports	
	Ability to generate a physical inventory report based on:	
LAMan-280	Asset category	
LAMan-281	Asset age	
LAMan-282	Asset location	
LAMan-283	Specific type of equipment	
LAMan-284	Ability to generate a physical inventory exception report.	
LAMan-285	Ability to generate a check-in/checkout log for temporarily assigned assets.	

LAMan-286	Ability to generate a report of items that require re-ordering (e.g., out of stock or below minimum threshold)	[redacted]
LAMan-287	Ability to generate reports listing equipment due for maintenance during a user-defined time period (e.g. generate a report on the first of every month for equipment that needs to be replaced by the end of the month).	
LAMan-288	Ability to generate reports listing equipment due for replacement during a user-defined time period (e.g., generate a report on the first of every month for equipment that needs to be replaced by the end of the month).	
LAMan-289	Ability to generate a report for equipment that needs replaced at the end of user defined period of time (e.g. quarterly, yearly, multi-year, etc.).	
LAMan-290	Ability to schedule an automated report for equipment that needs to be replaced by a user defined period of time (e.g. 30 days prior, end of the month, etc.)	
LAMan-291	Ability to automatically generate and print, at a user-defined interval, reports listing equipment overdue for replacement (e.g. generate a report on the first of every month for equipment for which replacement is overdue).	
LAMan-292	Ability to generate a report that documents all maintenance completed on a specific piece of equipment.	
LAMan-293	Ability to generate automated email messages to staff responsible for replacing overdue equipment.	
LAMan-294	Ability to generate automated email messages to staff responsible for replacing expired supplies.	
	The system is capable of generating a report, including current status of various requests, including, but not limited to:	
LAMan-295	Facility repair requests	
LAMan-296	Equipment repair requests	
LAMan-297	Purchase orders	
LAMan-298	Work requests	
LAMan-299	Ability to generate a report for all inspections that are coming due within a user defined time frame (e.g. end of month, next 30 days, etc.).	
LAMan-300	Ability to generate a report for all equipment that has been disposed of.	
LAMan-301	Ability to generate a report for all equipment including age of that equipment.	

LAMan-302	The ability to generate reports for equipment checked-in and checked-out logs.
LAMan-303	Ability to generate a report showing the complete history of an asset.
LAMan-304	Ability to generate a report showing active property assigned to an officer.
LAMan-305	Ability to generate a report showing the complete history of an asset.
LAMan-306	Ability to generate a report showing active property assigned to an officer.

[redacted]

Attachment H – Interface Descriptions

COTS Interfaces

ANI/ALI Interface

- [redacted]

Description:

[redacted]

Assumptions:

- [redacted]

Constraints:

- [redacted]
- [redacted]

HxGN OnCall Dispatch | [redacted]

Description:

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

Assumptions:

- [redacted]
- [redacted]

HxGN OnCall Dispatch | Informer

- NCIC/TLETS

[redacted]

[redacted]

HxGN OnCall Dispatch | Tracker

- [redacted]

Description:

[redacted]

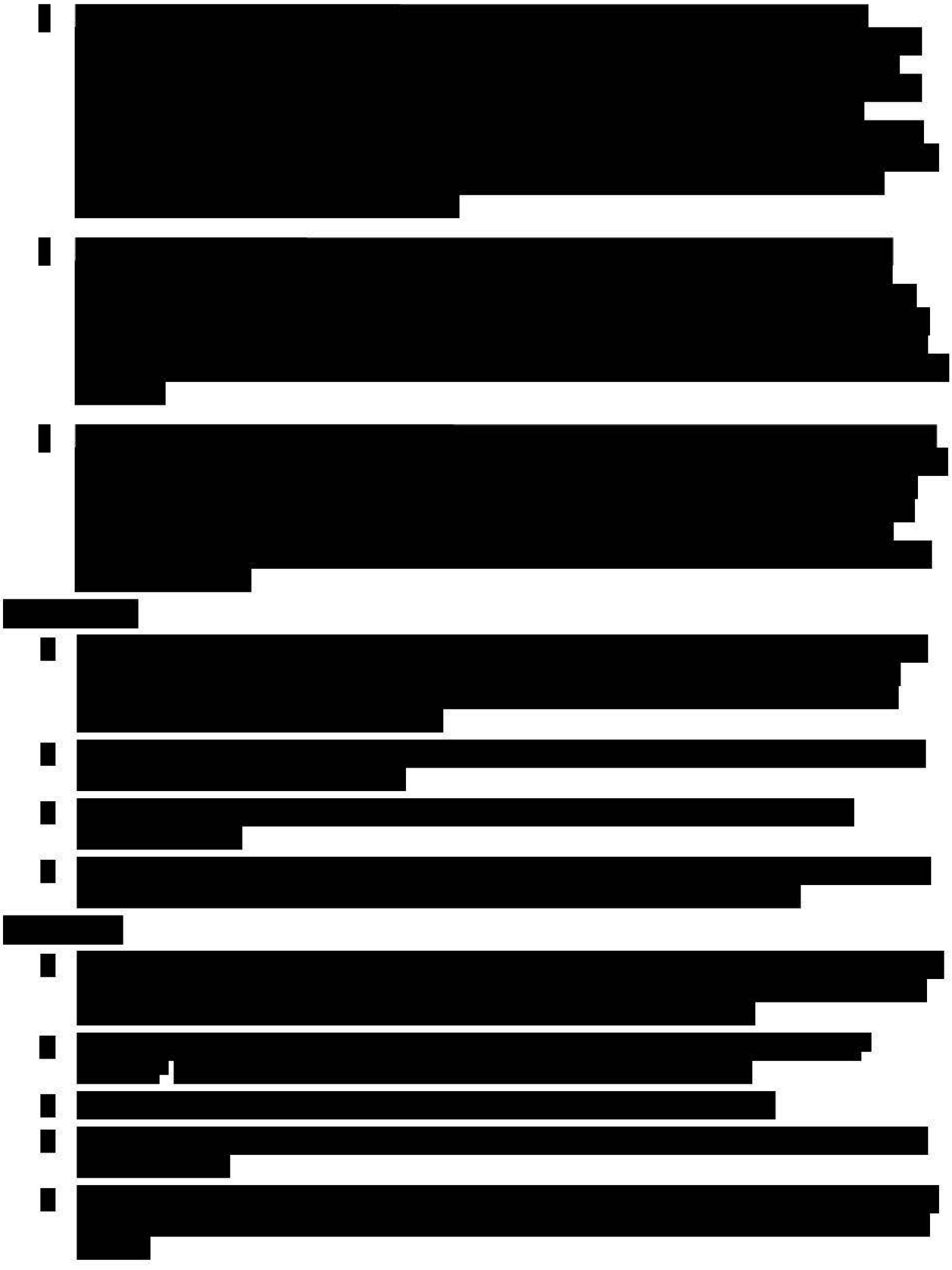
[redacted]

HxGN OnCall Dispatch | Notifications

- [redacted]

Description:

[redacted]



HxGN OnCall Dispatch | FireLink

[redacted]

Description:

[redacted]

HxGN OnCall Dispatch | CADLink

- [redacted]

Description:

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]

HxGN OnCall Dispatch | PTT

- [redacted]

Description:

[redacted]

[redacted]

[redacted]

[redacted]

HxGN OnCall Dispatch | [redacted] Interface

[redacted]

[redacted]

Standard Interfaces

Fire Station Alerting OnCall Dispatch Interface

- [redacted]

Description:

[redacted]

PLT Radio OnCall Dispatch Interface

[redacted]

[redacted]

- [redacted]
- [redacted]

Anti-Bias Reporting (Texas)

Description:

[redacted]

[redacted]

Custom Interfaces

CAD Informer interface for [redacted]

Description:

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

CAD Informer interface for [redacted]

Description:

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

CAD Informer interface for [redacted] Address Query

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

- [redacted]

Text to 911 [redacted]

Description:

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

CAD Interface for [redacted]

Description:

[redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
  - [redacted]
  - [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Bi-Directional RMS interface for [redacted]

Description:

[redacted]

RMS Import Interface from [redacted]

Description:

[redacted]

RMS Import Interface from [redacted]

Description:

[redacted]

RMS Export Interface to [redacted]

Description:

[redacted]

RMS Import Interface for [redacted]

Description:

[redacted]

Consulting Services

[redacted]

[redacted]

Attachment I – Glossary of Terms

Capitalized terms that are not defined below or within the body of the SOW, shall have the same meaning as set forth in the Master Terms Glossary.

"Acceptance" to mean acceptance of a Task in accordance with Task Acceptance Process.

"Agreement" shall have the same meaning as set forth under the header "Terms and Conditions."

"Benchmark Criteria" or "**Specifications**" means the objective criteria which identifies an intended outcome as reflected in, as applicable, an ICD, a Design Document, or Software Requirements (whichever document having last addressed the functionality in question being dispositive)

"Blocker Defect" means a Test Case has failed to satisfy the Benchmark Criteria that would correspond to a Level One Defect or Level Two Defect, or a Level One or Level Two Defect.

"Code Freeze" means a point in the Project where Customer may not make any change, configuration change, or other modification to the Software implemented as part of the Project.

"Core Team(s)" means all of the respective Subsystem Core Teams pertaining to the Project, which depending on the Project will collectively include: the Dispatch Core Team, the Mobile Core Team(s), and the Records Core Team.

"COTS Interfaces" means those Interfaces specifically identified in COTS Interface Questionnaire Completion Task in the SOW

"Customer Responsibilities" means (1) those specific tasks and obligations identified in the SOW as being the responsibility of the Customer and (2) those obligations, not stated in the SOW, but which would otherwise be reasonably considered as being Customer obligations and responsibilities.

"Custom Interfaces" means those Interfaces specifically identified in the applicable Task

"Customization" means a modification of the source code of Software.

"Cutover Plan" means a document reflecting the Activities and actions necessary to Cutover the System.

"Design Document" means a document articulating the design and intended output of a Customization.

"Documentation" means, whether in printed or electronic format, all documents (digital or hardcopy) delivered by Hexagon as part of the Project. Unless otherwise specified, it shall mean COTS Documentation.

"Facility" means a Customer provided facility/building/room that: (i) Can accommodate up to twelve (12) Customer participants; (ii) Has a projector and screen for displaying the content being presented, (iii) has Project Workstations for each participant; and a Customer workstation available for Hexagon's use while in the Facility.

"Functional Testing" means that testing process described in the Customer Functional Testing Task(s).

"GIS" means geographic information system

"Initial Schedule" means the initial iteration of the Project Schedule, which is contained in Attachment C of the SOW.

"Interface Control Document" or **"ICD"** means a document reflecting the design and requirements of a Custom Interface or certain I/Informer Interfaces, if any.

"Help Desk Portal" the electronic portal through which Customer may access the Help Desk to among other actions, log Services Requests, review the Knowledge Base,

"Hexagon Project Manager" means the person authorized by Hexagon to coordinate and manage the providing of Hexagon Services and Deliverables for the Project on behalf of Hexagon, in addition to being responsible for other duties specified in the Agreement and SOW.

"Master Terms Glossary" means that certain Common Terms Glossary set forth at https://www.hexagonsafetyinfrastructure.com/-/media/Legal/Hexagon/SI/TPS/CTG 06-2021.pdf

"Network Infrastructure" means the provision of adequate network and internet connectivity to provide sufficient operational bandwidth for the operation of the System in a manner consistent with the Product System Specifications together with all industry-standard network security, monitoring, and protection.

"Permissive Defect" means a substantially failed Test Case that would correspond to a Level Three or Level Four Defect, or a Level Three or Level Four Defect.

"Project Assumptions" means assumptions regarding the Project, which are listed in the SOW. Changes in any of the assumptions will affect the scope, schedule, and/or cost of the Project.

"Project Team" means the applicable Core Team and other resources assigned to provide information or services in connection with the Project, or applicable part thereof.

"Project Workstation" means a computer workstation (expressly excludes tablets or other smart devices) that has: (i) a modern web browser installed and ready for use; (ii) Internet access; (iii) at least one (1) external monitor with a resolution no smaller than 1920x1080 (understanding two (2) external monitors are recommended); (iv) the ability to connect to the web conference audio; and (v) a headset.

"Required Facilities" means a facility provided by the Customer that: (i) can accommodate up to twelve (12) Customer participants with workstations and monitors meeting the specifications for the Software described herein for each participant and (ii) has a projector and screen for displaying the content being presented. If the Customer's policies preclude connecting Hexagon-owned equipment to their network, a computer workstation for use by Hexagon for presenting content shall be made available.

"Server Setup Worksheet" means a document reflecting, among other details, the identification of servers, IP addresses, and node names for the System.

"Site Configuration Document" means a document reflecting the configurations made to the OnCall System.

"Software Requirements" means the functionality and capabilities affirmatively included in the OnCall Software as expressly specified Functional Matrices set forth in Attachment G-1 and G-2 in the Agreement, as appropriate to the Subsystem).

"SR" or **"Service Request"** a request logged into Hexagon's Help Desk Portal identifying a request for Hexagon to address a Defect, question, provide an Update, or provide an enhancement request, among other requests.

“Subject Matter Expert” or **“SME”** means a person(s) who has particular knowledge about a specific topic(s).

“System Administrator(s)” means a person or persons having the appropriate education, training, and/or experience in information technology to provide first tier support of the System.

“Task Prerequisites” means those events, deliverables, or accomplishments that are required to occur prior to the commencement of the applicable Task, except as may otherwise be agreed to through Conditional Acceptance.

“Test Case” means a set of conditions and parameters agreed to by the Parties which the Parties shall use to test whether the intended functionality identified in the Benchmark Criteria is reflected in the System.

“Test Case Failure” means a situation in which an executed Test Case has substantially failed in meeting the passage criteria set forth in the applicable portion of the Benchmark Criteria.

“Updated Initial Project Schedule” means the Initial Project Schedule updated by the Parties’ Project Managers during Project Kickoff Meeting Task and reflecting the actual Notice to Proceed date.

“VPN” means virtual private network.

“Warranty Period” means that one (1) year period beginning at Cutover for a Subsystem during which the applicable Project Software is subject to the warranty described in Attachment K.

Attachment J – GIS Requirements for the HxGN OnCall Dispatch System

HxGN OnCall Dispatch requires integration with a third-party mapping provider for GIS information. These third-party mapping services fall into three (3) main areas: Map Tile Services, Geocoding Services, and Routing Services. The selection, provisioning, and administration of its mapping services configuration of its map, maintenance and support of its map, and adherence to the requirements set forth herein is the responsibility of Customer. Hexagon shall not be responsible for resolving or addressing issues or Defects arising from Customer's non-conformance with requirements contained herein.

Map Service

[redacted]

Geocoding/Address Locator Service

[redacted]

Routing Service

[redacted]

Hexagon's Services expressly exclude ESRI related services, including, but not limited to, building or modifying of ESRI environments, providing consulting services related to ESRI environments, or other services related to ArcGIS software. The Customer is solely responsible for the use and creation of ArcGIS environments in conjunction with OnCall Dispatch. As you leverage ESRI as the mapping solution to integrate with OnCall, Customer may at its discretion seek additional guidance from ArcGIS professionals, materials published by ESRI, including the following link (https://enterprise.arcgis.com/en/server/latest/deploy/windows/single-machine-high-availability-active-active-deployment.htm) related to building a highly available GIS solution, or other appropriate resources.

Attachment K – Warranty

In accordance with Section 7.2 of the Agreement, Hexagon warrants the Hexagon Software provided in this Order shall materially conform to its Specifications for one (1) year from Cutover of the applicable Subsystem, provided that in the event of a nonconformity during the Warranty Period, Hexagon shall address the reported Defect in accordance with the Maintenance Terms within the Agreement.

Attachment L – Regional Provisions

The following terms, including any sub-attachments to this Attachment L, modify provisions set forth above to accommodate regional requirements. To the extent there is any conflict between the terms specified below and the terms set forth in the remainder of the SOW, the following shall control.

1. A Business Day includes up to eight (8) Business Hours, including breaks, during a twenty-four (24) hour period.

2. Upon Customer request, Hexagon personnel may undergo a criminal background check consisting of biographical information necessary to initiate an NCIC query and fingerprinting. To the extent the Customer requires Hexagon personnel to undergo such criminal background check, the Customer shall arrange for such criminal background check and be responsible for all costs associated with the criminal background check. The Customer agrees it will not charge Hexagon for fingerprinting if it conducts fingerprinting of Hexagon resources and it will accept completed fingerprint cards performed by other law enforcement agencies within the United States. Any remote personnel shall only be required to provide biographical information necessary to initiate a NCIC query and a fingerprint card completed by any law enforcement agency.
3. Per CJIS security policy, customers who wish to access U.S. national databases using mobile devices must use data encryption that is FIPS 140-2 certified and meets other CJIS requirements. The Customer is responsible for ensuring that their data communications infrastructure and devices comply with CJIS and applicable State requirements.
4. Hexagon agrees it shall remain compliant with the applicable portions of CJIS Guidelines as may be published by the FBI and state of Texas.

Attachment L-1 – CJIS Security Addendum

FEDERAL BUREAU OF INVESTIGATION

CRIMINAL JUSTICE INFORMATION SERVICES

SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

Attachment M – Performance Bond

Terms Within fifteen (15) Business Days of formation of Order 1, Hexagon shall provide to the Customer (Risk Management address with a copy to the County's designated IT contact) a performance bond securing a value consistent with the sum of all the payment milestones set forth in Attachment B. The performance bond will be provided from a licensed surety in the State of Texas and provided on the surety's form. The performance bond shall be in effect from the point of delivery of the performance bond to the Customer until Cutover of Order 1.

HEXAGON

Statement of Work

for

HxGN Connect

Cloud Consulting Services

PRESENTED BY:

Rebecca Villalona
Regional Sales Manager
Hexagon Safety, Infrastructure, & Geospatial
305 Intergraph Way
Madison, AL 35758 USA
Rebecca.villalona@hexagon.com

December 4, 2024

TABLE OF CONTENTS

Purpose

The SOW describes the Cloud Consulting Services for the Cloud Program. It documents Project implementation requirements, Cloud Application and Local Software functionality, the Activities and Tasks comprising the Project, the timeframe for completion of Activities and Tasks, the responsibilities for each Party, and the Task Acceptance Criteria.

Statement of Work Outline

The Services reflected in this SOW, exclusive of the Services described in Attachments G (Interface Addendum) and I (Additional Services), are included in the Quote[1] line item, "HxGN Connect Program Implementation Services." Services for Interfaces and Additional Services are reflected in Attachments G and I, if any, and separately identified in the Quote, if any.

The SOW includes and incorporates the following Attachments:

- Attachment A – Pricing Summary (Quote)
- Attachment B – Payment Milestones
- Attachment C – Initial Project Schedule
- Attachment D –Training Courses Curriculum
- Attachment E – System Configuration Diagram
- Attachment F – Functional Specifications Matrix
- Attachment G – Interface Addendum
- Attachment H – Glossary of Terms
- Attachment I – Reserved
- Attachment J – Onboarding Information Worksheet
- Attachment K – Cloud Service Schedules

Each task identified in the SOW includes the following as necessary: Task Description, description of Activities, Task Deliverables, Task Prerequisites and Assumptions, Hexagon/Customer Team Participation and Responsibilities, and Task Acceptance Criteria. The Tasks described in this SOW may not be listed chronologically, and the actual Project implementation Tasks and timelines will follow the Project Schedule, unless otherwise noted.

Order and Defined Terms

This SOW, together with the attached Quote, which is contained in Attachment A, is an Order made pursuant to the Master Terms. Execution of the Quote accompanying this SOW or other appropriate written instrument, including this SOW, reflects the Customer's acceptance of the Order. This SOW describes the Cloud Consulting Services and other Software (if purchased) provided by Hexagon in connection with the initial implementation of HxGN Connect. Hexagon will provide the Cloud Consulting Services to facilitate implementation of HxGN Connect as expressly set forth in this SOW (the "Project").

[1] For purposes of this Statement of Work, the Quote refers to Attachment A.

Unless otherwise defined in this SOW, capitalized terms shall have the same meaning as set forth in the Common Terms Glossary and Attachment H (Glossary) attached hereto.

Project Outline

The Project consists of two (2) phases: Initial Operating Capability (“IOC”) and Final Operating Capability (“FOC”). During IOC, Hexagon will Onboard the tenant(s) accounts associated with this Project and provide access to the HxGN Connect application. As part of FOC, Hexagon shall provide services to support Customer Activities as expressly described in this SOW.

All Tasks reflected in this SOW are regarded as complete and accepted upon completion of Task: System Availability.

HxGN Connect Program Functionality and Support

As part of the Cloud Program, Hexagon shall provide Credentials/License Keys to the Cloud Application components identified in the Quote. The Cloud Program shall have the capabilities and functionality set forth in the Specifications, which reflects all of the functionality Hexagon is obligated to provide in the HxGN Connect Program. From time to time, Hexagon may update HxGN Connect, including during the Project, which may modify the Specifications. Such updates as documented by Hexagon will reflect the then-current Specifications for purposes of this SOW. User Acceptance Testing shall only test that the functionality set forth in corresponding to Cloud Programs purchased (see Attachment A), and data is flowing into the HxGN Connect application as expected. Errors identified during testing are addressed in accordance with the terms related to Cloud Services Support. Only Blocker Errors are required to be resolved prior to completion of the System Availability Task. This scope does not include any Product Change Requests.

Upon completion of the IOC Completion Task, the Cloud Program Start Date shall have occurred. Consequently, Cloud Services Support will also begin at that time. The Customer is responsible for performing its Cloud Services Support obligations as reflected in the Master Terms for the duration of the Cloud Term, as may be extended.

Customer Project Team Structure

The Customer is responsible for providing qualified resources to staff the Core Team (described below) to facilitate a successful implementation of HxGN Connect. The Core Team roles and responsibilities are described in the following sections.

Core Team Roles and Responsibilities

The Core Team (as described below) shall consist of designated organization (Customer) personnel with the various skill sets and knowledge and backgrounds required to implement HxGN Connect. The following list identifies the required Core Team and its respective roles and corresponding responsibilities:

- **Project Manager** – responsible for the day-to-day coordination of Project Activities on behalf of the Customer. Note, there will be one overall Customer Project Manager.
- **System Administrator Personnel** – responsible for all system administration and configuration responsibilities related to the HxGN Connect Program. Note, it is recommended that each separate organization have its own System Administrator.
- **Subject Matter Experts (SMEs)** – responsible for representing end-users' needs and providing specific IT/networking expertise. SMEs should have a deep understanding of their organization's business processes. Note, it is recommended that each separate organization have SME(s) on the Core Team.

Project Assumptions and Responsibilities

The following reflects the assumptions and responsibilities regarding the Project. Changes in any of the assumptions will affect the scope, Project Schedule, and/or cost of the Project.

Agreement and Schedule Assumptions

- This Cloud Consulting Services Order and the Cloud Program Order have been executed by the Customer, accepted by Hexagon, and the Customer has provided a notice to proceed, Purchase Orders (PO) for both Orders, or written confirmation. Only the execution of the Orders or other acceptance documented in the Primary Contracting Document is necessary to bind the Customer.
- Prior to Project Kickoff, Customer shall have secured any necessary permissions or agreements with Tenants who are to exchange data with Customer and be bound to the responsibilities and obligations of this Order and the Agreement. This includes any required agreements between/among participating organizations.
- The Customer shall perform its assigned Activities set forth in this SOW in the timeframe identified within the Initial Project Schedule (Attachment C) and Project Schedule developed as part of Task: "Project Kickoff Meeting," as modified from time to time. If the Customer requests Hexagon extend the Initial Project Schedule or any subsequent Project Schedule, it acknowledges additional Consulting Services may be necessary for which a Change Order will be required. Note, it is assumed there is only one "Project Kickoff Meeting," unless otherwise negotiated.
- Hexagon will have timely access to Customer Project staff in accordance with the Project Schedule and Tasks. Customer shall make additional personnel available on a priority basis, as needed, to provide subject matter expertise to complete this Project.
- Customer shall have at least one (1): Project Manager, System Administrator, technical resource(s), and SME available to perform and/or support all Customer responsibilities and timely respond to Hexagon requests.

- The Customer shall provide Hexagon with or access to all data, documents, plans, reports, and diagrams, related to this Project and Hexagon responsibilities for this Project.
- Unless otherwise noted in this SOW, all Documentation, if any, provided by Hexagon under this SOW will be COTS Documentation and the Documentation will not be customized by Hexagon. All Documentation delivered will be in Hexagon-approved electronic format.
- Customer, and any Tenants, shall conform to the requirements of the Master Terms, including, but not limited to, those provisions related to the Cloud Program, at all times.
- Unless otherwise stated in the Task, all Tasks will be conducted remotely.
- If the Customer desires additional Services from Hexagon, the Parties can either enter into a separate Order for those Services or enter into a Change Order to explicitly modify this Order. Except for those Services expressly identified as being performed by Hexagon herein, it is not obligated to provide any other or additional Services under this Order.
- Notwithstanding anything to the contrary within the Master Terms, the Customer shall substantively respond to the delivery of a sign-off form within five (5) Business Days as part of the Task Acceptance Process.
- Historical data conversion or importation is not included in this Project.
- Hexagon shall provide its Project Services only during normal Business Hours.
- For meetings or workshops involving both the Customer and Hexagon there will be at least a fifteen (15) minute break every two (2) hours with a one (1) hour lunch break for meetings scheduled to last an entire day (eight (8) hours).

Hardware and Software Assumptions

- Local Software, if any, will be electronically delivered to the Local Environment.
- To the extent Local Software is delivered as part of this SOW, the Customer shall provide access to its Local Environment to Hexagon for the duration of the Project.
- No Local Software will be delivered during the IOC Phase.
- The Customer shall purchase, install, and test all physical hardware comprising the Local Environment.
- The Customer will ensure its hardware, operating system software, and other third-party products/environments conform with Attachment E – System Configuration Diagram.
- Customer shall purchase all applicable operating systems and software in the Local Environment, including, but not limited to, client workstations, and ensure such operating systems and software meet the minimum requirements as defined in Attachment E System Configuration Diagram.
- Customer shall be responsible for the wired and wireless connectivity between servers/clients and clients/clients and with the Cloud Applications.
- To the extent the Customer desires to use the Cloud Program or other deliverables provided herein in a manner or in combination with software or hardware that is not certified or recommended by Hexagon, then the Customer shall be solely responsible for such use. Hexagon shall not be responsible for the correction of any Errors, reduced performance, compromised functionality, or other unintended consequences arising from such use. The Customer also shall not withhold acceptance of any Task or the Cloud Program due to such use.

System Access Assumptions

- The Cloud Program shall store data (in either transit or at rest) in the Cloud Tenant. Customer is solely responsible for (i) assuring it is permitted by appropriate government organizations to transmit the intended information and store data (in either transit or at rest) in the Cloud Tenant

and (ii) otherwise complying with and ensuring this Project and the Cloud Program to be provided does not violate applicable government regulations.

- Customer shall purchase, install, configure, and administer its Network Infrastructure, including, but not limited to, its WAN/LAN and wireless infrastructure.
- Customer consents to Hexagon's inspection and use of Customer's data and systems, including, but not limited to, log files and databases, for the limited purpose of providing the Cloud Services and Cloud Consulting Services.
- If necessary, Hexagon shall access the Cloud Program, including Local Software, and Customer Data via a [redacted]
- The Customer is responsible for ensuring its data communications infrastructure and devices comply with applicable government requirements.

Third-Party Assumptions

- Customer shall schedule and coordinate third-party technical resources with the skills necessary to perform and/or support all Customer Responsibilities, respond to Hexagon requests, and support the testing of Interfaces, as required.
- Customer shall maintain, in good working order, all third-party systems which will integrate with Hexagon software or on which the Hexagon software depends as part of this Project except for the Third-Party Software included as part of the Cloud Program and provided thereunder.
- Customer shall be responsible for the operation and timely availability of external systems or third-party software necessary for the execution of the Project, if any.
- If a delay in the Project is caused by a third-party vendor or Tenants, Hexagon services not covered in this SOW may be required at additional costs.

Training and Development

Hexagon shall provide the Customer access to user and system administration documentation for HxGN Connect and related product component documentation.

At the Project Kickoff Meeting, Hexagon will also provide the Customer e-learning credentials (the "Base eLearning Credentials") for the e-learning courses purchased in the Quote accompanying this SOW ("Base eLearning Courses").

The e-learning classes reflect Hexagon's latest learning and training tool, which can and should be used throughout the Project. The product Documentation and Base e-learning Credentials may be used at all times during the Project; however, the Customer's access to the Base e-learning Credentials shall end one (1) year after formation of this Order, unless otherwise renewed. The Training Program Statement for the Base e-learning Credentials provided in this Project, is described in Attachment D, which may be supplemented with other Training Program Statements for additional e-learning classes purchased and not identified in this SOW.

The Customer should take advantage of these tools during all Phases of the Project. The comprehensive use of these learning tools will facilitate a better transition to HxGN Connect and can lead to more constructive exchanges with Hexagon resources during workshops and consulting sessions. As denoted at certain Tasks, certain prerequisites for Tasks will include Customer personnel having read the relevant sections of the Documentation and/or watched the relevant e-learning course.

Project Initiation

Prior to the Project Kickoff Meeting and after placement of the Order, the following initial Activities must be performed before any Tasks can occur:

- The Hexagon Project Manager will contact the Customer Project Manager. During this initial contact, the Hexagon Project Manager will:
    - Identify the Project Start Date, which should be within two (2) business days prior to the Project Kickoff Meeting;
    - Schedule the Project Kickoff Meeting;
    - Provide an agenda describing the goals of the Project Kickoff Meeting; and
    - Discuss factors that could affect the Project (*e.g.*, scheduling conflicts, communication factors, change management and other risk factors).
- Hexagon's Project Manager shall update the Initial Project Schedule to reflect local holidays; Hexagon resource availability; and any additional Services, Software, or other items included within the Order, identify the Project State Date, and provide the Updated Initial Project Schedule to the Customer Project Manager prior to the Project Kickoff Meeting.
- Hexagon shall provide the Customer an electronic copy of the User and System Administrator Documentation for HxGN Connect prior to the Project Kickoff Meeting.

Project Tasks

IOC Phase

1. Project Kickoff Meeting

Task Description

The objective of this Task is to confirm the updated Initial Project Schedule (Attachment C) provided on the Project Start and provide an overview of the Project. A meeting for Project Kickoff will be held after the Project Start date. There will be only one Project Kickoff meeting, regardless of how many Tenants are included in the Project. The Kickoff Meeting may be held in conjunction with the Kickoff Meeting for the OnCall Dispatch Order or independently.

The Project Kickoff Meeting shall last no more than one (1) hour.

During this Task, the Parties, including representatives from the Tenants, shall confirm the updated Initial Project Schedule as updated by the Hexagon Project Manager. The resulting updated Initial Project Schedule shall be substantially similar in duration as provided within Attachment C unless accepted by Hexagon. Prior to the Project Kickoff Meeting Task, the Customer Project Manager shall have reviewed the updated Initial Project Schedule and be in a position to succinctly identify any needed changes understanding material extensions of the Initial Project Schedule may require additional Hexagon Services to be added via a Change Order. Once the list of changes has been made to the updated Initial Project Schedule by the Hexagon Project Manager, the Hexagon Project Manager will thereafter provide the Project Schedule to the Customer Project Manager. From time to time, the Parties' Project Managers may modify the Project Schedule upon mutual written consent or upon transmission of an updated Project Schedule to the Customer Project Manager as part of a status report and the Customer Project Manager offers no objection to the updated Project Schedule within five (5) Business Days thereafter.

As part of the Project Kickoff Meeting, the Hexagon Project Manager shall provide to Customer: (i) access credentials to Hexagon online training materials and (ii) any applicable Interface Worksheets (as described in the Interface Addendum). At the Project Kickoff Meeting, the Customer shall provide: (i) contact information for all members of its Core Team and Executive/Departmental Sponsor, (ii) proposed alterations to the updated Initial Project Schedule, (iii) contact information for any third party vendors which HxGN Connect will integrate as contemplated in the Interface Addendum, (iv) review and complete the onboarding information worksheet (Attachment J), and (v) identify to Hexagon any perceived concerns or risks with the Project.

Task Deliverables

- Project Schedule
- Access credentials to Hexagon online training materials
- Onboarding information worksheet (Attachment J)

Task Prerequisites

- The Cloud Consulting Services Order and Cloud Program Order have been accepted in writing by the Customer and the Customer has issued to Hexagon Purchase Orders for the full amount reflected in both Quotes (or the Customer has indicated in writing it does not need to issue Purchase Orders to facilitate transactions of this type).
- Hexagon Project Manager has verbally communicated with the Customer to (i) identify the Project Start date and (ii) coordinate a date for the Project Kickoff Meeting.
- Customer has assigned a Customer Project Manager.

- Customer's Core Team has reviewed this SOW.
- Customer is in compliance with Attachment E – System Configuration Diagram.

Task Assumptions

- The Core Team, representatives from the Tenants, and the Hexagon Project Manager shall attend the Project Kickoff Meeting.
- The Project Kickoff Meeting will last no more than one (1) hour unless otherwise extended because other SOWs are to be discussed (as described above).

Hexagon Team Participation and Responsibilities

- The Hexagon Project Manager shall attend the Project Kickoff Meeting
- Hexagon shall:
    - Provide an overview of this Project and address non-technical questions;
    - Conduct an overview of the Project including a review of the SOW to verify all aspects of the Project approach;
    - Establish status reporting requirements (but no more frequently than once per month);
    - Provide the Customer the Base e-Learning Credentials for the Base e-learning Courses;
    - Gather information from the customer to complete the onboarding information worksheet; and
    - Prepare the updated Initial Project Schedule the parties will review during the Project Kickoff Meeting.

Customer Team Participation and Responsibilities

- The Core Team shall attend the Project Kickoff Meeting.
- The Customer shall:
    - Provide Hexagon: contact information for all members of its Core Team and Executive/Departmental Sponsor, (ii) proposed alterations to the updated Initial Project Schedule, and (iii) contact information for any third-party vendors which the HxGN Connect Program will integrate.
    - Provide information to complete the onboarding information worksheet; and
    - Identify any perceived risks or concerns.

Task Acceptance Criteria

This Task is complete at the conclusion of the Project Kickoff Meeting and delivery of the Project Schedule to Customer.

2. HxGN Connect Cloud Tenant Creation

The objective of this Task is to create and “spin-up” the Customer’s Production Tenant for the HxGN Connect Program.

The Production Tenant will be used by Customer during the Project and serve as the basis for the Production Tenant upon Cloud Cutover. Hexagon will inform the Customer once the applicable Production Tenant for Customer has been created.

Task Prerequisites

- Project Kickoff Meeting Task is complete.

Task Assumptions

- None

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Create the Production Tenant (only Production Tenant at this Task) with the HxGN Connect Cloud Program (excluding Interfaces) identified in the Cloud Program Order, which will be used for subsequent Tasks (Customer is not provided Credentials/License Keys at this time).

Customer Team Participation and Responsibilities

- None.

Task Acceptance Criteria

This Task shall be complete upon creation of the Customer’s Production Tenant for the HxGN Connect Cloud Program.

3. HxGN Connect Administrator Training

Task Description

The objective of this Task is to have the Core Team prepare for the subsequent Tasks. HxGN Connect Administrator training consists of e-learning training curricula (subject to being purchased) intended for the persons responsible for administering and configurating the HxGN Connect system (see Attachment D). Customer will complete its review of the Administrator and User training and other training Documentation ("IOC Training Materials") within 30 Business Days from the end of the Project Kickoff Meeting Task ("System Administrator Training Period").

Example topics in this Base e-learning Curricula include:

- Creating and managing user accounts
- Access management – creating and managing access tokens for API interfaces
- Defining HxGN Connect screen layouts
- Configuring map display data

Task Prerequisites and Assumptions

- Hexagon has provided access to Hexagon Base eLearning Credentials to Customer.
- HxGN Connect Cloud Tenant Creation Task is complete.
- No Hexagon live training is provided as part of IOC.

Hexagon Team Participation and Responsibilities

- None

Customer Team Participation and Responsibilities

Customer shall:

- Ensure its Project Manager has distributed access credentials to Hexagon online training materials and training Documentation to Core Team;
- Ensure its Core Team views and reads IOC Training Materials; and
- Manage the Customer's training compliance and report to Hexagon Project Manager once the Customer Core Team has completed the requirements of this Task.

Task Acceptance Criteria

This Task is complete upon the earlier of: (i) the Customer Project Manager reports the Customer Core Team has viewed and read the IOC Training Materials or (ii) the System Administrator Training Period has lapsed.

4. IOC Completion

This Task serves as a milestone and culmination of the previous Tasks. It is at this point in the Project that: Hexagon has created all relevant license keys and set up the Tenant account(s). Hexagon will host a virtual meeting with the Customer project manager and designated system administrator(s) to (i) deliver the Credentials/License Keys applicable to the Cloud Program, and (ii) walk the system administrator(s) through the steps to logon and setup the initial Tenant account(s) and guide the system administrator(s) in setting up the initial default user interface forms. Note, if additional virtual meetings are desired for each organization, they can be quoted.

Completion of this Task also serves to mark the completion of IOC Phase.

Task Deliverables

- Delivery of Credentials/License Keys for Cloud Program included within the Quote.
- Customer can login to the Cloud Program using Credentials/License Keys and navigate to the initial user interface screens.

Task Prerequisites

- HxGN Connect Cloud Tenant Creation Task is complete.

Task Assumptions

- Customer has necessary hardware, equipment, and Network Infrastructure ready and available to access the Cloud Program.
- The Credentials Delivery Meeting is of a limited duration and only intended to cover the two topics specified above.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Host the Credentials Delivery Meeting;
- Deliver Credentials/License Keys for Cloud Program;
- Ensure the Customer can log into the Cloud Program to confirm connectivity; and
- Address Customer reported issues with accessing HxGN Connect.

Customer Team Participation and Responsibilities

Customer shall:

- Ensure its Project Manager and System Administrator(s) attend the Credentials Delivery Meeting. Note, if the Customer desires a separate meeting for each Tenant, additional meetings can be quoted;
- Access the HxGN Connect Program via the Credentials/License Keys provided during the Credentials Delivery Meeting;
- Report to Hexagon verbally during the Credentials Delivery Meeting whether the Customer can access the Cloud Program or identify issues encountered in accessing the HxGN Connect Program; and
- Work collaboratively with Hexagon if Customer encounters issues in accessing HxGN Connect, to troubleshoot and address the issue until resolution.

Task Acceptance Criteria

This Task is complete when Hexagon has delivered the Cloud Program Credentials/License Keys to Customer and confirmed the Customer is able to access HxGN Connect.

FOC Phase

5. Configuration of HxGN Connect Program

Task Description

HxGN Connect is a highly configurable software suite that is intended to be configured by the Customer and reconfigured by the Customer as needs change. This Task is intended to provide the Customer time within the scope of the FOC and Hexagon consulting services, to facilitate Customer's initial configuration of the HxGN Connect Program. This Task is intended only for the Customer. Other Tenants desiring configuration services may separately order or request a Change Order for such Services, which are not included in this scope. This Task assumes the Customer wants assistance in setting up an initial configuration in HxGN Connect. If the Customer does not want assistance with initial system configuration, then this Task shall be regarded as complete.

The Customer shall complete all configurations within thirty (30) days after the Task commences (the "Configuration Period"). Hexagon will host up to two (2), two (2) hour configuration consulting sessions to assist the Customer in configuring HxGN Connect. The first configuration consulting session will occur no earlier than five (5) Business Days after this Task commences. The remaining configuration consulting session should be complete prior to user acceptance testing. Additional configuration sessions can be quoted as requested.

The configuration sessions should be attended by System Administrator(s) and Subject Matter Experts (SMEs) who fully understand their organization's business processes.

Task Deliverables

- HxGN Connect configuration session(s).

Task Prerequisites

- HxGN Connect System Administration Training Task is complete.
- IOC Completion Task is complete.

Task Assumptions

- Customer SMEs have significant knowledge of and/or access to Customer Business Processes.
- Customer has available at least one (1) SME for the HxGN Connect configuration sessions

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Conduct up to two (2) Configuration Session(s).

Customer Team Participation and Responsibilities

Customer shall:

- Make its desired configurations to the HxGN Connect Program within the Configuration Period; and
- Ensure its Core Team, as applicable, attends and participates in the configuration session(s).

Task Acceptance Criteria

This Task is complete upon the earlier of: Customer advising Hexagon it has completed making its configuration changes or the Configuration Period has lapsed.

6. COTS Interface Product Installation and Configuration

Task Description

During this Task, Hexagon will install and unit test the COTS Interfaces in the Customer's Cloud Tenant.

The following are regarded as "COTS Interfaces":

- HxGN Connect Interface | OnCall Dispatch

Although the Customer is expected to participate in Hexagon's internal testing of the COTS Interfaces, the Customer will formally test interface functionality during the User Acceptance Testing Task.

Task Deliverables

- Installation and configuration of the COTS Interfaces

Task Prerequisites

- Operation or availability of all external systems or Third-Party Software.
- IOC Completion Task is complete.

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Install COTS Interfaces in the Customer's Cloud Tenant; and
- Unit test interfaces.

Customer Team Participation and Responsibilities

Customer shall:

- Ensure SMEs are available to support Hexagon Activities as needed.

Task Acceptance Criteria

This Task is complete when each COTS Interface is installed and configured subject to the functionality and features within the COTS version of the COTS Interface.

7. User Acceptance Testing

The objective of this Task is to test the HxGN Connect Program and its interfaces and identify any Blocker Errors.

Following completion of the Configuration of the HxGN Connect Program Task and specified Interface Addendum Tasks, the Customer will test the HxGN Connect Program interfaces to identify Blocker Errors. The UAT will consist of Customer evaluating whether the HxGN Connect Program is able to materially achieve the intended outcome set forth in the Specifications with ordinary use. No other testing or evaluation is contemplated in the FOC Phase of this Project. The Customer shall complete UAT within five (5) Business Days from the latter of: the date the Task Configuration of Cloud HxGN Connect Program is complete or specified Interface Addendum Tasks are complete ("UAT Commencement").

Within one (1) Business Day of the completion of UAT, Customer shall provide the Hexagon Project Manager a written report of any Blocker Errors encountered during UAT ("Blocker Error Report"), if any. For any Blocker Error identified in the Blocker Error Report, the Customer shall provide, at minimum, the following information: a description of the Error and the steps used to reproduce it, the functionality tested when the Blocker Error was encountered, the manner in which the functionality was tested, and the outcome when the functionality was tested. If the Blocker Error Report is not provided to Hexagon within the time allotted, it is presumed UAT was completed without any Blocker Errors, and this Task is complete. The Customer may report Permissive Errors to Hexagon through Hexagon's Customer Resource Management (CRM) system, which will be addressed in accordance with the Master Terms. The existence or Permissive Errors shall not preclude or be a condition of completion of any subsequent Tasks.

Task Prerequisites

- Configuration of HxGN Connect Program Task has been completed.
- COTs Interface Product Installation and Configuration Task is complete.

Task Assumptions

- UAT will consist of only testing the HxGN Connect Program against the Specifications identified in the HxGN Connect Program Order.
- Only qualified Customer personnel will conduct UAT. Qualified Customer personnel are considered resources who have completed the online training sessions required up to this point in the Project and reviewed the identified portions of the System Administration documentation in this SOW in the preceding Tasks.

Hexagon Team Participation and Responsibilities

- None

Customer Team Participation and Responsibilities

Customer shall:

- Complete UAT for the HxGN Connect Program in the manner described above within five (5) Days; and
- Provide the Blocker Error Report within one (1) Business Day following completion of UAT with, at minimum, the details described above.

Task Acceptance Criteria

This Task is complete upon the earlier completion of UAT and tendering the Blocker Error Report to Hexagon or six (6) Business Days from UAT Commencement.

8. Address Blocker Errors from UAT

Task Description

During this Task, Hexagon will investigate, troubleshoot, and resolve valid Blocker Errors documented in the Blocker Error Report. Notwithstanding the Task Acceptance Criteria below, which assumes the existence of Blocker Errors, this Task is complete if the Customer does not timely return the Blocker Report or if the Customer reports the absence of any Blocker Errors. Permissive Test Case Failures are addressed in accordance with the Cloud Support Services provisions of the Master Terms.

After receiving the Blocker Error Report, Hexagon will investigate each Blocker Errors identified in the Blocker Error Report to diagnose the source and cause of the Blocker Error. To the extent requested, Customer agrees to promptly respond to requests for additional information regarding each Blocker Error requested by Hexagon. Upon diagnosing the Blocker Error and validating the Error encountered meets the attributes of a Blocker Error, Hexagon resources shall proceed to resolve the Blocker Error and update the HxGN Connect Program accordingly. If the investigation determines the reported Blocker Error did not meet the attributes of a Blocker Error then the reported Error will be reclassified in accordance with the levels provided in the Master Terms. Alternatively, if the investigation shows the reported Blocker Error was caused by Customer and/or third-party hardware, Network Infrastructure, or software not provided by Hexagon, or non-conformance with Attachment E, then Hexagon will provide such information to the Customer for the Customer to resolve and the Blocker Error will be closed and regarded as complete.

As part of its resolution efforts, Hexagon may at its discretion provide a procedural or programmatic work around, a configuration change, or provide an Update to the HxGN Connect Program. Once the Blocker Error(s) is addressed, Hexagon will report to Customer the Blocker Error has been addressed and the Customer will have five (5) Business Days to test only the resolution to confirm the resolution efforts addressed the Blocker Error (“Resolution Testing Period”)

Upon addressing all Blocker Errors, the HxGN Connect Program is a “**Production Ready System.”** A Production Ready System signifies completion of all configuration and testing Tasks.

Task Deliverables

- Response to Blocker Errors

Task Prerequisites

- User Acceptance Testing Task is complete.

Task Assumptions

- None

Hexagon Team Participation and Responsibilities

Hexagon shall:

- Investigate and address the Blocker Errors reported on the Blocker Error Report; and
- Advise Customer once the valid Blocker Errors have been resolved in a manner described above.

Customer Team Participation and Responsibilities

Customer shall:

- Promptly respond to requests for additional information from Hexagon related to a reported Blocker Error; and

- Test Blocker Error resolution efforts within the Resolution Testing Period.

Task Acceptance Criteria

This Task will be complete when Hexagon has addressed valid Blocker Errors and the Customer has either confirmed the Blocker Errors are resolved or the Resolution Testing Period has lapsed.

9. User Training

The objective of this Task is to facilitate the transfer of knowledge and information necessary for the Users to use the HxGN Connect Program for its intended purposes.

The Customer is solely responsible for training its Users. Appreciating User training is a critical element of the Project, Hexagon has provided specific online training materials for the Core Team (see Attachment D). It is recommended that Customer develop its own training program, including, but not limited to: creating a training plan suitable for its needs and leveraging the Hexagon online training materials and Documentation to ensure its Users have acquired the necessary knowledge and are in a position to use the HxGN Connect Program. The Customer may start User training at any point in the Project. The Customer shall complete its User Training within thirty (30) calendar days after User Acceptance Testing ("User Training Period").

Task Prerequisites and Assumptions

- User Acceptance Testing Task is complete.

Hexagon Team Participation and Responsibilities

- None

Customer Team Participation and Responsibilities

Customer shall:

- Disseminate User training materials to its Users; and
- Complete User training within the User Training Period.

Task Acceptance Criteria

This Task is complete upon the earlier of: (i) the Customer Project Manager reporting the Customer's Users have completed User Training or (ii) the User Training Period has lapsed.

10. System Availability

Task Description

This Task reflects the final Task within the Project.[2] Customizing the HxGN Connect user interface, data sharing options, and workflows can be performed directly in the HxGN Connect production tenant.

Upon completion of this Task the production HxGN Connect system is ready for use. The Customer may use the Cloud Program in production at its convenience.

Task Deliverables

- None

Task Prerequisites

- Achievement of Production Ready System

Task Assumptions

- This is the final Task of the Project, and the Customer may use in production at its convenience.

Hexagon Team Participation and Responsibilities

- None

Customer Team Participation and Responsibilities

- None

Task Acceptance Criteria

This Task is considered complete when all prior SOW tasks have been completed.

[2] For purposes of clarity, the completion of this Task constitutes “Cloud Cutover” notwithstanding any alternate connotation or meaning to the contrary within the Common Terms Glossary.

Attachment A – Pricing Summary

HxGN Connect	Total
Cloud Program Fee	
Year 1 HxGN Connect Cloud Program Fee (Due at IOC Completion)	$30,492
Implementation Services	
HxGN Connect Implementation Services	$83,751
Recurring Cloud Program Fees	
Annual Recurring HxGN Connect Cloud Fee – Year 2	$32,017
Annual Recurring HxGN Connect Cloud Fee – Year 3	$33,617
Annual Recurring HxGN Connect Cloud Fee – Year 4	$35,298
Annual Recurring HxGN Connect Cloud Fee – Year 5	$37,063
Optional Recurring Cloud Program Fees - Years 6-10	
Annual Recurring HxGN Connect Cloud Fee – Year 6	$38,916
Annual Recurring HxGN Connect Cloud Fee – Year 7	$40,862
Annual Recurring HxGN Connect Cloud Fee – Year 8	$42,905
Annual Recurring HxGN Connect Cloud Fee – Year 9	$45,051
Annual Recurring HxGN Connect Cloud Fee – Year 10	$47,303

Pricing Assumptions:

- This offer is valid until December 20, 2024.
- The Dynamo Curriculum/E-Learning Licenses (quantity of 10) included in this pricing are for a 12-month duration to begin once the first training licenses are provided as set forth in this Statement of Work.
- Hexagon's Cloud Program Fees begin upon initial delivery of License Keys and must be renewed annually.
- Sales tax is not included in this quote. Final sales tax billed will reflect the applicable tax rates at time of sale as required by law.

Attachment B – Payment Milestones

The payment milestones percentages below are only for the HxGN Connect described in the HxGN Connect SOW. The total fee for implementation of HxGN Connect is $83,751.

PAYMENT MILESTONE	PAYMENT (%)
Upon Completion of Task: Project Kickoff Meeting	50%
Upon Completion of Task: Address Blocker Errors from UAT	50%

HxGN Connect Cloud Program Order: For purposes of clarity, the Cloud Program Fee for the first year of the Cloud Program is $30,492 and the Cloud Program Fee for the second year of the Cloud Program is $32,017 and is due in accordance with the Agreement.

Attachment C – Initial Project Schedule

Task Name	Duration	Business Days Since Start
Hexagon Connect – Project Plan	**106.16 days**	**0 days**
Initial Operation Capability (IOC) Phase	**38.16 days**	**2 days**
HxGN Connect Cloud Tenant Creation	**0.13 days**	**10 days**
Project Kickoff Meeting	**8 days**	**2 days**
HxGN Connect Administrator Training	**30 days**	**10.13 days**
Customer Core Team Completes Dynamo - Connect Admin Training	30 days	10.13 days
IOC Phase Completion	**30.03 days**	**10.13 days**
PM sets up the hand off meetings with the customer Tenants	0.03 days	40.13 days
Final Operation Capability (FOC) Phase	**66 days**	**40.16 days**
Configuration of HxGN Connect Program	**30 days**	**40.16 days**
Customer configures Connect	30 days	40.16 days
Configuration Consulting Session 1	1 day	44.16 days
Configuration Consulting Session 2	1 day	60.16 days
Hexagon installs the Connect Gateway for I/CAD or OCD interface connectivity	2 days	60.16 days
Connect configuration support during Customer Configuration	30 days	40.16 days
COTS Interface Product Installation and Configuration	**1 day**	**40.16 days**
User Acceptance Testing	**6 days**	**70.16 days**
Customer executes User Acceptance Testing	5 days	70.16 days
Customer Provides Blocker Error Report	1 day	75.16 days
Address Blocker Errors from UAT	**8 days**	**76.16 days**
HxGN addresses blocker errors	1 day	76.16 days
Customer Tests Resolved Blocker Errors	5 days	79.16 days
Production Ready System	**0 days**	**84.16 days**
User Training	**30 days**	**76.16 days**
Customer conducts user training	30 days	76.16 days
System Availability	**1 day**	**84.16 days**

Attachment D – Training Courses Curriculum

The following is a list of HxGN Connect E-Learning courses offered by Hexagon:

- Dynamo Curriculum: HxGN Connect – Admin (HXTC0007)
- Dynamo Curriculum: HxGN Connect – User (HXTC0008)

Attachment E – System Configuration Diagram

HEXAGON

Williamson County, TX
HxGN Connect
Managed Service (SaaS) Configuration

December 2024

Client Hardware Specifications

Color Legend

- - - - Hosted services in Cloud Environment
Black – Base products
Red – Optioned products
Green – Customer-furnished products
[redacted]

[redacted]

HEXAGON

Williamson County, TX
HxGN Connect
Managed Service (SaaS) Configuration

December 2024

Color Legend

- - - - Hosted services in Cloud Environment
Black – Base products
Red – Optioned products
Green – Customer-furnished products
[redacted]

E-Learning*

Dynamo Curriculum HxGN Connect Admin **(Qty: 4)**
Dynamo Curriculum HxGN Connect User **(Qty: 6)**

**Each license lasts for one year and can be renewed upon request.*

HxGN Connect Production Cloud Tenant

[redacted]

On-Premise Environment

[redacted]

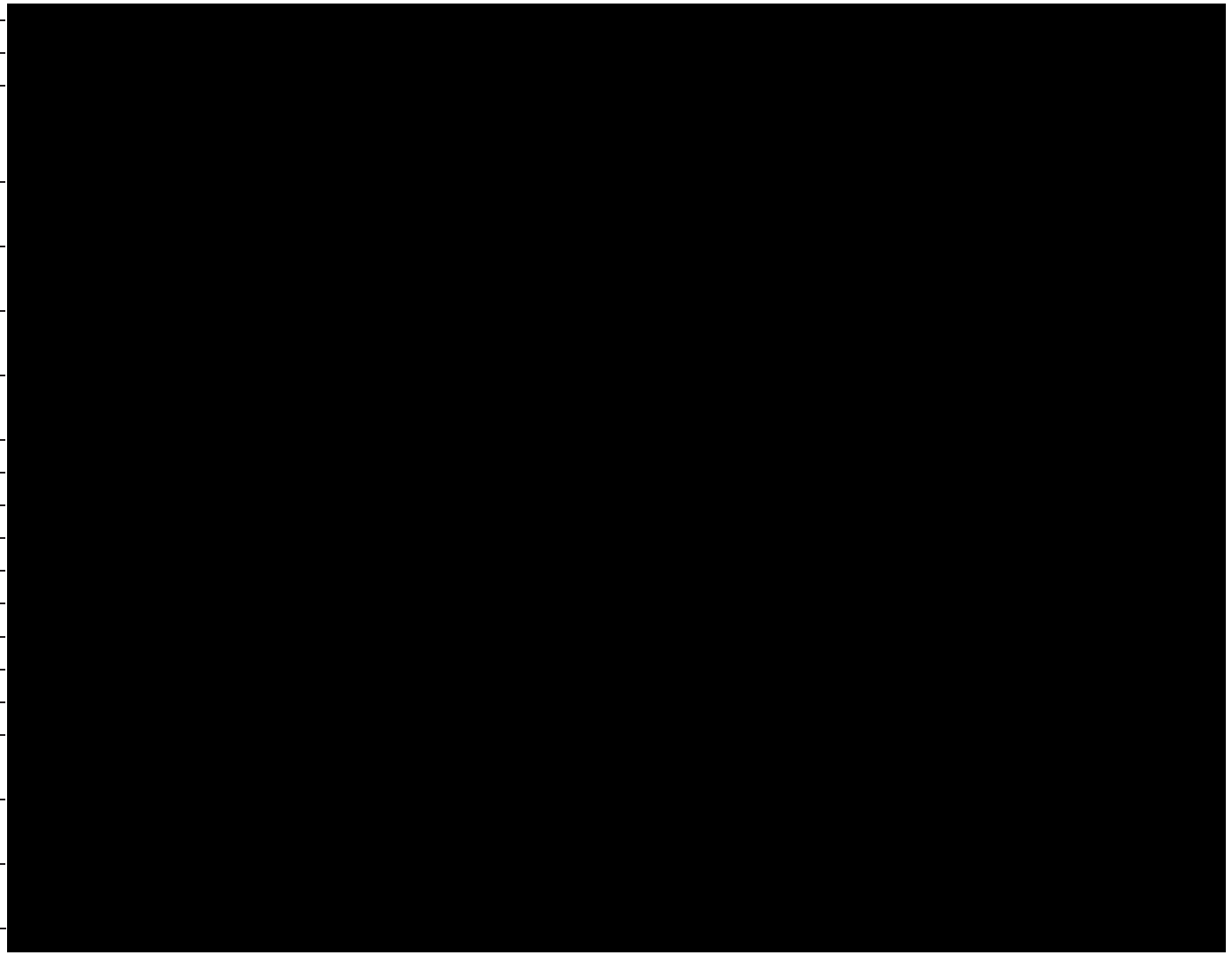
Attachment F – Functional Specifications Matrix

This matrix is intended to provide a list of all functionality HxGN Connect can perform. Please note functionality is only available for purchased Cloud Programs that match the application listed in the bill of materials in Attachment A.

HxGN Connect Live Share Capabilities Matrix (2024.09) – Cloud

9/30/2024

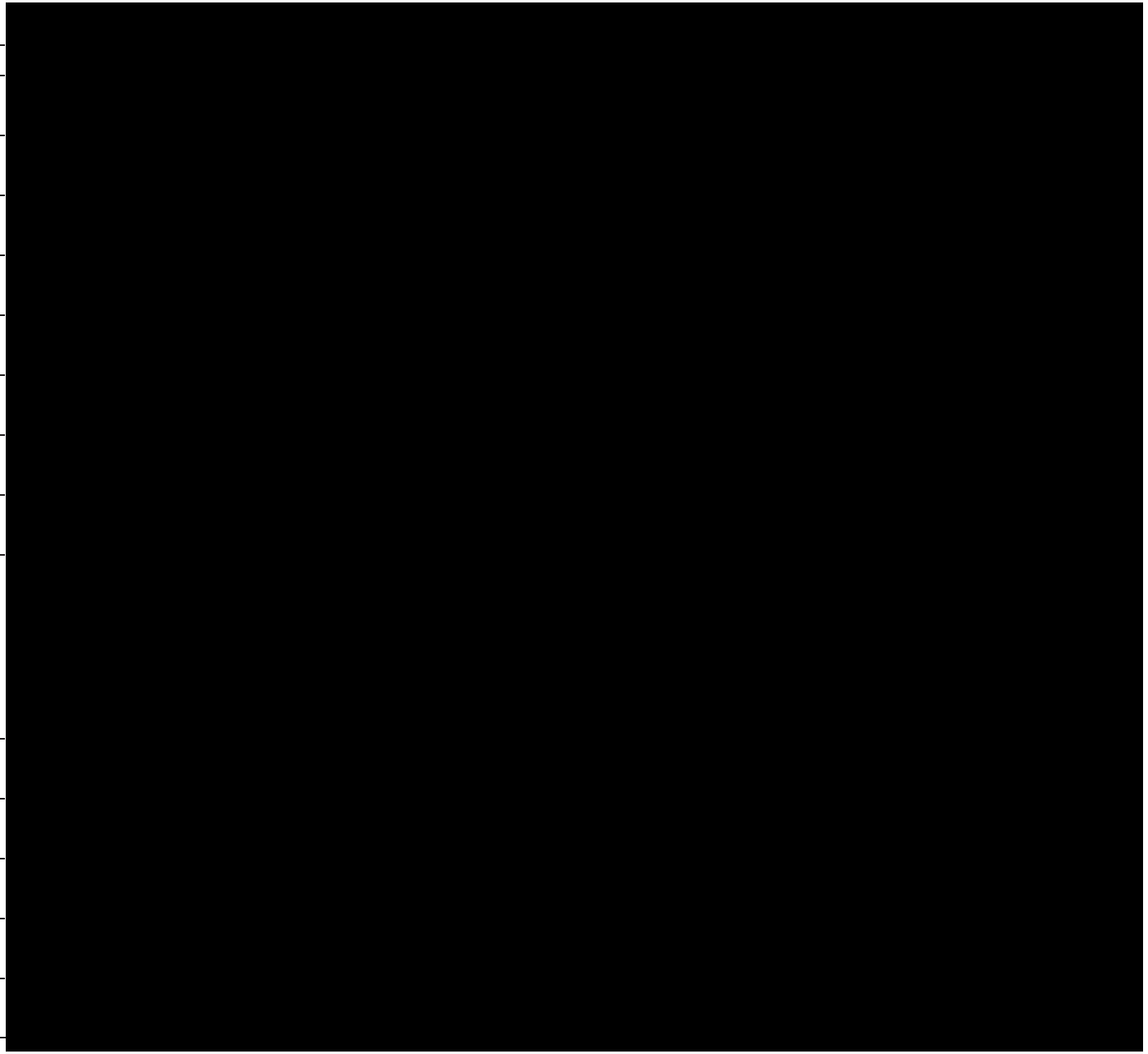
	Section
1.	About
2.	Administration
3.	Administration
4.	Administration
5.	Administration
6.	Administration
7.	Administration
8.	Administration
9.	Administration
10.	Administration
11.	Administration
12.	Administration
13.	Administration
14.	Administration
15.	Administration
16.	Administration
17.	Administration
18.	Administration



	Section	[redacted]
19.	Administration	
20.	Administration	
21.	Administration	
22.	Administration	
23.	Administration	
24.	Administration	
25.	Administration	
26.	Administration	
27.	Administration	
28.	Administration	
29.	Administration	
30.	Administration	
31.	Administration	
32.	Administration	
33.	Administration	
34.	Administration	
35.	Administration	

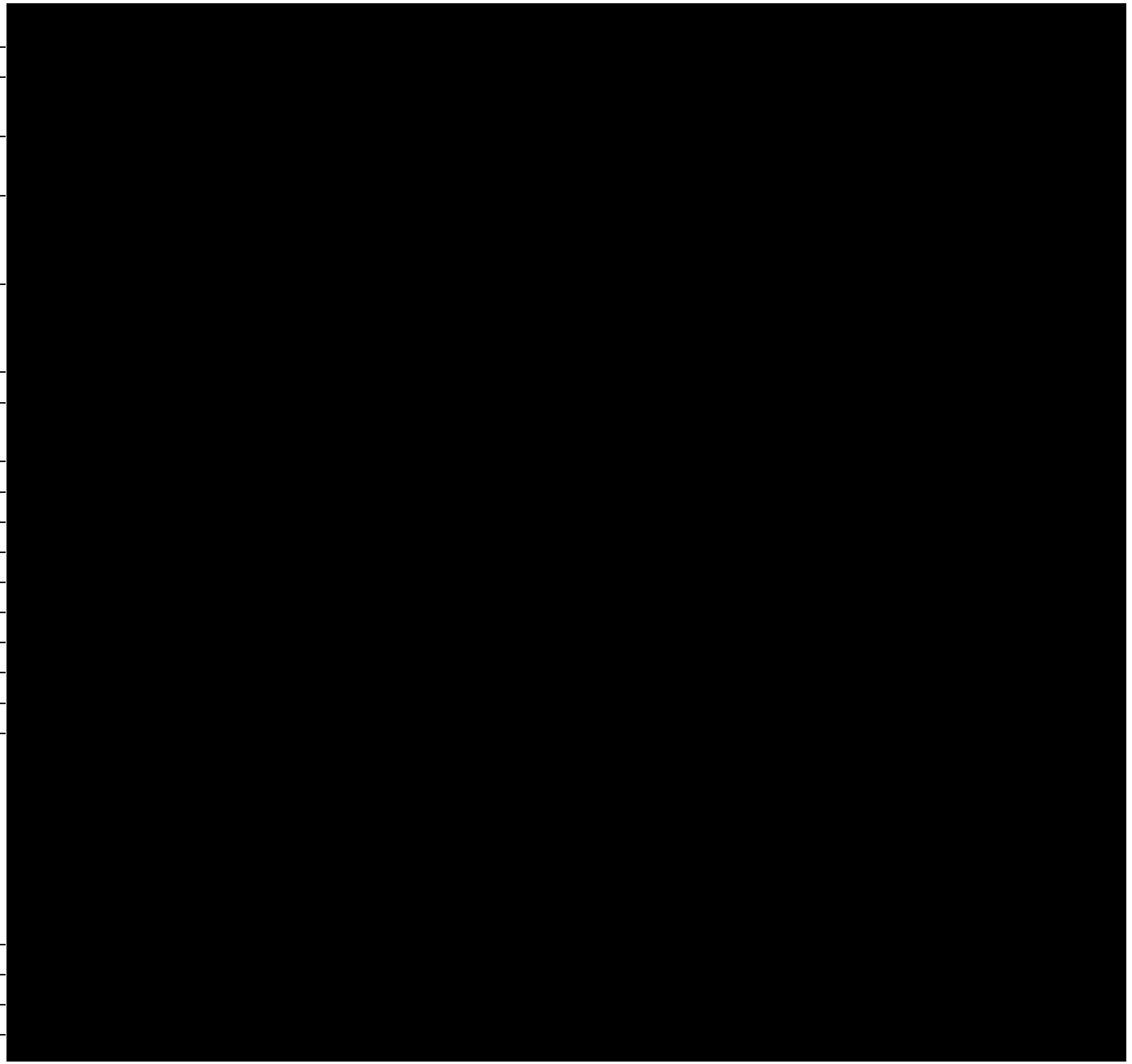
	Section	[redacted]
36.	Administration	
37.	Administration	
38.	Administration	
39.	Administration	
40.	Administration	
41.	Administration	
42.	Administration	
43.	Administration	
44.	Administration	
45.	Administration	
46.	Administration	
47.	Administration	
48.	Administration	
49.	Administration	
50.	Administration	
51.	Administration	
52.	Administration	
53.	Administration	

	Section
54.	Administration
55.	Administration
56.	Administration
57.	Administration
58.	Administration
59.	Administration
60.	Administration
61.	Administration
62.	Administration
63.	Administration
64.	Administration
65.	Administration
66.	Administration
67.	Administration



	Section	[redacted]
68.	Administration	
69.	Administration	
70.	Administration	
71.	Administration	
72.	Administration	
73.	Administration	
74.	Administration	
75.	Administration	
76.	Administration	
77.	Administration	
78.	Administration	
79.	Administration	
80.	Administration	
81.	Administration	
82.	Administration	
83.	Administration	
84.	Administration	
85.	Administration	
86.	Administration	
87.	Administration	
88.	Administration	
89.	Administration	
90.	Administration	

	Section
91.	Administration
92.	Administration
93.	Administration
94.	Administration
95.	Administration
96.	Administration
97.	Administration
98.	Alarms
99.	Alarms
100.	Alarms
101.	Alarms
102.	Alarms
103.	Alarms
104.	Alarms
105.	Alarms
106.	Alarms
107.	Alarms
108.	Alarms
109.	Alarms



	Section
110.	Alarms
111.	Alarms
112.	Assets
113.	Assets
114.	Assets
115.	Assets
116.	Assets
117.	Assets
118.	Assets
119.	Assets
120.	Assets
121.	Assets
122.	Assets
123.	Assets
124.	Channel
125.	Channel
126.	Channel
127.	Channel
128.	Channel

[redacted]

	Section	[redacted]
129.	Channel	
130.	Channel	
131.	Channel	
132.	Channel	
133.	Channel	
134.	Channel	
135.	Channel	
136.	Channel	
137.	Channel	
138.	Channel	
139.	Channel	
140.	Channel	
141.	Channel	
142.	Channel	
143.	Chat	
144.	Chat	
145.	Chat	
146.	Chat	
147.	Chat	
148.	Chat	
149.	Chat	

	Section
150.	Chat
151.	Chat
152.	Chat
153.	Chat
154.	Chat
155.	Chat
156.	Chat
157.	Chat
158.	Chat
159.	Devices
160.	Devices
161.	Devices
162.	Devices
163.	Devices
164.	Devices
165.	Devices
166.	Devices
167.	Devices
168.	Devices
169.	Devices
170.	Devices
171.	Facebook
172.	Help

[redacted]

	Section
173.	Image Feed
174.	IFrame
175.	Incidents
176.	Incidents
177.	Incidents
178.	Incidents
179.	Incidents
180.	Incidents
181.	Incidents
182.	Incidents
183.	Incidents
184.	Incidents
185.	Incidents
186.	Incidents

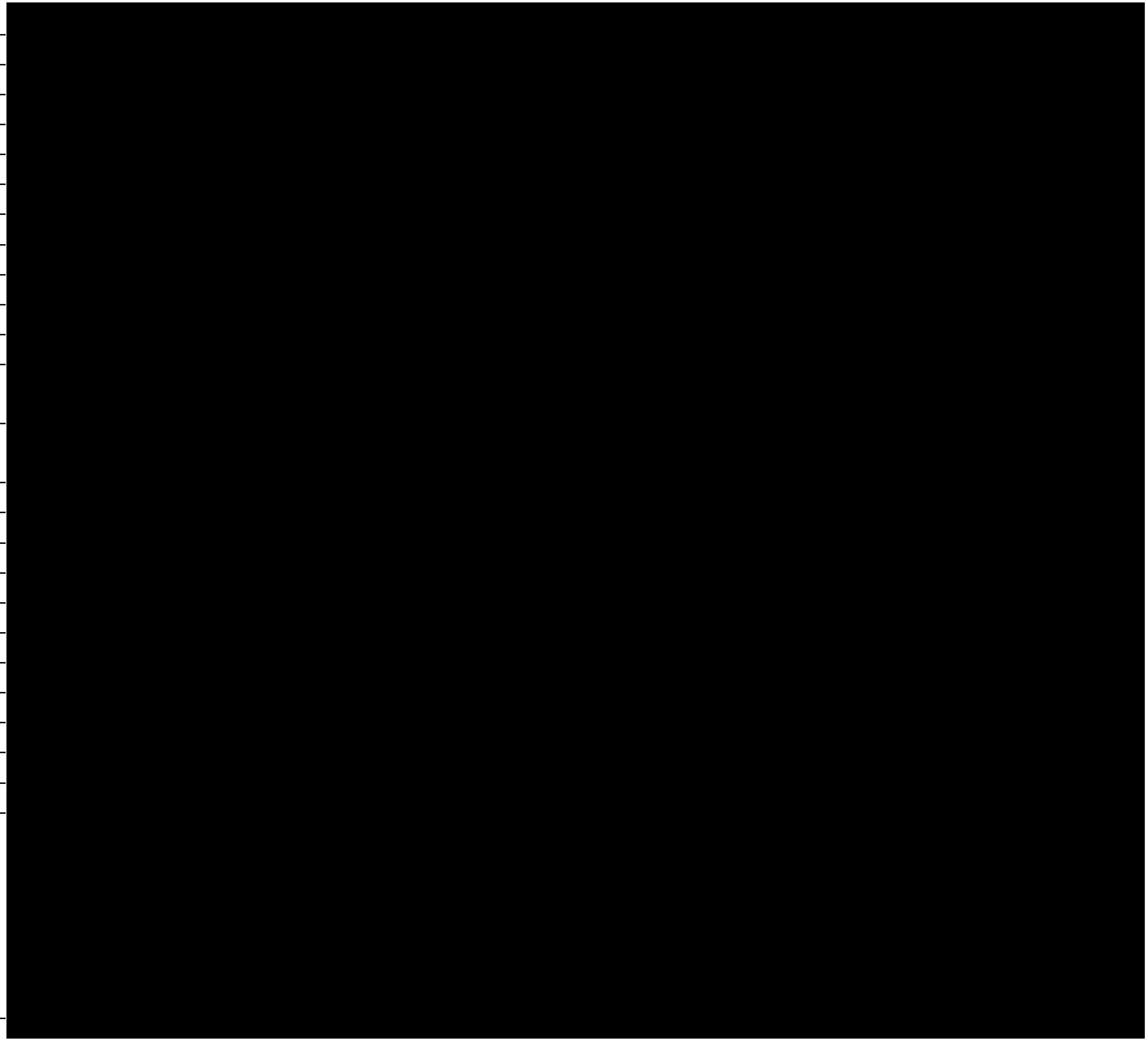
[redacted]

	Section	[redacted]
187.	Incidents	
188.	Incidents	
189.	Incidents	
190.	Incidents	
191.	Incidents	
192.	Incidents	
193.	Insights	
194.	Insights	
195.	Insights	
196.	Insights	
197.	Insights	
198.	Insights	
199.	Insights	
200.	Links	
201.	Luciad	
202.	Map	

	Section
203.	Map
204.	Map
205.	Map
206.	Map
207.	Map
208.	Map
209.	Map
210.	Map
211.	Map
212.	Map
213.	Map
214.	Map
215.	Map
216.	Map
217.	Map
218.	Notifications
219.	Notifications
220.	Notifications
221.	Notifications
222.	Notifications
223.	Notifications

[redacted]

	Section
224.	Notes
225.	Notes
226.	Notes
227.	Notes
228.	Notes
229.	Notes
230.	Notes
231.	Notes
232.	Notes
233.	Notes
234.	Organizations
235.	RSS
236.	Shapes
237.	Shapes
238.	Shapes
239.	Shapes
240.	Shapes
241.	Shapes
242.	Shapes
243.	Shapes
244.	Shapes
245.	Shapes
246.	Shapes
247.	Shapes



	Section
248.	Shapes
249.	Shapes
250.	Shapes
251.	Shapes
252.	Shapes
253.	Shapes
254.	Units
255.	Units
256.	Units
257.	Units
258.	Units
259.	Units
260.	Units
261.	Units
262.	Units
263.	Units
264.	User Profile
265.	User Profile
266.	User Profile
267.	User Profile
268.	User Profile
269.	User Profile
270.	User Profile

[redacted]

	Section	[redacted]
271.	Workspace	
272.	Video	
273.	Video	
274.	Video	
275.	Video	
276.	Video	
277.	Video	
278.	Video	
279.	Video	
280.	Video	
281.	Video	
282.	Video	
283.	Video	

	Section
284.	Video
285.	Video
286.	Video
287.	Video
288.	Video
289.	Video
290.	Video
291.	Video
292.	Video
293.	Video
294.	Video
295.	Waze
296.	Alarms
297.	Assets
298.	Device
299.	Shapes

[redacted]

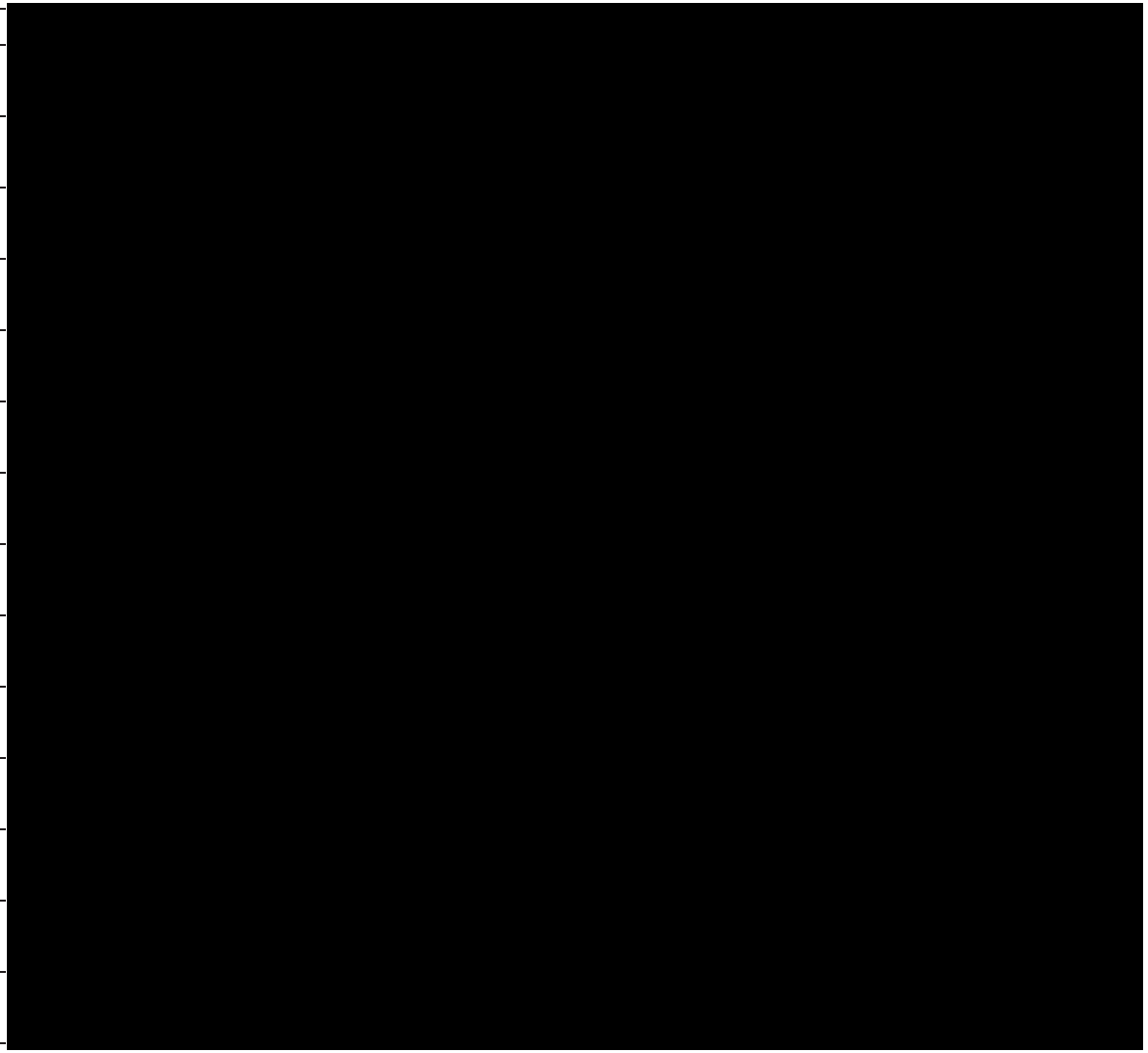
	Section	[redacted]
300.	Incidents	
301.	Units	
302.	Video	
303.	OnCall	

* Provisioner only – Hexagon

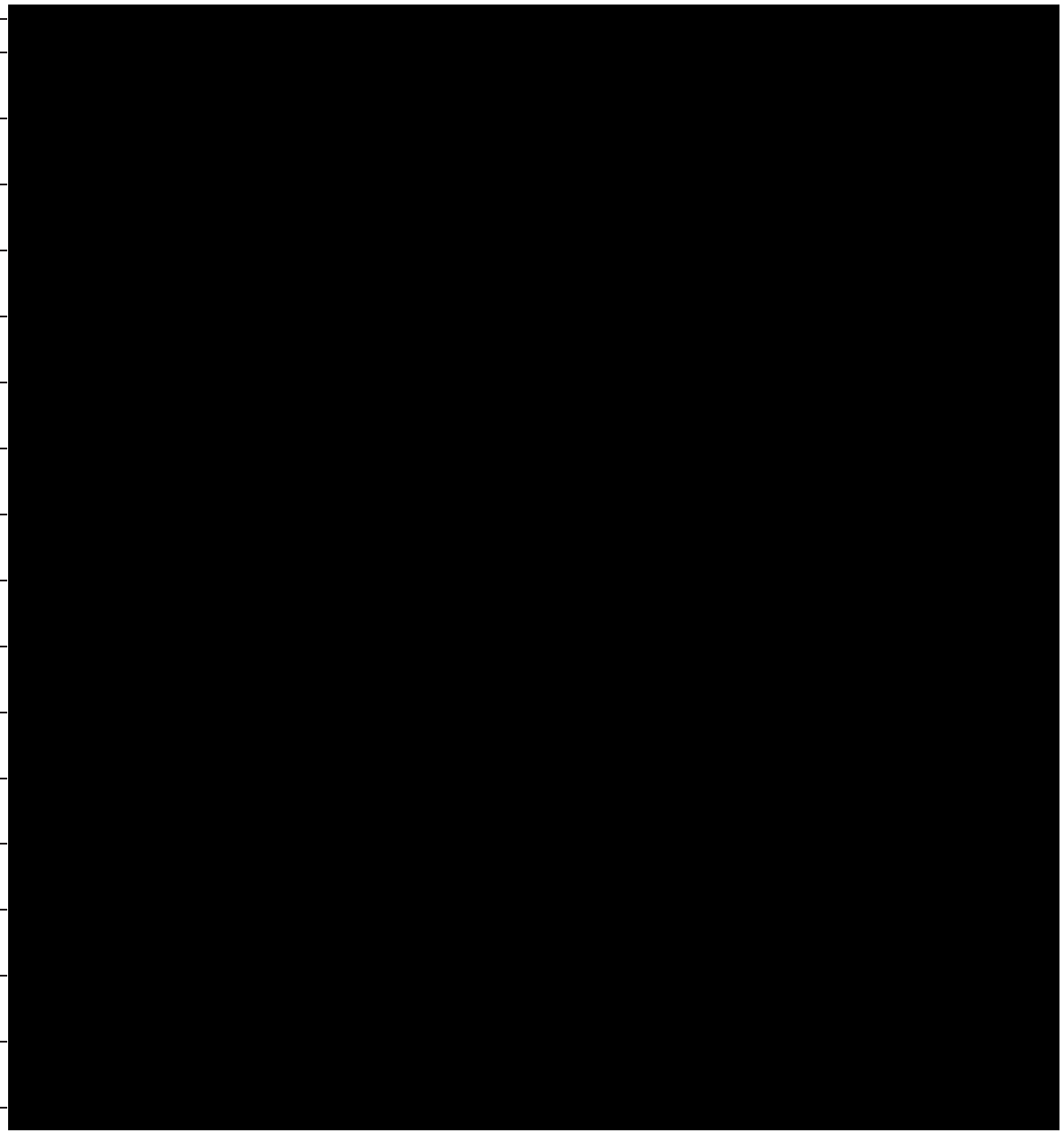
HxGN Connect Live Share | Mobile (2024.09)

9/30/2024

	Section	Category
1.	Menu	Mobile
2.	Menu	Mobile
3.	Menu	Mobile
4.	Menu	Mobile
5.	Chat	Mobile
6.	Chat	Mobile
7.	Chat	Mobile
8.	Chat	Mobile
9.	Chat	Mobile
10.	Chat	Mobile
11.	Chat	Mobile
12.	Chat	Mobile
13.	Chat	Mobile
14.	Chat	Mobile



	Section	Category
15.	Channel	Mobile
16.	Channel	Mobile
17.	Channel	Mobile
18.	Channel	Mobile
19.	Channel	Mobile
20.	Channel	Mobile
21.	Channel	Mobile
22.	Channel	Mobile
23.	Channel	Mobile
24.	Channel	Mobile
25.	Channel	Mobile
26.	Channel	Mobile
27.	Channel	Mobile
28.	Channel	Mobile
29.	Channel	Mobile
30.	Channel	Mobile



	Section	Category
31.	Channel	Mobile
32.	Channel	Mobile

[redacted]

HxGN Connect Interfaces Capabilities Matrix (2024.09) – On-premises

9/30/2024

	Section
1.	Gateway
2.	CSV
3.	OnCall
4.	OnCall
5.	I/CAD 9.4
6.	BLK247

[redacted]

Attachment G – Interface Addendum

[no custom interfaces included at this time]

Attachment H – Glossary of Terms

Capitalized terms within the SOW are defined as follows:

"Benchmark Criteria" or **"Specifications"** means the objective criteria which identifies an intended outcome as reflected in, as applicable, an ICD, a Design Document, or Software Requirements (whichever document having last addressed the functionality in question being dispositive)**.**

"Blocker Error" means a Level One Error.

"Cloud Consulting Services Order" means this Order for Cloud Consulting Services related to the Cloud Applications identified in the HxGN Connect Program Order

"Cloud Program Order" means that certain Order, which identifies the Cloud Applications and Cloud Term, executed simultaneously with this Order. For purposes of clarity, the Cloud Program Order is separate and distinct from the Cloud Consulting Services Order.

"Common Terms Glossary" means that certain collection of defined terms set forth at the link: https://www.hexagonsafetyinfrastructure.com/-/media/Legal/Hexagon/SI/TPS/CTG 06-2021.pdf **"Core Team"** means those certain Customer resources as described in Section 6.

"COTS Interfaces" means those pre-built, product delivered Interfaces specifically identified in the Order Document and the Interface Addendum (if any).

"Customer" means the organization that purchases and has a contract with Hexagon for the HxGN Connect Program. A Customer may have one Tenant (i.e., one organization) or multiple Tenants. For example, a Customer could be a police department, and it could have Tenants for each major department within the police department. In this case it is an INTRA Agency scenario, but with multiple Tenants. There could also be a Customer that is comprised of more than one organization.

"Customer Responsibilities" means (1) those specific tasks and obligations identified in the SOW as being the responsibility of the Customer and (2) those obligations, not stated in the SOW, but which would otherwise be reasonably considered as being Customer obligations and responsibilities.

"Custom Interfaces" means those Interface(s) developed as part of the Project and specifically identified in the Order Document and Interface Addendum (if any).

"Day" means a calendar day.

"Documentation" means any COTS materials describing the system or use of the system. These materials may be delivered only in electronic format, such as online help, e-learning courses, and/or other documentation files delivered with software. Custom versions of documentation will need to be quoted.

"FOC" means Final Operational Capability.

"GIS" means geographic information system

"Hexagon Project Manager" means the person authorized by Hexagon to coordinate and manage the providing of Hexagon Services and Deliverables for the Project on behalf of Hexagon, in addition to being responsible for other duties specified in the Agreement and SOW.

"Initial Project Schedule" means the initial iteration of the Project Schedule, which is contained in Attachment C of the SOW.

"Interface Control Document" or **"ICD"** means a document reflecting the design and requirements of a Custom Interface based upon the requirements set forth in the Interface Addendum.

"IOC" means Initial Operating Capability.

"Network Infrastructure" means the provision of adequate network and internet connectivity to provide sufficient operational bandwidth for the operation of the Cloud Program in a manner consistent with the Product System Specifications together with all industry-standard network security, monitoring, and protection.

"**Permissive Errors**" means a substantially failed Test Case that would correspond to a Level Two, Level Three, or Level Four Error (as defined in the Common Terms Glossary) if the Error occurred in a live environment.

"Production Ready System" means the earlier of: the point at which the Customer is either satisfied with the testing results for the Cloud Program or the resolution of all Blocker Errors reporting during UAT.

"Project Assumptions" means assumptions regarding the Project, which are listed in the SOW. Changes in any of the assumptions will affect the scope, schedule, and/or cost of the Project.

"Project Start" means the date following mutual acceptance of the Cloud Consulting Services Order on which Hexagon communicates to the Customer the Project shall commence.

"Project Team" means the applicable Core Team and other resources assigned to provide information or services in connection with the Project, or applicable part thereof.

"Standard Interfaces" means those Interfaces specifically identified in the Interface Addendum (if any).

"Subject Matter Expert" or "SME" means a person(s) who has particular knowledge about a specific topic(s).

"System Administrator(s)" means a person or persons having the appropriate education, training, and/or experience in information technology to provide first tier support of the System.

"Task Prerequisites" means those events, Deliverables, or accomplishments that are required to occur prior to the commencement of the applicable Task, except as may otherwise be agreed by Hexagon.

"Tenant" means an organization or collection of organizations that is authorized to use HxGN Connect and is subject to the applicable provisions of the Master Terms. The Tenant need not be synonymous with the Customer,

"Updated Initial Project Schedule" means the Initial Project Schedule updated by the Parties' Project Managers during Project Initiation Task and reflecting the actual Project Start.

Attachment I – Reserved

Attachment J – Onboarding Worksheet

The information provided on this worksheet is required to establish a Customer Tenant account in HxGN Connect. Once the Tenant account is created, the person(s) designated as the system administrator can modify this information as needed in HxGN Connect.

Tenant Name: _____

This is the name describing the Tenant in the HxGN Connect application.
Example: *Phoenix Public Works Dept*

[redacted] (U.S. only) _____

Location: _____ _____ _____

City State Country

Primary Administrator email address: _____

The email address of the person designated as the primary system administrator for the HxGN Connect Tenant account.

Industries – Identify the industry most closely associated with your organization

Government

___ Mayor's office

___ Traffic dept

Public Safety

___ EMS/Ambulance

___ Fire Dept

___ Highway Patrol

___ Police Agency

___ Sheriff

Private and Non-Profits

___ Hospital

___ Public Works

___ Transit Company

___ Utility Company

___ Volunteer Group

Attachment K – Cloud Service Schedule

CLOUD SERVICES SCHEDULE

PRODUCT:
Part: HCN1300 – Product Name: HxGN Connect Live Share

CLOUD PLATFORM PROVIDER:
[redacted]

REDUNDANCY:
[redacted]

SERVICE LEVEL:
[redacted]

SERVICE CREDIT:
10% of the monthly fee for this Cloud Application

CLOUD SERVICES SUPPORT AVAILABILITY HOURS:
[redacted]

ADDITIONAL TERMS

Capacity. The product made the subject of this Cloud Services Schedule processes, stores, and displays multimedia, documents, and other attachments as part of collaboration functionality. By purchasing the product, the Customer has purchased the capacity to upload, process, and store a maximum of [redacted] of data in the production environment, and [redacted] of data in any non-production environment, per Customer during each full year of the Cloud Term, beginning with the one year period commencing on the Cloud Program Start Date. (Partial years in the Cloud Term shall be subject to proportionately pro-rated transaction capacity limitations.) If Customer exceeds the purchased storage capacity, Hexagon may, at its election, suspend operation of the product, reduce the operation of the product, or upon Customer's continued use of the product with notice that its usage exceeds purchased capacity, invoice Customer for additional storage as necessary to provide capacity consistent with Customer's actual usage.

Information Sharing. The product (or related products) enables Customer, and actors and entities Customer enables, to share information from systems of record with persons and entities accessing a multi-tenant application, including persons and entities not affiliated with Customer. Through direct action of Customer, or actors and entities it enables, (such as direct adjustment of settings by Customer or agencies enabled by Customer), and/or through action of Hexagon which is directed by Customer in writing, permissions may be configured so as to grant certain information access to some tenants or users accessing the multi-tenant application and deny information access to other tenants. It will be possible to share information with persons and entities unrelated to Customer, dependent upon configuration choices. It is Customer's responsibility to assure the appropriateness and legality of sharing information with those provided access as a result of data sharing configurations made by Customer or actors it enables or made by Hexagon at the written direction of any employee or representative of Customer. By enabling information accessibility options and permissions (either directly, through actors it enables, or thorough written direction to Hexagon as aforesaid), Customer warrants that it is entitled to receive and to share the subject information with all persons and entities to whom access will be enabled, that the sharing of information violates no law or agreement to which Customer is a party, that all agreements required by applicable law or policy to enable the sharing of information are in place, and that Customer has investigated the facts and circumstances necessary to reasonably provide this warranty, including the Credential assignment policies and practices followed by tenants with whom information will be so shared.

CLOUD SERVICES SCHEDULE

PRODUCT:
Part: HCN1301 – Product Name: HxGN Connect Live Share – Smart Advisor

CLOUD PLATFORM PROVIDER:
[redacted]

REDUNDANCY:
[redacted]

SERVICE LEVEL:
[redacted]

SERVICE CREDIT:
10% of the monthly fee for this Cloud Application

CLOUD SERVICES SUPPORT AVAILABILITY HOURS:
[redacted]

ADDITIONAL TERMS

Information Sharing. The product (or related products) enables Customer, and actors and entities Customer enables, to share information from systems of record with persons and entities accessing a multi-tenant application, including persons and entities not affiliated with Customer. Through direct action of Customer, or actors and entities it enables, (such as direct adjustment of settings by Customer or agencies enabled by Customer), and/or through action of Hexagon which is directed by Customer in writing, permissions may be configured so as to grant certain information access to some tenants or users accessing the multi-tenant application and deny information access to other tenants. It will be possible to share information with persons and entities unrelated to Customer, dependent upon configuration choices. It is Customer's responsibility to assure the appropriateness and legality of sharing information with those provided access as a result of data sharing configurations made by Customer or actors it enables or made by Hexagon at the written direction of any employee or

representative of Customer. By enabling information accessibility options and permissions (either directly, through actors it enables, or thorough written direction to Hexagon as aforesaid), Customer warrants that it is entitled to receive and to share the subject information with all persons and entities to whom access will be enabled, that the sharing of information violates no law or agreement to which Customer is a party, that all agreements required by applicable law or policy to enable the sharing of information are in place, and that Customer has investigated the facts and circumstances necessary to reasonably provide this warranty, including the Credential assignment policies and practices followed by tenants with whom information will be so shared.

CLOUD SERVICES SCHEDULE

PRODUCT:
Part: HCN1307 – Product Name: HxGN Connect Interface | Incident API

CLOUD PLATFORM PROVIDER:
[redacted]

REDUNDANCY:
[redacted]

SERVICE LEVEL:
[redacted]

SERVICE CREDIT:
10% of the monthly fee for this Cloud Application

CLOUD SERVICES SUPPORT AVAILABILITY HOURS:
[redacted]

ADDITIONAL TERMS

Capacity. The product made the subject of this Cloud Services Schedule is a particular Application Programming Interface ("API") used to interface systems or applications. Each call to this API represents a transaction across the API. These transactions typically consist of requests to create, update, or delete a data record in an environment, product, or application supplied by Hexagon. For each unit of the API product purchased, Customer has purchased the capacity to process a maximum of [redacted] incident transactions in the production environment, and [redacted] incident transactions in any non-production environment across the API during each full year of the Cloud Term, beginning with the one year period commencing on the Cloud Program Start Date. (Partial years in the Cloud Term shall be subject to proportionately pro-rated transaction capacity limitations.) If Customer exceeds the purchased transaction capacity, Hexagon may, at its election, suspend operation of the API, reduce the operation of the API, or upon Customer's continued use of the API with notice that its

usage exceeds purchased capacity, invoice Customer for additional units of the API product as necessary to provide capacity consistent with Customer's actual usage.

Information Sharing. The product (or related products) enables Customer, and actors and entities Customer enables, to share information from systems of record with persons and entities accessing a multi-tenant application, including persons and entities not affiliated with Customer. Through direct action of Customer, or actors and entities it enables, (such as direct adjustment of settings by Customer or agencies enabled by Customer), and/or through action of Hexagon which is directed by Customer in writing, permissions may be configured so as to grant certain information access to some tenants or users accessing the multi-tenant application and deny information access to other tenants. It will be possible to share information with persons and entities unrelated to Customer, dependent upon configuration choices. It is Customer's responsibility to assure the appropriateness and legality of sharing information with those provided access as a result of data sharing configurations made by Customer or actors it enables or made by Hexagon at the written direction of any employee or representative of Customer. By enabling information accessibility options and permissions (either directly, through actors it enables, or thorough written direction to Hexagon as aforesaid), Customer warrants that it is entitled to receive and to share the subject information with all persons and entities to whom access will be enabled, that the sharing of information violates no law or agreement to which Customer is a party, that all agreements required by applicable law or policy to enable the sharing of information are in place, and that Customer has investigated the facts and circumstances necessary to reasonably provide this warranty, including the Credential assignment policies and practices followed by tenants with whom information will be so shared.

CLOUD SERVICES SCHEDULE

PRODUCT:
Part: HCN1308 – Product Name: HxGN Connect Interface | Unit API

CLOUD PLATFORM PROVIDER:
[redacted]

REDUNDANCY:
[redacted]

SERVICE LEVEL:
[redacted]

SERVICE CREDIT:
10% of the monthly fee for this Cloud Application

CLOUD SERVICES SUPPORT AVAILABILITY HOURS:
[redacted]

ADDITIONAL TERMS

Capacity. The product made the subject of this Cloud Services Schedule is a particular Application Programming Interface ("API") used to interface systems or applications. Each call to this API represents a transaction across the API. These transactions typically consist of requests to create, update, or delete a data record in an environment, product, or application supplied by Hexagon. For each unit of the API product purchased, Customer has purchased the capacity to process a maximum of [redacted] unit transactions in the production environment, and [redacted] unit transactions in any non-production environment across the API during each full year of the Cloud Term, beginning with the one year period commencing on the Cloud Program Start Date. (Partial years in the Cloud Term shall be subject to proportionately pro-rated transaction capacity limitations.) If Customer exceeds the purchased transaction capacity, Hexagon may, at its election, suspend operation of the API, reduce the operation of the API, or upon Customer's continued use of the API with notice that its

usage exceeds purchased capacity, invoice Customer for additional units of the API product as necessary to provide capacity consistent with Customer's actual usage.

Information Sharing. The product (or related products) enables Customer, and actors and entities Customer enables, to share information from systems of record with persons and entities accessing a multi-tenant application, including persons and entities not affiliated with Customer. Through direct action of Customer, or actors and entities it enables, (such as direct adjustment of settings by Customer or agencies enabled by Customer), and/or through action of Hexagon which is directed by Customer in writing, permissions may be configured so as to grant certain information access to some tenants or users accessing the multi-tenant application and deny information access to other tenants. It will be possible to share information with persons and entities unrelated to Customer, dependent upon configuration choices. It is Customer's responsibility to assure the appropriateness and legality of sharing information with those provided access as a result of data sharing configurations made by Customer or actors it enables or made by Hexagon at the written direction of any employee or representative of Customer. By enabling information accessibility options and permissions (either directly, through actors it enables, or thorough written direction to Hexagon as aforesaid), Customer warrants that it is entitled to receive and to share the subject information with all persons and entities to whom access will be enabled, that the sharing of information violates no law or agreement to which Customer is a party, that all agreements required by applicable law or policy to enable the sharing of information are in place, and that Customer has investigated the facts and circumstances necessary to reasonably provide this warranty, including the Credential assignment policies and practices followed by tenants with whom information will be so shared.

CLOUD SERVICES SCHEDULE

PRODUCT:
HCN1314 - HxGN Connect - Tennant Access

CLOUD PLATFORM PROVIDER:
[redacted]

REDUNDANCY:
[redacted]

SERVICE LEVEL:
[redacted]

SERVICE CREDIT:
No Applicable

CLOUD SERVICES SUPPORT AVAILABILITY HOURS:
[redacted]

CLOUD SERVICES SCHEDULE

PRODUCT:
Part: HCN1317 – Product Name: HxGN Connect Smart Advisor | Incident Agents

CLOUD PLATFORM PROVIDER:
[redacted]

REDUNDANCY:
[redacted]

SERVICE LEVEL:
[redacted]

SERVICE CREDIT:
10% of the monthly fee for this Cloud Application

CLOUD SERVICES SUPPORT AVAILABILITY HOURS:
[redacted]

ADDITIONAL TERMS

Capacity. The product made the subject of this Cloud Services Schedule is a particular Application Programming Interface ("API") used to interface systems or applications. Each call to this API represents a transaction across the API. These transactions typically consist of requests to create, update, or delete a data record in an environment, product, or application supplied by Hexagon. For each unit of the API product purchased, Customer has purchased the capacity to process a maximum of [redacted] incident transactions in the production environment, and [redacted] incident transactions in any non-production environment across the API during each full year of the Cloud Term, beginning with the one year period commencing on the Cloud Program Start Date. (Partial years in the Cloud Term shall be subject to proportionately pro-rated transaction capacity limitations.) If Customer exceeds the purchased transaction capacity, Hexagon may, at its election, suspend operation of the API, reduce the operation of the API, or upon Customer's continued use of the API with notice that its

usage exceeds purchased capacity, invoice Customer for additional units of the API product as necessary to provide capacity consistent with Customer's actual usage.

Information Sharing. The product (or related products) enables Customer, and actors and entities Customer enables, to share information from systems of record with persons and entities accessing a multi-tenant application, including persons and entities not affiliated with Customer. Through direct action of Customer, or actors and entities it enables, (such as direct adjustment of settings by Customer or agencies enabled by Customer), and/or through action of Hexagon which is directed by Customer in writing, permissions may be configured so as to grant certain information access to some tenants or users accessing the multi-tenant application and deny information access to other tenants. It will be possible to share information with persons and entities unrelated to Customer, dependent upon configuration choices. It is Customer's responsibility to assure the appropriateness and legality of sharing information with those provided access as a result of data sharing configurations made by Customer or actors it enables or made by Hexagon at the written direction of any employee or representative of Customer. By enabling information accessibility options and permissions (either directly, through actors it enables, or thorough written direction to Hexagon as aforesaid), Customer warrants that it is entitled to receive and to share the subject information with all persons and entities to whom access will be enabled, that the sharing of information violates no law or agreement to which Customer is a party, that all agreements required by applicable law or policy to enable the sharing of information are in place, and that Customer has investigated the facts and circumstances necessary to reasonably provide this warranty, including the Credential assignment policies and practices followed by tenants with whom information will be so shared.