

ORDER DOCUMENT

The terms and conditions of the Contract are incorporated into and made a part of this Order Document. Capitalized terms used in this Order Document and not otherwise defined herein will have the meaning assigned to such terms in the Contract.

1. TERMS AND CONDITIONS.

This Order Document and the Attachments referenced in Section 2 below apply only to the products and services described in the pricing summary attached hereto as Attachment A ("**Pricing Summary**") and the Statement of Work attached hereto as Attachment B. Except for any terms and conditions expressly set forth below in this Order Document, the terms and conditions of the Contract control.

2. ATTACHMENTS.

Attachment A – Pricing Summary

Attachment B – Statement of Work

Attachment C – Equipment Addendum

Attachment D – Managed Software-as-a-Service Addendum

Exhibit D-1 – Roles and Responsibilities

Exhibit D-2 – Managed Services Special Terms and Conditions

Exhibit D-3 – Disaster Recovery Terms and Conditions

Exhibit D-4 – Operations Optimizer Terms and Conditions

Attachment E – Wireless Data Service Addendum

Attachment F – Maintenance and Support Addendum

Attachment G – Data Processing Addendum

Attachment H – Network Coverage Commitment

Attachment I – Security Addendum

Attachment J – Software Addendum

3. PRICING.

- a. **Pricing Summary.** Pricing for the products and services identified in the Pricing Summary and the Statement of Work shall be set forth in the Pricing Summary attached to this Order Document as Attachment A.
- b. **Purchase Commitment.** The Authority commits to purchase the quantities set forth in the Pricing Summary. If the Authority fails to purchase the committed quantities by the end of the Term, Itron will retroactively adjust pricing and invoice the Authority for the difference between the amount paid and the amount owed under the adjusted pricing. Customer may adjust the quantity for each line item of Itron Equipment as needed to support the project as long as the total spend for Itron Equipment equals or exceeds the total Itron Equipment price in the Pricing Summary as of the Order Document Effective Date.
- c. **Pricing Period and Pricing Modifications.** Prices for the quantity of Itron Equipment and duration of Itron Recurring Services (as defined below) set forth in the Pricing Summary as of the Order Document Effective Date are effective until December 31, 2028 (the "**Deployment Period**"), and will not be adjusted except as provided below:

- i. On September 1, 2028 , the then-current price will be adjusted for the upcoming calendar year by a percentage equal to the variation of the Index (as defined below) over the prior twelve (12) month period subject to the following.
 - 1. For Itron Equipment, “Index” means the PPI Commodity data for Final demand goods, seasonally adjusted (WPSFD41), as published by the US Department of Labor. The Index is accessible at www.bls.gov/data/.
 - 2. For Itron Maintenance and Support, Managed SaaS, and Distributed Intelligence Pricing (together “**Recurring Services**”), “Index” means the CPI - All items in U.S. city average, all urban consumers, seasonally adjusted (CUSR0000SA0), as published by the US Department of Labor. The Index is accessible at www.bls.gov/data/.
 - ii. For Equipment only, Itron may, from time-to-time upon written notice to the Authority, issue surcharges on new and/or unfulfilled Purchase Orders to offset material increases in Itron’s associated costs arising from: (i) unusual foreign currency exchange variations; (ii) impacts of duties, tariffs, and other government actions(excluding taxes); and (iii) any other macroeconomic circumstances outside of Itron's reasonable control (“Economic Surcharges”). Economic Surcharges will be proportional to the actual increases in Itron’s operating costs. Itron will provide the Authority with advance notice of any Economic Surcharges.
- d. Estimated Pricing.** The pricing summary includes budgetary, non-binding pricing should the Authority elect to purchase Recurring Services following the initial term of the Contract. The estimated pricing is provided for budgeting purposes only and is not guaranteed. Both parties agree to negotiate in good faith to come to mutually aggregable terms for pricing beyond the initial term.

4. PROFESSIONAL SERVICES.

Itron will perform the Professional Services in accordance with the Statement of Work attached hereto as Attachment B to this Order Document.

5. OTHER ATTACHMENTS TO THE ORDER DOCUMENT.

- a. **Equipment Addendum.** The Equipment Addendum (attached hereto as Attachment C) governs the purchase, delivery, and warranty of Equipment purchased by the Authority.
- b. **Managed Software as a Service Addendum.** The Managed Software as a Service Addendum (attached hereto as Attachment D)
- c. **Wireless Data Service Addendum.** The Wireless Data Service Addendum (attached hereto as Attachment E) governs the provision of wireless data services.
- d. **Maintenance and Support Addendum.** Itron provides Maintenance and Support Services in accordance with the Maintenance and Support Addendum (attached hereto as Attachment F).
- e. **Data Processing Addendum.** The Data Processing Addendum (attached hereto as Attachment G) provides requirement for the handling of Personal Data. For the avoidance of doubt, Itron does not collect or process Personal Data.
- f. **Network Coverage Commitment.** The Parties agree to the Network Coverage Commitment as set forth in Attachment H.
- g. **Security Addendum.** The Security Addendum (attached hereto as Attachment I) provides security requirements for the Work.

- h. **Software Addendum.** Itron provides licensed Software to the Authority in accordance with the Software Addendum (attached hereto as Attachment J).

6. DISTRIBUTED INTELLIGENCE.

If the Authority elects to purchase the Distributed Intelligence Platform, the Parties will execute an amendment to add the Distributed Intelligence Application Addendum to this Order Document. Itron will provide the Distributed Intelligence Platform in accordance with the Distributed Intelligence Application Addendum and the AMI Implementation SOW.

7. MISCELLANEOUS.

Except as otherwise expressly provided or modified in this Order Document, the (i) terms and conditions of the Contract (including any addendums attached thereto) remain in full force and effect, and (ii) the Contract, including this Order Document, constitute the entire and exclusive agreement between the Parties regarding the subject matter hereof, and supersede all proposals and prior agreements, oral or written, and all other communications.

ATTACHMENT A TO THE ORDER DOCUMENT

Pricing Summary

**Balance of page intentionally left blank;
Pricing Summary to follow on next page**

ATTACHMENT B TO THE ORDER DOCUMENT

Statement of Work

**Balance of page intentionally left blank;
Statement of Work to follow on next page**

ATTACHMENT C TO THE ORDER DOCUMENT

Equipment Addendum

1. Additional Definitions.

The following defined terms are in addition to those defined in the Agreement General Terms and Conditions:

Deployment Period means the Agreement Effective Date through the completion of System Acceptance Test.

Electricity Meter (or Electric Meter) means a device used to measure and record one or more electrical quantities at a meter point. The meter's programming or configuration determines the numbers and types of quantities it can store.

Equipment means Contractor Equipment and Third-Party Equipment.

Firmware means the object code version of software embedded in Equipment.

Contractor Equipment means equipment listed on an Order Document for sale to Authority under this Agreement that is manufactured and branded by or on behalf of SUPPLIER.

Network Devices means Access Points, Relays, and Socket Access Points.

Third-Party Equipment means equipment listed on an Order Document for sale to Authority under this Agreement that is not manufactured and branded by or on behalf of Contractor.

Warranty Period means the Contractor Equipment warranty period specified in the table in Section 9.

2. Ordering Equipment.

Upon execution of the Agreement, Itron will manage ordering of Equipment based upon agreed installation schedules.

3. Invoicing.

Contractor will invoice Authority for Equipment, and any related surcharges, and reimbursable shipping-related expenses, on the date the Equipment arrives at the port of entry and payment shall be made by Authority in accordance with the terms set forth in the Agreement.

4. Lead Times & Ship Dates.

- a. **TIME, QUANTITY, AND DELIVERY IS OF THE ESSENCE.** The Authority may purchase additional or spare Equipment by issuing a Purchase Order to Contractor. Contractor will assign a scheduled shipment date as close as possible to the Authority's requested date specified in an accepted Purchase Order based on Contractor's then-current lead times ("**Lead Times**"). Upon request, Contractor will inform Authority of current Lead Times. Contractor will work with contracted carriers to minimize any necessary delays, such as due to extreme weather. Contractor will acknowledge receipt by return email to the sender of each Purchase Order within 72 hours of receipt. Contractor will accept or communicate to Authority within one week of receipt of a Purchase Order specific reason(s) for any non-acceptance of a Purchase Order, e.g., incorrect part numbers or unit prices.
- b. **Documentation.** Contractor will provide a Shipping File and Test Results File for Contractor Equipment and of the agreed upon format to the designated SFTP server for automated processing by Authority. Contractor will ensure that the Device File is shipped to the MSaaS Support Center and loaded into the AMI HES prior to the receipt of the Equipment.

5. Equipment Firmware.

The purchase of Contractor Equipment includes a nonexclusive license under Contractor copyrights to use Firmware in Contractor Equipment. The license to any Firmware in Third-Party Equipment purchased by Authority through Contractor shall be between Authority and the manufacturer of the Third-Party Equipment.

6. Returns.

Except as otherwise agreed to in this Equipment Addendum, Contractor does not accept returns unless: (i) Contractor shipped a product or quantity other than as specified in the Purchase Order, and (ii) such product is unused. If the return is attributable to a Contractor error, then Contractor will reimburse Authority for the cost of the return of the product provided such return is provided in accordance with Contractor's then current RMA policy and procedures. Contractor's target RMA processing time from receipt of the returned Contractor Equipment to shipment of the repaired or replaced Equipment is forty-five (45) calendar days.

7. Warranty.

- a. **Contractor Equipment Warranty.** Except to the extent otherwise expressly agreed to by the Parties in writing in an Order Document, Contractor warrants to Authority that the Contractor Equipment will be (i) free from defects in materials and workmanship; and (ii) will comply with and perform in accordance with the applicable published Contractor documentation for the Contractor Equipment, including without limitation data sheets, reference guidance and specifications (collectively "**Specifications**") for the periods set forth below ("**Warranty Period**"). Any subsequent changes to the Specifications during the Warranty Period will not materially impair, diminish or remove Contractor Equipment functionality or performance of the Contractor Equipment purchased by Authority under this Order Document.

Product	Standard Warranty Period	Extended Warranty Period (if purchased)
Access Points (AP)	1 year from shipment	8 years (1+7 years)

Socket Access Point (AP)	1 year from shipment	8 years (1+7 years)
Relays	1 year from shipment	8 years (1+7 years)
Itron AMI Meters	3 years from shipment	8 years (3+5 years)
Field Service Unit (FSU)	1 year from shipment	None

- b. Warranty Remedy.** Except to the extent otherwise provided herein, Contractor's sole obligation and Authority's exclusive remedy in connection with the breach of a warranty provided under this Section 8 shall be for Contractor to, at its option and expense, (i) provide the Authority with a firmware or software fix to correct the nonconformity, (ii) repair non-compliant Contractor Equipment or provide Authority with new replacement Contractor Equipment after Authority has returned non-conforming Contractor Equipment properly packaged and prepaid to a repair facility designated by Contractor in accordance with Contractor's then-current RMA procedures, or (iii) if Contractor determines (in its reasonable judgment) that it is unable to provide a remedy specified in item (i) or (ii) of this section, Contractor will provide the Authority with a refund of the purchase price for the applicable Contractor Equipment. Contractor Equipment that is repaired or replaced pursuant to this Section 10 will be warranted for the remainder of the original warranty period or sixty (60) days, whichever is longer. During the Deployment Period, Contractor will pay the cost of returning non-conforming Contractor Equipment to the place of repair designated by Contractor and Contractor will pay the cost of delivering repaired or replacement Contractor Equipment to Authority. Following the completion of the Deployment Period, the Authority is responsible for any labor costs associated with removal or reinstallation of Contractor Equipment and the Authority will pay the cost of returning non-conforming Contractor Equipment to the place of repair designated by Contractor and Contractor will pay the cost of delivering repaired or replacement Contractor Equipment to Authority.
- c. Exclusions.** The warranty provided herein does not cover Contractor Equipment defects or nonconformities caused by: (i) changes or repairs made to Contractor Equipment without Contractor's prior written consent, (ii) use with cables, mounting kits, antennas, battery backups and other devices, Third-Party software or firmware that Contractor has not provided to Customer or approved in writing for use with Contractor Equipment, (iii) for Equipment stored or installed by the Authority, the Authority's or a Third-Party's (not under Contractor control) misuse, abuse, neglect, negligence, or failure to store, install, test, handle or operate Contractor Equipment in accordance with its Documentation, (iv) a Force Majeure event, or (v) incorrect data, or data entry or output by the Authority or a Third-Party not under Contractor's control. The Authority may request that Contractor repair Contractor Equipment damaged by any of the foregoing; if Contractor agrees to make such repairs, the Authority may be charged additional Fees.

- d. **Disclaimer.** EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, CONTRACTOR DISCLAIMS ALL EXPRESS OR IMPLIED WARRANTIES, CONDITIONS OR REPRESENTATIONS INCLUDING, WITHOUT LIMITATION, (I) IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, (II) WARRANTIES OF TITLE AND AGAINST INFRINGEMENT AND (III) WARRANTIES ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. TO THE EXTENT ANY IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD.

8. **Excessive Failure Warranty.**

- a. **Definition.** “**Excessive Failure**” means the failure of three-and-a-half percent (3.5%) or more of the same model of installed Electricity Meters or eight percent (8%) or more of the same model of installed Network Devices to comply with the Warranty in Section 10(a) resulting from the same root cause, as verified by Contractor, within any rolling twelve (12) month period during the Warranty Period.
- b. **Exclusions.** An Excessive Failure shall not include any Electricity Meters or Network Devices that are outside the applicable Warranty Period at the time of failure or that are excluded from warranty coverage pursuant to Section 8(c) of this Equipment Addendum.
- c. **Process.** If the Authority reasonably believes that an Excessive Failure has occurred during the Excessive Warranty Period, the Authority shall promptly inform the Contractor. Upon receipt of such notice, the Parties shall work diligently to investigate and determine the occurrence of the suspected Excessive Failure. Authority shall provide reasonable support, as well as access to information, records, personnel, facilities, and systems, as reasonably requested by Contractor during the investigation of any suspected Excessive Failure. Each Party shall bear its own expenses incurred during the investigation of a suspected Excessive Failure. Upon verification of an Excessive Failure by Contractor, Contractor shall develop a resolution plan to address and remediate the Excessive Failure and include a quality assurance plan to prevent a similar failure in the future (the “**Excessive Failure Resolution Plan**”). The development of the Excessive Failure Resolution Plan shall be undertaken and completed in a diligent and prompt fashion.
- d. **Contractor Liability for Excessive Failure.** If the plan requires that the failed Electricity Meters or Network Devices be de-installed for repair or replacement, then Contractor will, at its expense, (a) provide qualified field labor to de-install defective Electricity Meters or Network Devices within Authority’s service territory in excess of the Excessive Failure threshold and install conforming replacements for such equipment pursuant to a mutually agreed upon statement of work, or (b) reimburse Authority’s actual, reasonable, and documented costs of performing such de-installation and re-installation work using its own resources in the form of a credit against amounts due by Authority under this Agreement, up to the amount set forth in the below table:

Equipment Type	Per Unit Reimbursement (Not to Exceed)
Electricity Meters	\$40

Access Points and Relays	\$1,500
Socket APs	\$80

- e. **Limitations.** The additional remedies for Excessive Failures during the Warranty Period under this Section 11 will only be available if Authority makes commercially reasonable efforts to: (i) promptly investigate all potentially defective Electricity Meters or Network Devices identified on Authority's most recent system performance and maintenance reports, (ii) promptly return all Electricity Meters and / or Network Devices that fail to satisfy the warranties set forth in Section 10 (Warranty) below the Excessive Failure threshold to Contractor in accordance with Contractor's then-current RMA process, (iii) promptly notify Contractor in writing once Authority believes, acting reasonably, that an Excessive Failure has occurred or is likely to occur, (iv) provides Contractor with access to relevant Authority records as necessary for Contractor to confirm Authority's compliance with the investigation, return and reporting requirements of this Section.

The remedies set forth in this Section 11 (Excessive Failure during Warranty Period), shall be Authority's sole remedy for breach of warranty specific to Excessive Failure during the Warranty Period.

9. Equipment End of Sale.

- a. **Notice.** Contractor will provide Authority with no less than a three hundred and sixty-five (365) day notice period before discontinuing the sale of any Contractor Equipment set forth in an Order Document, provided that pricing for such equipment remains valid and Authority has purchased such Contractor Equipment within the three hundred and sixty-five (365) day period preceding the date upon which notice is to be given. During the foregoing notice period, Authority may place non-cancellable non-returnable "last time buy" Purchase Orders for any Contractor Equipment identified in the end of sale notice. Authority must take delivery of all such Contractor Equipment ordered after receipt of such notification within the three hundred and sixty-five (365) day period of the Purchase Order acceptance date or within thirty (30) days from shipment availability, whichever is longer. Contractor's sole obligation with respect to the discontinuance of Third-Party Equipment is to provide Authority with any end of sale notice that Contractor receives from the Third-Party Equipment manufacturer.
- b. **Replacement Contractor Equipment.** Contractor will not end of sale any Contractor Equipment while the pricing for such Itron Equipment remains valid, other than as a result of a Force Majeure event, without making functionally equivalent replacement equipment available for purchase by Authority, provided such functionality is listed in the Contractor Documentation for such Contractor Equipment in use by Authority. Any such replacement equipment will be backwards compatible and interoperable with other Contractor Equipment and Service Offerings to the same extent as the Contractor Equipment it was designed to replace. Contractor may either (i) disable any new functionality or features provided by the replacement equipment, or (ii) if Contractor is unable to disable any new functionality or features in the replacement equipment, or Authority elects to purchase such new functionality or features, charge Authority the applicable fees for such new functionality or features

10. Third-Party Equipment Warranty.

Contractor is not the manufacturer of the Third Party Equipment and makes no representations or warranties whatsoever, directly or indirectly, express or implied, as to the durability, fitness for use, merchantability, condition, quality, performance or non-infringement of Third-Party Equipment. Third-Party Equipment shall be subject to any warranties provided by the Third-Party Equipment manufacturer. Contractor will assign to Authority all Third Party Equipment warranties provided by the Third Party Equipment manufacturer. Contractor will pass through to Authority and make commercially reasonable efforts to enforce on Authority's behalf, any warranties and remedies available from the Third Party Equipment manufacturer.

11. Survival.

The sections of this Addendum that require performance subsequent to termination shall survive termination or expiration of the Agreement or any Order Document or Statement of Work, including, without limitation, any and all warranties.

ATTACHMENT D to the Order Document

Managed Software-as-a-Service Addendum

- 1. Relationship to General Terms and Conditions.** This Software-as-a-Service Addendum (this “Addendum”) is governed by the General Terms and Conditions of the Agreement and applicable Order Documents and Attachments related thereto.
- 2. Entire Addendum.** This Addendum consists of these General SaaS Terms and Conditions, which generally apply to all Service Offerings, and any attached Special Terms and Conditions, which apply to specific Service Offerings. Unless otherwise provided, references to this Addendum shall be deemed to encompass these General SaaS Terms and Conditions and any attached Special Terms and Conditions.
- 3. Order of Precedence.** In the event of any inconsistencies, ambiguities or conflicts between these General SaaS Terms and Conditions and the Special Terms and Conditions, the Special Terms and Conditions shall prevail, but only with respect to the applicable Service Offering.
- 4. Additional Definitions.** The following defined terms are in addition to those defined in the General Terms and Conditions of this Agreement:

Annual Adjustment means Itron’s annual price increase as set forth in the Order Document above.

Endpoint means an electric meter or water endpoint receiver-transmitter, battery-powered device, or any other device that Itron has agreed to monitor as part of a Service Offering which Endpoints are identified in the Order Document or Pricing Summary.

General SaaS Terms and Conditions means the terms and conditions set forth in the main body of this Addendum comprised of Sections 1 (“Relationship to General Terms and Conditions”) through 20 (“Roles and Responsibilities”).

Hybrid SaaS means Customer has purchased a Service Offering for Software in addition to an object code license to Software pursuant to the terms of the Software Addendum.

Maintenance Services means services provided under the Maintenance and Support Services Addendum attached to the Agreement as may have been amended.

Minimum Subscription Term means the minimum number of SaaS Billing Cycles during which Customer is required to subscribe for each Service Offering, which shall be four (4) SaaS Billing Cycles following the applicable Service Offering Commencement Date, unless otherwise stated in the applicable Order Document or Pricing Summary.

One-Time Setup Fee means the one-time setup fee for each Service Offering identified in the applicable Order Document or Pricing Summary.

Recovery Point Objective or RPO means the maximum tolerable time period which data might be lost from production Software due to a service interruption event.

Recovery Time Objective or RTO means the duration of time allowing for the execution of all failover processes required to return access, connectivity, functionality, and operation of production Software to Customer following declaration of a disaster event.

SaaS means software-as-a-service whereby Itron or its designated provider hosts and provides Customer with access to Software on Servers via the internet.

SaaS Billing Cycle means a period of one year beginning on the Service Offering Commencement Date for the initial Service Offering or any anniversary thereof.

SaaS Application Availability means the total number of minutes in a calendar month that the applicable Software is available and accessible by Customer via a Customer and Itron managed VPN tunnel, and that enables the Customer to perform its daily operational functions via (a) a web browser client, (b) web services interface and (c) thin client. Scheduled downtime and planned maintenance are excluded from this calculation. A determination of availability will be based on 24x7 accessibility, less any exclusions set forth in this Addendum.

Servers means the physical computer hardware owned by Itron or its designated provider on which Software will be installed, operated, and maintained.

Service Offering means SaaS, including Hybrid SaaS, plus any services that are additional or supplemental to SaaS, as described in the applicable Special Terms and Conditions.

Service Offering Commencement Date means, with respect to each Service Offering, the earlier of (a) validation of such Service Offering implementation by Itron pursuant to the applicable Statement of Work, or (b) seven (7) days after completing application system setup and the Customer is able to access such Service Offering, provided Customer shall test such access and notify Itron of any issues within seven (7) days from Itron providing valid access credentials.

Software means each machine readable (object code) versions of computer program identified on the applicable Order Document or Pricing Summary for which Customer has purchased a Service Offering.

Special Terms and Conditions means Service Offering-specific terms and conditions set forth on Attachment A to this Addendum.

Subscription Fees means annual fees identified in the applicable Order Document or Pricing Summary for each Service Offering, plus the Annual Adjustment, if any. Where Customer has purchased Hybrid SaaS, license fees and fees for applicable Maintenance Services are not included within the Subscription Fees and must be paid separately. Where Customer is not purchasing Hybrid SaaS, fees for applicable Maintenance Services are included within the Subscription Fees.

Subscription Term means the subscription term purchased by Customer for each Service Offering, which begins upon the applicable Service Offering Commencement Date.

UIQ Suite means UtilityIQ Suite headend software. Specifically for the Project, UtilityIQ Suite includes the following Software applications: Advanced Metering Manager (AMM), Meter Program Configurator (MPC), MultiSpeak adaptor, DLI service (file retrieval), and Control Platform (includes Firmware Upgrader (FWU) and Network Center). If Customer elects to purchase Outage Detection System (ODS), ODS will be included in the UIQ Suite.

5. Access Rights and Restrictions.

5.1. Access Rights. SaaS is only available for Itron Software identified in the table set forth in this Section 5.1 below for which Customer has purchased a Service Offering and paid all applicable fees. Subject to Customer's compliance with the Agreement (including payment of all applicable fees which, in the case of Hybrid SaaS (as defined in Subscription Fees definition above), shall include Software licensing fees and Maintenance Services support fees), Itron hereby grants to Customer, for the Subscription Term(s) purchased, a non-exclusive, non-transferable (except as provided for in the Agreement), non-assignable, limited right to access and use the Service Offerings, with respect to Endpoints owned or otherwise controlled by Customer, for its internal business purposes in the Territory (as defined in the General Terms and Conditions of the Agreement).

Itron Software Eligible to Receive SaaS

- UIQ Suite
- Distributed Intelligence (DI)
- Operations Optimizer (OO)

5.2. **Restrictions on Use.** Customer and its authorized users may not: (a) modify, translate or create derivative works of any Service Offering or related Documentation; (b) copy, reproduce, distribute, republish, download, display, post or transmit any portion of a Service Offering or related Documentation in any form or by any means, except Customer may copy Documentation as necessary for internal business purposes only; (c) sell, assign, transfer, lease or sublicense any Service Offering; (d) allow any third party, other than authorized users, to access any Service Offering or related Documentation without Itron's prior written consent; (e) use any Service Offering or related Documentation to provide services to third parties, or otherwise use any Service Offering on a "service bureau" or "timesharing" or subscription basis including, in connection with devices or equipment not owned or otherwise controlled by Customer; (f) reverse engineer, disassemble, decrypt, extract or otherwise reduce any Service Offering to a human perceivable form or otherwise attempt to determine the source code or algorithms of any Service Offering (except to the extent the foregoing restriction is expressly prohibited by applicable law); (g) infringe any of Itron's or its providers' Intellectual Property Rights; (h) publicly publish the results of any benchmark tests run on any Service Offering without Itron's written consent; (i) use any Service Offering or related Documentation to engage in any fraudulent, illegal or unauthorized act; (j) knowingly introduce into or transmit through any Service Offering any material containing software viruses, worms, trap doors, back doors, Trojan horses or other harmful or malicious computer code, files, scripts, agents or programs; (k) remove, alter or obscure any titles, product logo or brand name, trademarks, copyright notices, proprietary notices or other indications of Itron's or its providers' Intellectual Property Rights, whether such notice or indications are affixed on, contained in or otherwise connected to a Service Offering; (l) attempt to gain unauthorized access to a Service Offering or Itron's or its providers' systems or networks; (m) merge any Service Offering with any other product or service, except as authorized by this Order Document, without Itron's prior written consent and the payment of any additional fees; or (n) access or use any Service Offering or related Documentation to build or support, and/or assist a third-party in building or supporting, products or services competitive to Itron or its providers.

5.3. **Content Restrictions.** Customer may not distribute, download, or place on any Itron or its providers' website or Server, or use with any Service Offering, any content that: (a) Customer knows infringes the Intellectual Property Rights of any third party or violates any rights of publicity or privacy; (b) violates any applicable law, statute, ordinance; (c) is defamatory, trade libelous, unlawfully threatening or unlawfully harassing; or (d) is obscene, pornographic or indecent (items (a) – (d) are collectively referred to as "**Prohibited Content**"). Itron reserves the right to remove any Prohibited Content from the Server without prior notice to Customer. Customer will indemnify, defend and hold Itron and its providers harmless for any claims, liabilities, losses, causes of action, damages, settlements, and costs and expenses (including, without limitation attorneys' fees and costs) arising from any third-party claims related to or generated by any Prohibited Content distributed, downloaded, or placed on any Itron or its providers' website or Server or used with any Service Offering by Customer.

5.4. **Breach of Restrictions.** Customer's breach of the restrictions set forth in Section 5.2 ("Restrictions on Use") or Section 5.3 ("Content Restrictions") shall constitute a material breach of the Agreement and may result in revocation and suspension or termination of all rights and licenses

granted under this Addendum with respect to the Service Offerings; provided Itron provides advance written notice to Customer and an opportunity to cure of no less than thirty (30) business days. Revocation does not preclude Itron from pursuing any legal and equitable remedies for Customer's breach of these restrictions.

5.5. **Software License Option.** Anytime during the Subscription Term, Customer shall have the right, at its discretion and with notice to Itron, to transition to a term license for on premise or third-party hosted implementation of UIQ Suite, for the remainder of the SaaS Subscription Term, provided that Customer will continue to pay the same fees under the Order Document, which will then be applied to maintenance and support (for the software that has been moved to an on-premise or third party hosted solution) rather than SaaS Subscription Fees, for the same duration of the SaaS Subscription Term.

6. **Invoicing and Payment.** Customer shall pay Subscription Fees in advance for each SaaS Billing Cycle for which it has purchased a Service Offering. Itron will invoice Customer for the One-Time Setup Fee and initial Subscription Fees for each Service Offering upon the Service Offering Commencement Date. Initial Subscription Fees shall be prorated based on the number of months remaining in the current SaaS Billing Cycle following the Service Offering Commencement Date. Itron may not discontinue a Service Offering during the Minimum Subscription Term as long as Customer is current on payment of Subscription Fees. If Customer discontinues a Service Offering prior to expiration of the Minimum Subscription Term for that Service Offering, Itron will invoice Customer, and Customer will pay, for any unpaid Subscription Fees for the respective Service Offering through the end of the applicable Minimum Subscription Term. Maintenance Services fees and license fees relating to Hybrid SaaS are not included in this Addendum or the Subscription Fees and will be invoiced in accordance with the Maintenance and Support Services Addendum and Software Addendum, as applicable.

7. Monthly Application Availability Service Level.

7.1. **Service Level.** Provided Customer has paid all applicable fees (including all Subscription Fees and, in the case of Hybrid SaaS, all maintenance and license fees) SaaS Application Availability with respect to each production environment Service Offering will be at least 99.9%, measured and reported monthly beginning in the first full calendar month following the respective Service Offering Commencement Date ("Monthly SaaS Application Availability Service Level"). The Monthly SaaS Application Availability Service Level will be measured and calculated separately for each Service Offering. Itron records and data, including Customer generated incident/problem tickets and outage reports, will be the sole basis for all SaaS Application Availability Service Level measurements and calculations. In the event Itron becomes aware of any significant issues related to availability or functionality with Itron's Service Offerings, Itron shall notify the Customer's designated point of contact in accordance with Itron's Incident Management Program.

7.2. **Service Level Credits.** As Customer's sole and exclusive remedy for Itron's failure to meet the foregoing Monthly SaaS Application Availability Service Level, subject to the service level exclusions in Section 8.1 (Service Level Exclusions) below, Customer will be entitled to credits as follows:

SaaS Application Availability (production environments only)	
Monthly SaaS Application Availability performance	Credit (% of monthly Subscription Fee for applicable SaaS Application)
≥99.5% and <99.9%	2%
≥98.5% and <99.5%	4%
≥96.0% and <98.5%	10%

≥94.5% and <96.0%	12.5%
<94.5%	20%

- 7.3. **SaaS Application Availability Service Level Reporting.** Itron will measure and report out to the Customer the Service Levels on a monthly basis, each calendar month, starting with the Service Level Triggers defined below. That report will list UIQ performance against the Application Availability SLA in the prior month and any Service Level credits that may apply. Following each such report, Itron and Customer will discuss such. The Service Level credits due will be applied against Itron's charges for the second month following the month in which the credits were incurred, except at the end of a final SaaS term in which case credits may be applied first to other fees under the Order Document or if that is not possible, then to any other Customer purchase from Itron. Service Level reports will be available to Customer within thirty (30) days after the last day of the prior month.
- 7.4. **Chronic SLA Failure.** The above-referenced credits are Customer's sole and exclusive remedy for Itron's failure to meet the Monthly SaaS Application Availability Service Level; provided, however, that if the Monthly SaaS Availability Service Level is less than ninety percent (90%) for three (3) consecutive months at any time during the term of this Order Document (a "**Chronic SLA Failure**"), Itron shall provide Customer with a remediation action plan and schedule for such remediation upon Customer's request. Additionally, Customer may terminate this Order Document at its sole discretion for cause in accordance with Section 11.1 (Termination for Cause) of the Agreement based on such Chronic SLA Failure.

8. Service Level Exclusions; Disclaimers.

- 8.1. **Service Level Exclusions.** Itron shall not be liable for failing to meet any service level commitment set forth in this Addendum (including any Special Terms and Conditions) or any Order Document to the extent such failure is attributable to any one or more of the following: (a) planned maintenance, or scheduled upgrades; (b) an event triggering a disaster recovery pursuant to Section 19 ("Disaster Recovery") and for a twenty-four (24) hour period after the resumption of service following such an event to allow the system to return to normal operating ranges; (c) suspension or restriction of service under Section 11 ("Suspension or Restriction of Service") of this Addendum; and (d) conditions beyond Itron's reasonable control, including but not limited to: (i) failure of any backhaul between the Service Offering and the Endpoints not managed by Itron directly; (iii) failures in external Internet or VPN configurations not managed by Itron; (iv) a Force Majeure event; (v) false reports of unavailability as a result of outages or errors of any Itron measurement system; (vi) an act or omission of Customer or third parties (other than Itron's contractors, subcontractors or suppliers) not in compliance with Customer's rights or obligations, including security incidents caused by such act or omission; (vii) incident investigation or computer failures that could not reasonably have been prevented by Itron; (viii) failures of equipment, hardware, software, or services not provided by Itron or its subcontractors or otherwise authorized by Itron; and (ix) Customer's material delay in performing tasks designated as its responsibility in this Agreement.
- 8.2. **Disclaimers.**
- 8.2.1. **Third-Party Content.** Itron is not the owner of third-party Software or third-party Service Offerings that Customer purchases through Itron (collectively "Third-Party Content") and makes no representations or warranties whatsoever, directly or indirectly, express or implied, as to the suitability, durability, and fitness for use, merchantability, condition, quality, performance or non-infringement of any Third-Party Content. Third-Party Content shall be subject solely to any service levels or warranties provided by the third-party provider. Itron will pass through to Customer and make commercially reasonable efforts to enforce on

Customer's behalf, any service levels, warranties and remedies received from such third-party provider.

- 8.2.2. Use of SaaS with Third-Party Devices.** Customer may use a Service Offering to collect data from Endpoints equipped with radio communication devices not manufactured or provided by Itron ("Third-Party Radio Device"). Itron makes no representations or warranties whatsoever, directly or indirectly, express or implied, as to the suitability, durability, and fitness for use, merchantability, condition, quality, performance or non-infringement of, and disclaims all liability with respect to, Third-Party Radio Devices. For any Third-Party Radio Devices identified by Itron as compatible with Service Offerings, Itron may provide reasonable support to address functional communication with such Service Offerings, if mutually agreed in writing. Itron shall have no liability (a) if a Third-Party Radio Device is not responding or communicating or (b) for unread endpoints due to defective or unreachable attachment Radio Devices. Customer shall contact the supplier of such device for support.
- 9. Sizing of Software-as-a-Service.** Itron will size Service Offerings, Servers, and systems for Customer's specific deployment. System sizing depends upon the Service Offering and types of devices and sensors and may be a factor in determining Subscription Fees. Sizing criteria may include number of system endpoints, number of network devices, residential meter configuration, commercial and industrial meter configuration, desired data collection intervals, storage duration for historical data, and the number of concurrent and total users of the application. Any material sizing changes above and beyond ten (10) percent of the applicable criteria during a Subscription Term will require a Change Order and may result in a change in Subscription Fees.
- 10. Conditions on Use of Service.** Customer will use the Service Offerings only in accordance with Itron user guides, the Agreement (including, this Addendum, the General Terms and Conditions, applicable Order Documents), and laws and government regulations. Except with respect to the QA environment, the rights of any user to access and use the Service Offerings cannot be shared or used by more than one individual (unless such license is reassigned in its entirety to another authorized user), provided Itron is not responsible for any issues related to such shared access by Customer, and Customer shall make every reasonable effort to prevent unauthorized third parties from accessing the Service Offerings.
- 11. Suspension or Restriction of Service.** Itron may suspend or restrict all or part of the Service Offerings at any time to protect the integrity and functionality of the Software, Servers, platforms, and systems ("System Integrity Impacts"), or for a material breach of Section 5.2 ("Restrictions on Use"), Section 5.3 ("Content Restrictions") or Section 10 ("Conditions on Use of Service") ("Breach Impacts") (collectively "System Impacts"), until such System Impacts are resolved. Itron will provide as much notice as is practical under the circumstances before suspension due to System Integrity Impacts. For suspension due to Breach Impacts, Itron will provide ten (10) business days' advance written notice to Customer and an opportunity to cure.
- 12. Incident Management.** Itron will provide Customer support and incident and problem management services, which include responding to alerts, tracking the issue, troubleshooting the problem and escalating to Itron subject matter experts or third-party providers, in accordance with the Maintenance and Support Services Addendum.
- 13. Customer Technical Responsibilities.** Customer is responsible for selecting, acquiring, securing and maintaining all equipment and ancillary services needed to connect to, access, or otherwise use and maintain compatibility with the Service Offerings, at Customer's sole expense.
- 14. User IDs and Passwords.** Itron shall provide Customer with user identifications and passwords ("User IDs") to access the Service Offerings. Customer shall be solely responsible for all use of Customer's subscriptions and accounts. Customer shall maintain the confidentiality of all User IDs assigned to

Customer. Except with respect to the QA environment, User IDs may not be shared or used by more than one user.

15. Planned Maintenance. Planned maintenance, whenever reasonably practicable, will be performed during off-business hours between 6:00 p.m. to 12:00 a.m. Customer's local time, with as little disruption to Customer's use of the Service Offerings as possible. All planned maintenance will go through Itron change control which requires a project plan, back-out plan, customer approval, and mutually agreeable date and time of the maintenance window, subject to change in the event of storm or other electric emergencies. Should the Planned Maintenance window exceed the mutually agreed upon maintenance duration and the system is unavailable for normal operations, Itron will open a Severity 1 ticket and will continue to troubleshoot the issue until remediated. Unplanned maintenance, whenever reasonably practicable, shall also be performed during off-business hours between 6:00 p.m. and 12:00 a.m., Customer's local time.

16. Unplanned Maintenance. Itron will provide Customer with notice of unplanned maintenance as soon as reasonably practical and a minimum of twenty-four (24) hours written notice unless fixing a Level 1 problem. Itron will use commercially reasonable efforts to minimize Service Offering disruptions.

17. Business Continuity.

17.1. Itron has architected and operates a high availability and scalable infrastructure to facilitate virtualized customer environments with various fault tolerant components. Fault tolerance and failover methodologies allow Itron to maximize system availability and confidently uphold the committed Services Levels. Itron will conduct daily backups of back office application configuration files and associated data. These backups are for operational purposes only and are not a disaster recovery solution or a solution to be used by the Customer for testing or analysis purposes. Itron will periodically (at least annually) test the restore capability of its business continuity solution and will provide a summary of the latest test results upon request by Customer. System and database backups are performed via a schedule to provide for a full weekly backup and daily differential backups. System backups and snapshots are also taken prior to any system change that has been approved via the Itron Global Managed Services Change Control Board. The system can be recovered from the backup in an event of a failure. Business continuity is designed to provide recovery for component failures within a datacenter, this does not provide coverage for the loss or connectivity to a data center.

17.2. All incidents requiring system recovery will be required to adhere to Itron's incident management policy and related standard operating procedures. BUSINESS CONTINUITY: RPO = 72 hours; RTO = 5 business days.

18. Transition Support Services.

Upon termination or expiration of this Addendum, at Customer's request and expense, and subject to mutual written agreement by the Parties, Itron will provide services to support the transition of any applicable Managed Services (as defined below) to a Customer-supported on-premise model or a replacement service provider of Customer ("**Transition Services**"). Transition Services may include, but are not limited to, network and data migration, handoff of required security credentials (keys, certs), and any necessary application configuration changes. In order to allow Customer to better understand the cost and scope of such Transition Services, the Parties agree to schedule and jointly develop a potential transition plan within twelve (12) months of the Order Document Effective Date, under which the hosting, management, and monitoring functions of the Service Offerings could be transitioned to a Customer-supported on-premise model or a replacement service provider of Customer. Any Transition Services provided by Itron shall be mutually agreed upon by the Parties and described in a separate agreement or statement of work, which shall describe the duration, scope, and additional fees and costs associated with such Transition Services.

Disaster Recovery. Disaster Recovery (“DR”) is an optional fee-based service that is offered by Itron for some product offerings. If purchased, Itron will provide DR in accordance with Exhibit D-3.

- 19. Roles and Responsibilities.** This Addendum and the Statement of Work list the respective responsibilities of Customer and Itron to implement the Service Offerings. Exhibit D-1 of this Addendum lists all the respective responsibilities of Customer and Itron to ensure reliable operation of the SaaS Service Offering.
- 20. Return of Customer Data.** Upon written request by Customer made within six (6) months after any expiration or termination of this Addendum, Itron shall at Customer’s direction promptly return or destroy and erase from all of Itron’s systems any Customer Data in its possession, custody or control, provided however, Itron may retain copies as part of archival records (including backup systems) that Itron keeps in the ordinary course of business.

ATTACHMENT D
EXHIBIT D-1

Roles and Responsibilities

Description (Note R=Responsible, A=Accountable, P=Participates, I Informed)	Itron	Customer
Back office network administration		
Maintain customer data center network and customer corporate network connections to support AMI application environments	R	
Maintain WAN backhaul network connections (APs and Socket APs to AMI system), monitoring and troubleshooting (including escalating to relevant provider (public WAN provider, utility, and so on)	R	
Maintain utility LAN-to-AMI system connectivity, including monitoring and troubleshooting (front haul)	R	
Maintain monitors to enable the NOC to respond to alerts and escalate internally and externally, as necessary	R	
Maintain B2B network connections (VPN/DSL) and associated security and access control measures to enable Remote Management	R	
Maintain back office network configuration Management	R	
Provide network connections (AP and Relays) capacity planning to support MPLS, IPSEC, VPN space planning	R	
Provide capacity planning procurement.	R	
Management of interfaces, integrations across Itron Systems (i.e. IEE, UIQ)	R	
Management of API's / creation of export files for integration out to other utility systems (MultiSpeak, CMEP, etc.)	R	
Management of API's / receiving Itron data files into other utility systems (MultiSpeak, CMEP, etc.)		R
Server administration/operating system (OS)		
Troubleshoot OS problems	R	
Manage file systems (i.e. snapshots, backups, data management)	R	
Maintain monitors to enable the NOC to respond to alerts and escalate internally and externally, as necessary	R	
Apply OS patches and updates, and test (Per Itron Engineering specifications to ensure compatibility. Itron to maintain OS and database versions to ensure support eligibility. Monthly patching with hotfixes and updates implemented as applicable through change control)	R	
Apply security related patches and test (Itron may deploy as an emergency change control and notify Customer after the fact)	R	
Create user (shell) accounts, as required	R	
Maintain all current software licensing requirements for applicable third-party software (Oracle, Red Hat Enterprise Linux, and so on)	R	
Maintain current hardware maintenance agreements for all equipment and servers in customer data center(s)	R	

Provide remote for activities requiring physical presence (power cycle hardware, escort vendors, and so on)	R	
Maintain server and OS configuration management	R	
Provide server capacity planning (specifically related to organic growth as defined in this addendum)	R	P
Provide capacity planning procurement (specifically related to organic growth as defined in this addendum)	R	
Storage administration - Performed by Systems Engineer		
Maintain external storage systems (SAN hardware and software), including updates, patches, and fixes (Monthly patching, hotfixes, and updates implemented as applicable through change control)	R	
Maintain current maintenance agreements for SAN hardware and software	R	
Implement and maintain storage file system for AMI applications, according to Itron performance specifications	R	
Maintain monitors to enable the NOC to respond to alerts and escalate internally and externally, as necessary	R	
Maintain SAN configuration management	R	
Provide storage capacity planning (specifically related to organic growth)	R	P
Provide capacity planning procurement (specifically related to organic growth)	R	
Database administration		
Maintain monitors to enable the NOC to respond to alerts and escalate internally and externally, as necessary	R	
Manage database table space usage and next extent sizes	R	
Perform database reorganizations	R	
Backup database redo (archive) logs	R	
Resolve database problems	R	
Apply database updates and patches, and test	R	
Perform regular (typically weekly) database purge/archive tasks (“retention”)	R	
Maintain current all software licensing requirements for applicable third-party software (Oracle)	R	
Maintain database configuration management	R	
Provide database capacity planning	R	
Provide capacity planning procurement	R	
Backups		
Provide backup infrastructure (hardware/software)	R	
Perform regular backups	R	
Manage off-site backups (backup retention for 14 days)	R	
Monitor backup jobs	R	
Restore from backup media, as necessary	R	
Periodically validate/test backup restore procedure	R	
Maintain backup configuration management	R	
Application administration		
Install and configure application updates, patches, and fixes	R	
Maintain application tuning (configuration management)	R	

Maintain monitors to enable the NOC to respond to alerts and escalate internally and externally, as necessary	R	
Monitor and respond to alerts, and escalate internally and externally, as necessary	R	
Support Customer's testing of new AMI application releases and patching in lower environments (such as QA or Staging), and approve updates to upper environments (Production and Rapid Recovery), if applicable	R	A
Application Configuration during implementation and post implementation	R	A
Application Config, (i.e. Meter Config Profiles, Billing Windows (operational business related configurations)) in sustainment	A	R
Register and System type of Configuration Settings (in backend of UIQ)/ System caches / Oracle caches	R	
Change Control Activities within Itron are approved by Itron CAB and require Utility CAB participation and approval (Including but not limited to patching, upgrades, hotfixes, infrastructure changes, etc.) Itron Change Control submissions include a project plan, rollback plan, maintenance date and time, and customer approval.	R	A
AMI application administrative tasks		
Perform adds/deletes/change to AMI system user accounts (user administration via UIQ CAAS module)		R
Schedule/Run AMI application batch jobs	R	
Monitor critical-identified read and export batch jobs	R	
Coordinate batch jobs and backups	R	
Security		
Provide physical and logical security of equipment	R	P
Provide physical and logical security of data	R	
Itron Fronthaul and Backhaul Connectivity Responsibility (VPN, MPLS, Direct Connect Circuit (maintain Itron side of the VPN tunnel or circuit providing the fronthaul and backhaul connectivity)	R	
Customer Fronthaul and Backhaul Connectivity Responsibility (VPN, MPLS, Direct Connect Circuit (maintain Customer side of the VPN tunnel or circuit providing the fronthaul and backhaul connectivity)	R	R
Create and maintain security policies to equipment and data	R	I
Maintain security of configuration management	R	
Monitor and assess security strategies	R	
Respond to and remediate security incidents as applicable. Notify Customer per Itron Incident Management Program severity level	R	I
Support and participate in system security reviews and audits (application stack that runs to audit - Qualys)	R	
Conduct security penetration test of all critical Itron components (Application level testing)	R	P
Support and participate in penetration tests initiated and commercially responsible by Customer or a third-party engaged by Customer	P	R
Operations policies and procedures		
Maintain Help Desk, Tier 1 (AMI application operational issues raised by end user within customer)	R	P

Maintain Application Support Desk, Tier 2 (technical support to customer's support coordinators)	R	P
Provide onsite coordination and tracking of Customer Support issues (remediating field devices by Customer)	R	A
Allow direct escalation to Tier 3 (TAC and NOC) support personnel	R	
Modify Management policies and procedures	R	
Modify Management policies and procedures specific to Customer	R	A
Update Incident Management policies and procedures	R	A
Monitor logs for non-security events	R	
Monitor logs for security events and assess, remediate, document, and notify Customer as applicable	R	
Report on SLA and other performance measurements (provide SLA and performance measurement calculations when requested by Customer)	R	I
Review monthly performance and agree on Service Level credits	R	P
Provide Reports on Open Tickets, Status, Resolutions, etc. (Utilities can access Remedy to pull reports or autogenerate)	R	P
Perform and Deliver Root Cause Analysis Reports as required (Note for hosting only on P1 and w/in 5 bus days is standard - this would be a negotiation item as part of SaaS contracting)	R	P
Meter deployment management		
Provide meter installation (Update: The team responsible for installing the meters)	R	
Provide regular status updates on meter deployment progress and plans	R	
Provide properly formatted device files (MMF) for all meters	R	
Manage import of device files (MMF) for all meters into AMM	R	
Provide properly formatted location files for all meter installations, including GPS coordinates to SFTP	P	R
Retrieve location files from SFTP for all meters for import into AMM	R	
Provide monitoring and troubleshooting of meters remaining in Discovered or Removed states within AMM	R	I
Participate in as-needed planning, analysis, and status meetings (additional work post-contract to be handled through subsequent SOWs)	R	P
Provide monitoring and troubleshooting of meters remaining in installed, Initializing, InitFailed or Unreachable states within AMM. Initial investigations are the responsibility of Itron (see Network Operations below).	R	
Provide field investigation of meters as requested by Itron.	P	R
Provide configuration management of NICs (reconfigure meter NICs to match meter program information of type, if applicable)	R	
Apply firmware updates (and support testing) to meters as they come online, if applicable.	R	

Apply firmware updates (and support testing) to meters as new firmware versions are released	R	
Mesh network operations		
Provision and install APs, Socket APs and Relays (after Deployment Period and Optimization; relevant for organic growth of meter locations or device replacement)	P	R
Provision and install APs, Socket APs and Relays during the Deployment Period (Itron to upload location information into AMM for newly installed APs, Socket APs and Relays during the Deployment Period)	R	I
Provide properly formatted device files for all APs, Socket APs and Relays	R	
Provide properly formatted location files for all meter installations, including GPS coordinates (for all such devices moved or added after the Deployment Period or Optimization)	P	R
Manage import of device and location files for all APs, Socket APs and Relays into AMI system (for all such devices moved or added after the Deployment Period and Optimization).	R	
Validate APs and Socket APs after installation (after the Deployment Period and Optimization, relevant for organic growth of meter locations or device replacement)	P	R
Validate APs and Socket APs during the Deployment Period	R	
Participate in regularly scheduled operations status and customer support meetings (during the Deployment Period)	P	R
Participate in regularly scheduled operations and customer support meetings (monthly or during the quarterly business review (QBR))	R	P
Manage procurement/billing of WAN carrier (cellular operators)	R	
Apply firmware updates (and support testing), if applicable, to all deployed devices, including WAN modems	R	
Perform regular “network sweeps” to update firmware and configure newly deployed devices covered in the scope of the agreement	R	
Monitor reachability of APs, Socket APs and Relays (ADD Notification to utility if AP is down)	R	
Troubleshoot reachability of APs, Socket APs and Relays	R	
Perform network operation statistics gathering, analysis, trending, and reporting	R	
Provide field investigation of meters, APs, Socket APs and Relays (as requested and post Itron’s initial remote troubleshooting of devices) to help determine root cause of meter deployment issues	R	I
Provide meter hardware replacement and maintenance after Deployment period		R
Provide AP and Relay hardware replacement and maintenance after Deployment period		R
Provide AP and Relay configuration management	R	
Provide AP and Relay capacity planning (specific to territory expansion beyond what was contractually defined)	R	A
Provide AP and Relay procurement		R
Initiate remote disconnects/reconnects		R

Perform export verification through deployed Itron monitors	R	
Perform meter read verification through deployed Itron monitors	R	
Conduct performance reporting auditing	R	P
Perform SLA tracking (SLA and performance measurement calculation provided at Customer's request)	R	I
Perform regulatory requirement tracking		R
Perform remote meter program changes	R	A
Perform new meter program configuration and approval		R
Perform firmware upgrades and auditing	R	
Perform data maintenance within the application, incorporating both meter and installation (location) information (meter change / location issue)	R	I
Perform device swaps within the application	R	I
Coordinate field visits for faulty/suspect devices as requested by Itron	P	R
Apply changes to interrogation schedules	R	A
Monitor and Report on Success of interrogation schedules	R	
Identify Meters Not Communicating and perform back office analysis and troubleshooting	R	
Disaster recovery		
Participate in annual rapid recovery walk-through exercise and test failover drills	R	P
Maintain and update rapid recovery plan in accordance with changes to the environment (Update annually)	R	P
Test customer data connections and backup communications with Itron	P	R
Maintain network connectivity between data center(s) (primary and secondary) to meet the design requirements (RPO)	R	
Provide adequate notice of rapid recovery walk-through schedule (annual Disaster Recovery failover exercise schedule)	P	R
Maintain and provide an overall customer rapid recovery plan, encompassing AMI application dependencies (including acceptance criteria) (Itron to provide Disaster Recovery method of procedure (MOP) for Customer to include in their rapid recovery plan)	P	R
Coordinate with Customer regarding returning from failed over status back to primary data center	R	P

ATTACHMENT D
EXHIBIT D-2

Managed Services Special Terms And Conditions

Special Terms and Conditions – Managed Services. The Special Terms and Conditions contained within this Section apply to Itron’s Managed Services Service Offering.

1. Managed Services – Descriptive Overview.

- 1.1.** When Customer subscribes to Managed Services, as part of the overall Service Offering Itron will provide SaaS for the applicable Software, plus Itron will also assume some of Customer’s SaaS-related operational responsibilities, including management of reads from monitored and available Endpoints or Provisioned and Optimized Endpoints (as applicable), collecting data, and delivering data files or messages to Customer at agreed-upon intervals in agreed upon data formats. Itron will attempt to remotely diagnose and resolve Endpoint exceptions, including events and alarms, detected by Itron or reported by Customer. If the exception cannot be resolved remotely, Itron will notify Customer that Customer must perform in-field investigation and replacement.
- 1.2.** Managed Services are only available for Itron Software identified in the table set forth in this Section 1.2 below for which Customer has purchased such Managed Services and paid all applicable fees.

Itron Software Eligible to Receive Managed Services
UIQ Suite

- 1.3. Managed Services – Definitions.** The following defined terms are applicable to these Special Terms and Conditions for Managed Services:

Anchor Read means the “register value” stored once daily in a register in the Communication Module as installed in the Endpoint (usually at midnight).

Communications Module or **NIC** means Itron’s network interface card that may be installed in Equipment.

Endpoint has the meaning set forth in the General SaaS Terms and Conditions.

Equipment has the meaning set forth in the Equipment Addendum.

Managed Services means SaaS, plus the additional services to be provided by Itron as set forth in these Special Terms and Conditions for Managed Services.

Optimization is a UIQ term which means the procedure by which the layout of the network, Equipment configuration and implementation have been validated (“Optimized”) by performing active and passive tests to confirm that performance and redundancy meet the design specifications and other requirements of the Agreement. Optimization is to be executed on an area-by-area basis (or specified portion thereof), after a minimum of 99.5% of the Endpoints have been deployed to achieve the required level of saturation of the area. Itron will complete Optimization every six (6) months, if necessitated by the addition of new Endpoints, while Managed Services are active.

Provisioned means an Endpoint that is located in an area of the NAN and which is in any of the following operational states within the UIQ System: "active," "inactive," or "disconnected," but which is not: (i) in a “new,” "discovered," "installed," "initializing," "unreachable" or "init failed"

state; or (ii) considered to be in the process of being deployed or being repaired under warranty. Endpoint operational states are defined in the Meter Lifecycle Reference document. Typically, UIQ is configured so a meter is set to “unreachable” if it’s not read within 72 hours.

Service Level Trigger means satisfaction of the particular condition(s) noted in these Special Terms and Conditions.

- 2. Roles and Responsibilities.** This Addendum and the Statement of Work list the respective responsibilities of Customer and Itron to implement the Service Offerings. Exhibit D-1 of this Addendum lists all the respective responsibilities of Customer and Itron to ensure reliable operation of the SaaS Service Offering.

2.1. SaaS and Managed Services Installation and Setup. Subject to Section 2 (Roles and Responsibilities) above, the Statement of Work and Exhibit D-1, and payment of applicable fees, Itron will:

- (a) provide, at its expense, the facilities, operating infrastructure, Itron Intellectual Property, Personnel, equipment, software, training and other resources necessary to provide the Service Offerings (collectively called the “**Resources**”),
 - 1. to the extent necessary or appropriate to provide the Service Offerings: (i) maintain licenses for all third party software installed on the Servers and used in the provision of the Service Offerings; (ii) obtain maintenance and support for, update, upgrade, enhance and implement security and operating system fixes and new versions of third party software installed on the Servers and used in the provision of the Service Offerings; and (iii) maintain all other licenses, registrations, authorizations and filings necessary for it to perform its responsibilities in connection with the Service Offerings including paying all fees and taxes associated with such licenses, registrations, authorizations and permits,
 - 2. provide sufficient project management resources in connection with the provision of the Service Offerings,
 - 3. physically and logically isolate all Customer data and operate each Service Offering environments as a separate instance from those of its other clients at all times,
 - 4. comply with such applicable legal and regulatory requirements as relate to the Service Offerings,
 - 5. control and maintain the security of all identification codes and passwords in relation to the Service Offerings and access by any Itron Personnel and promptly report to Customer any errors or irregularities in the Service Offerings or any unauthorized use of any part thereof of which it is aware, and
 - 6. establish the necessary system or systems to enable it to prepare and provide to Customer on a regular basis the reports through which Customer may monitor the provision of the Services Offerings and the Service Levels.

- 3. Service Levels – Managed Services.** This Section 3 of the Special Terms and Conditions for Managed Services sets forth the service levels for Managed Services. Such service levels are only available for

Itron Software identified in the tables set forth below for which Customer has purchased Managed Services and paid all applicable fees.

- 3.1. Service Level Metrics.** Subject to the procedures described below, Itron will provide Service Level credits to Customer if Itron fails to meet the Service Levels specified below (“Service Levels and Service Level Credits”). If Itron fails to meet more than one Service Level in a single measurement period, Customer will be entitled only to the highest applicable Service Level credit across all metrics. No Service Level credits will apply if Customer is not current in its payment obligations under this Order Document. Credits are exclusive of any applicable taxes charged to Customer or collected by Itron. THE SERVICE LEVEL CREDITS ARE CUSTOMER’S SOLE AND EXCLUSIVE REMEDY FOR ITRON’S FAILURE TO MEET ANY SERVICE LEVEL AGREEMENT PROVIDED, HOWEVER, THAT IF ANY SERVICE LEVEL IS NOT ACHIEVED FOR THREE (3) CONSECUTIVE MONTHS, ITRON SHALL PROVIDE CUSTOMER WITH A REMEDIATION ACTION PLAN AND SCHEDULE FOR REMEDIATION.
- 3.2. Reporting.** Itron will measure and report Service Levels on a monthly basis, each calendar month, starting with the Service Level Triggers defined below. That report will list UIQ performance against all Service Levels in the prior month and any Service Level credits that may apply. The Service Level credits due will be applied against Itron’s charges for the second month following the month in which the credits were incurred, except at the end of a final SaaS term in which case credits may be applied first to other fees under the Order Document or if that is not possible, then to any other Customer purchase from Itron. Service Level reports will be available to Customer within thirty (30) days after the last day of the prior month.
- 3.3. Tracking Optimized Meters.** Itron Managed Service SLAs in this Section 3 are for meters that are Provisioned and Optimized. Optimization status is not tracked by area (e.g., Area A is Optimized) but by individual service point identifier (a unique non-changing number that identifies each meter socket where a meter will be deployed). If a meter in an Optimized Service Point ID is replaced by another meter, the new meter installed in the same Service Point is automatically considered for the SLA calculation. At the end of each Optimization, Itron will provide the list of Service Point IDs that are Optimized to Customer.
- 3.4. Pre-Optimization SLAs.** During the Deployment Period, until Meters can be Optimized (e.g., while waiting for Optimization Areas to reach 98% deployment saturation, or for remediation work recommended by Optimization to be completed), Itron will measure the pre-Optimization Read performance Service Levels as set forth in this Section 3.3 (“**Pre-Optimization SLAs**”), for meters while the meters await Optimization.
- (a) The Pre-Optimization SLAs will apply to a meter when: it (1) becomes a Provisioned Meter, and (2) has been read successfully for five (5) consecutive days.
 - (b) The Pre-Optimization SLAs will apply once there are at least 3,000 meters eligible for the SLAs to eliminate distortions caused by a small number of meters.
 - (c) Once an area is Optimized and the list of Service Point IDs is marked as Optimized, those Service Point IDs will be removed from the Pre-Optimization SLA calculation.
 - (d) Meters deployed in an Optimized area after the area has been Optimized, will be included for Pre-Optimization SLAs until the next Optimization occurs during the Deployment Period.
 - (e) After the Deployment Period, the Pre-Optimization SLAs will no longer apply, provided that Itron agrees that any meter installed in new locations after the Deployment Period will

become Optimized within six (6) months without cost to Customer, except if additional Equipment is required

3.4.1.Pre-Optimization Daily Register Read Service Level.

(a) **Service Level Trigger.** The Service Level Trigger for the Pre-Optimization Daily Register Read Service Level occurs when the applicable Meters are Provisioned.

(b) **Service Level.** For newly available data on the Endpoint, the UIQ System will gather and process Anchor Reads from Provisioned Meters and make available, via the “export” mechanism, at least ninety-six percent (96%) of Anchor Reads captured at midnight each day, by 8:00 a.m. local time the next day (“**Pre-Optimization Daily Register Read Service Level**”).

(c) **Service Level Calculation.** The following formula is used to show how this metric is calculated:

- a. For each day in the calendar month, starting on the second day of the calendar month, parse the UIQ exports to gather the anchor reads timestamped from the prior midnight and included in the exports by 8:00AM.
- b. Numerator: Aggregate the total number of anchor reads timestamped at 00:00 that were collected from the previous day from Integrated Meters marked as Provisioned and Optimized with a state in UIQ of Active, Inactive, or Disconnected and delivered to UIQ for export by 8:00AM, as confirmed by the timestamp of the meter read. As an example, for the daily performance of October 3, parse all of the UIQ exports between 00:00 on October 3 and 08:00 on October 3 and count the number of anchor reads with a timestamp of 00:00 October 3.
- c. Denominator: Total Integrated Meters marked as Provisioned with a state in UIQ of Active, Inactive, or Disconnected multiplied number of expected Anchor Reads per Day
- d. The final SLA is calculated by averaging the performance of every day of the given calendar month

(d) **Service Level Credits.** Subject to the service level exclusions set forth in [Section 8.1](#) (Service Level Exclusions) of the General SaaS Terms and Conditions, Customer will be entitled to the following credits as its sole and exclusive remedy for Itron’s failure to meet the foregoing Pre-Optimization Daily Register Read Service Level:

Pre-OptimizationDaily Register Read Service Level Credits (production environments only)	
Daily performance averaged over the calendar month	Service Level Credit (% of monthly Managed Services Subscription Fee with respect to the applicable Itron SaaS Application)
> 96%	0%
< 96% and >= 93%	5%
<93% and >= 90%	10%
<90% and >= 85%	15%
<85.0%	20%

3.4.7 Pre-Optimization Daily Interval Read Service Level.

(a) **Service Level Trigger.** The Service Level Trigger for the Pre-Optimization Daily Interval Read Service Level occurs when the applicable Meters are Provisioned.

(b) **Service Level.** For newly available data on the Endpoint, the UIQ System will gather and process Interval Reads from Provisioned Meters and deliver, via the “export” mechanism of the UIQ System, at least ninety-six percent (96%) of Interval Reads timestamped between 00:00 and 23:59:59 the prior day and collected throughout the day and make available for export by 8:00AM of the current day (“Daily Interval **Read Service Level**”).

(c) **Service Level Calculation.** The following formula is used to show how this metric is calculated:

- a. For each day in the calendar month, starting on the second day of the calendar month, parse the UIQ exports between 00:00 on the prior day to 08:00 of the current day to gather the interval reads timestamped between 00:00 and 23:59:59 from the prior day
- b. Numerator: Aggregate the total number of interval reads that were timestamped between 00:00 and 23:59:59 of the previous day from Integrated Meters marked as Provisioned and Optimized with a state in UIQ of Active, Inactive, or Disconnected and exported by 8AM the following day, as confirmed by the timestamp of the intervals. For clarity as an example, for daily performance on October 3, parse the UIQ exports between 00:00 on October 2 through 08:00 on October 3 and count all the intervals with a timestamp between 00:00 on October 2 and 23:59 on October 2.
- c. Denominator: Total Integrated Meters marked as Provisioned with a state in UIQ of Active, Inactive, or Disconnected multiplied number of expected Interval Reads per Day
- d. The final SLA is calculated by averaging the performance of every day of the given calendar month

(d) **Service Level Credits.** Subject to the service level exclusions set forth in Section 8.1 (Service Level Exclusions) of the General SaaS Terms and Conditions, Customer will be entitled to the following credits as its sole and exclusive remedy for Itron’s failure to meet the foregoing Pre-Optimization Daily Interval Read Service Level:

Pre-Optimization Daily Interval Read Service Level Credits (production environments only)	
Daily performance averaged over the calendar month	Credit (% of monthly Managed Services Subscription Fee with respect to the applicable Itron SaaS Application)
$\geq 96\%$	0%
$< 96\%$ and $\geq 93\%$	1%
$< 93\%$ and $\geq 90\%$	3%
$< 90\%$ and $\geq 85\%$	5%
$< 85.0\%$	10%

3.5. Optimized Data Service Level.

3.5.1. Service Level Applicability. The Daily Register Read Service Level, Daily Interval Read Service Level, Near Real-Time Read Service Level, and Connect and Disconnect Service Level (collectively, the “Optimized Data Service Level”) set forth in this Section 3.5 apply

to the Itron Software identified in the following table for which Customer has purchased Managed Services and paid all applicable fees:

Itron Software Eligible to Receive Data and On-Demand Read Service Level
UIQ: Advanced Metering Manager

3.5.2.Daily Register Read Service Level.

(a) **Service Level Trigger.** The Service Level Trigger for the Daily Register Read Service Level occurs when the applicable Endpoints are Provisioned and Optimized.

(b) **Service Level.** For newly available data on the Endpoint, the UIQ System will gather and process Anchor Reads from Provisioned and Optimized Endpoints and make available via the “export” mechanism, at least ninety-nine and one-half percent (99.5%) of Anchor Reads captured at midnight each day, by 8:00 a.m. local time the next day (“**Daily Register Read Service Level**”).

(c) **Service Level Calculation.** The following formula is used to show how this metric is calculated:

- For each day in the calendar month, starting on the second day of the calendar month, parse the UIQ exports to gather the anchor reads timestamped from the prior midnight and included in the exports by 8:00AM.
- Numerator: Aggregate the total number of anchor reads timestamped at 00:00 that were collected from the previous day from Integrated Meters marked as Provisioned and Optimized with a state in UIQ of Active, Inactive, or Disconnected and delivered to UIQ for export by 8AM, as confirmed by the timestamp of the meter read. As an example, for the daily performance of October 3, parse all of the UIQ exports between 00:00 on October 3 and 08:00 on October 3 and count the number of anchor reads with a timestamp of 00:00 October 3.
- Denominator: Total Meters marked as Provisioned and Optimized with a state in UIQ of Active, Inactive, or Disconnected multiplied number of expected Anchor Reads per Day.
- The final SLA is calculated by averaging the performance of every day of the given calendar month.

(d) **Service Level Credits.** Subject to the service level exclusions set forth in [Section 8.1](#) (Service Level Exclusions) of the General SaaS Terms and Conditions, Customer will be entitled to the following credits as its sole and exclusive remedy for Itron’s failure to meet the foregoing Provisioned Endpoint Daily Register Read Service Level:

Daily Register Read Service Level Credits (production environments only)	
Daily performance averaged over the calendar month	Service Level Credit (% of monthly Managed Services Subscription Fee with respect to the applicable Itron SaaS Application)
> 99.5%	0%
< 99.5% and >= 99.0%	2%
<99.0% and >= 98.0%	5%

Daily Register Read Service Level Credits (production environments only)	
Daily performance averaged over the calendar month	Service Level Credit (% of monthly Managed Services Subscription Fee with respect to the applicable Itron SaaS Application)
<98.0% and >= 96.0%	10%
<96.0%	20%

3.5.3.Daily Interval Read Service Level.

(a) **Service Level Trigger.** The Service Level Trigger for the Daily Interval Read Service Level occurs when the applicable Meters are Provisioned.

(b) **Service Level.** For newly available data on the Endpoint, the UIQ System will gather and process Interval Reads from Provisioned Meters and deliver, via the “export” mechanism of the UIQ System, at least ninety-nine and one-half percent (99.5%) of Interval Reads timestamped between 00:00 and 23:59:59 the prior day and collected throughout the day.

(c) **Service Level Calculation.** The following formula is used to show how this metric is calculated:

- For each day in the calendar month, starting on the second day of the calendar month, parse the UIQ exports between 00:00 on the prior day to 08:00 of the current day to gather the interval reads timestamped between 00:00 and 23:59:59 from the prior day
- Numerator: Aggregate the total number of interval reads that were timestamped between 00:00 and 23:59:59 of the previous day from Integrated Meters marked as Provisioned and Optimized with a state in UIQ of Active, Inactive, or Disconnected and exported by 8AM the following day, as confirmed by the timestamp of the intervals. For clarity as an example, for daily performance on October 3, parse the UIQ exports between 00:00 on October 2 through 08:00 on October 3 and count all the intervals with a timestamp between 00:00 on October 2 and 23:59 on October 2.
- Denominator: Total Meters marked as Provisioned and Optimized with a state in UIQ of Active, Inactive, or Disconnected multiplied number of expected Interval Reads per Day.
- The final SLA is calculated by averaging the performance of every day of the given calendar month.

(d) **Service Level Credits.** Subject to the service level exclusions set forth in [Section 8.1](#) (Service Level Exclusions) of the General SaaS Terms and Conditions, Customer will be entitled to the following credits as its sole and exclusive remedy for Itron’s failure to meet the foregoing Provisioned Endpoint Daily Interval Read Service Level:

Daily Interval Read Service Level Credits (production environments only)	
Daily performance averaged over the calendar month	Credit (% of monthly Managed Services Subscription Fee with respect to the applicable Itron SaaS Application)
> 99.5%	0%

<99.5% and >=98.5%	2%
<98.5% and >=97.5%	5%
<97.5% and >=96.0%	10%
<96.0%	15%

3.5.4.Near Real-Time Read Service Level. The AMI system will meet the requirement of having available 5-minute (commercial) or 15-minute (residential) interval data every 15 minutes for Provisioned and Optimized Meters

(a) **Service Level Trigger.** The Service Level Trigger for the Near Real-Time Read Service Level occurs when the applicable Endpoints are Provisioned and Optimized. As each meter is Optimized (for clarity, any new meter installed in an Optimized Area automatically becomes Optimized), Itron will identify the Endpoints that will be added to the set of Provisioned and Optimized Endpoints subject to the Near Real-Time Read Service Level.

(b) **Service Level.** For newly available intervals (e.g. the 15-minute interval or the three (3) 5-minute intervals) available on the Endpoint, the UIQ System will gather and process interval reads every 15 minutes from Provisioned and Optimized Endpoints and make available to the “export” mechanism of the UIQ System at least ninety-five percent (95.0%) of interval reads timestamped by the meter in the last 15 minutes, with the next 15 minutes (“**Near Real-Time Read Service Level**”). As an example, interval reads timestamped at between 02:45 and 03:00 will be retrieved and exported by 03:15.

(c) **Service Level Calculation.** The following formula will be used to calculate this Service Level:

- For each 15 minutes of each day, starting on the first calendar day of each month, parse the UIQ database to gather the read interval timestamped within 15 minutes of the end of interval from the prior 15 minute period along with the time that the interval was acquired.
- Numerator: Aggregate total number of interval reads from Meters marked as Optimized with a state in UIQ of Active, Inactive or Disconnected that were timestamped the period 15 minutes. As an example, if the collection(s) which are completed between 03:00 and 03:15 AM have 100,000 intervals timestamped between 02:45 and 03:00, the Numerator for the daily calculation is increased by 100,000 meters.
- Denominator: The total number of Meters marked as Optimized with a state in UIQ of Active, Inactive or Disconnected at the beginning of the day multiplied by the number of intervals expected in each 15 minute period.
- The final SLA is calculated by averaging the performance of every 15 minutes of every day of each calendar month.

(d) **Service Level Credits.** Subject to the service level exclusions set forth in [Section 8.1](#) (Service Level Exclusions) of the General SaaS Terms and Conditions, Customer will be entitled to the following credits as its sole and exclusive remedy for Itron’s failure to meet the foregoing Provisioned and Optimized Endpoint Data Read Service Level:

Near Real-Time Read Service Level Credits (production environments only)	
Every 15-Minute interval read performance averaged over the calendar month	Credit

	(% of monthly Managed Services Subscription Fee with respect to the applicable Itron SaaS Application)
$\geq 95.0\%$	0%
$< 95.0\%$ and $\geq 92.5\%$	2%
$< 92.5\%$ and $\geq 90.0\%$	5%
$< 90.0\%$	10%

3.5.5.Connect and Disconnect Service Level. The Connect and Disconnect Service Level set forth in this Section 4.4 applies to the Itron Software identified in the following table for which Customer has purchased Managed Services and paid all applicable fees:

Itron Software Eligible to Receive Data and Connect and Disconnect Service Level
UIQ: Advanced Metering Manager

(a) **Service Level Trigger.** The Service Level Trigger for the Connect and Disconnect Service Level occurs when the applicable Endpoints are Provisioned and Optimized. As each additional area is Optimized, Itron will identify the Endpoints that will be added to the set of Provisioned and Optimized Endpoints subject to the Connect and Disconnect Service Level.

(b)**Service Level.** The UIQ System will successfully execute at least (98.0%) of all (i) on-demand remote connect and (ii) on-demand remote disconnect requests made by Customer for Provisioned and Optimized Endpoints which are actively communicating (“**Connect and Disconnect Service Level**”) within 120 seconds. An on-demand remote connect request or on-demand disconnect request is a single transaction to a single Endpoint, initiated by a single user of the UIQ system. For the purposes of calculating this Service Level, multiple attempts to connect with a single device within a twenty (24) hour period will count as one failed attempt; on-demand remote connect request or on-demand disconnect request (single or batch) targeted at an Endpoint which was not read in previous 24 hours will be excluded. Service level credits will apply only if there is a minimum of 500 on-demand remote connect request or on-demand disconnect request in the applicable month.

(c) **Service Level Credits.** Subject to the service level exclusions set forth in Section 8.1 (Service Level Exclusions) of the General SaaS Terms and Conditions, and provided that the minimum number of on-demand remote connect request or on-demand disconnect requests has been met pursuant to the table below, Customer will be entitled to the following credits as its sole and exclusive remedy for Itron’s failure to meet the foregoing Connect and Disconnect Service Level:

Connect and Disconnect Service Level Credits (production environments only)	
% of Connect and Disconnect Requests Successfully Executed in the Applicable Month	Credit* (% of monthly Managed Services Subscription Fee with respect to the applicable Itron SaaS Application)
≥98.0% and 100.0%	0%
≥95.0% and <98.0%	2%
≥90.0% and <95.0%	5%
≤90.0%	10%
*Credits will apply only if there is a minimum of 500 on-demand connect or disconnect requests in the applicable month. Multiple attempts to connect with a single device within a twenty-four (24) hour period will count as one failed attempt.	

4. Environments

The following environments are defined under Managed Services

<u>Environment</u>	<u>Product/Application</u>	<u>Provision</u>
Production	UIQ	Scaled for full endpoint deployment
Production	UIQ	Data retention: 45-days
Disaster Recovery	UIQ	Scaled for full production endpoint deployment
Lower-Tiered (Test)	UIQ	Scaled to 1,000 endpoints

ATTACHMENT D
EXHIBIT D-3

Disaster Recovery Terms and Conditions

1. Definitions.

“Recovery Point Objective” or “RPO” means the maximum tolerable time period which data might “be lost from production Software due to a service interruption event.

“Recovery Time Objective” or “RTO” means the duration of time allowing for the execution of all failover processes required to return access, connectivity, functionality, and operation of production Software to Customer following declaration of a disaster event.

1.1 Disaster Recovery. Disaster Recovery (“DR”) is an optional service that is offered by Itron to hosted customers who purchase DR for an additional fee. Upon Customer’s purchase of DR services and payment of applicable fees as set forth in the Order Document or Pricing Summary, Itron will maintain DR services at a dedicated facility that is equipped to facilitate hosted operations, meter reading and interrogations, and Field Area Network (“FAN”) communications in the event DR is needed.

1.2 RPO and RTO Objectives. The Recovery Point Objective (RPO) for DR is four (4) hours. The Recovery Time Objective (RTO) for DR is twelve (12) hours. As Customer’s sole and exclusive remedy for Itron’s failure to meet the foregoing RPO and RTO objectives, Customer will be entitled to credits as follows:

Disaster Recovery Service Level Credits (disaster recovery environment only)	
# of hours of data loss beyond the maximum allowable 4 hours Recovery Point Objective (RPO)	Credit (% of monthly Managed Services Subscription Fee with respect to the applicable Disaster Recovery offering)
≥2	0%
≥4	5%
≥6	20%
>8	30%

1.3 Process. In the event of a Severity Level 1 Error (as defined in the Maintenance and Support Services Addendum), Itron will evaluate the scale of the incident, readily available mitigation plans, and the estimated time to recover. If it is apparent to Itron that an incident meeting the standards of a disaster as set forth in Itron’s Disaster Recovery plan has occurred with no possibility of mitigation, Itron will declare a disaster and begin the notification process. Itron will notify the Customer of an any such event that will result in service interruption in excess of twelve (12) hours. Once a disaster has been declared, Itron’s responsibilities for Software-as-a-Service SLAs will be temporarily suspended until the time at which Customer’s environment has been failed over and is operating in the secondary DR datacenter.

1.4 Annual Testing. Upon mutual agreement, separate SOW and for identified cost, Itron can exercise the full DR capabilities once per calendar year on Customer’s production environments and provide the results of each such test to the Customer. In the event of a DR test or exercise, no additional costs shall apply and cost only apply for additional tests unless there is an issue.

1.5 Additional Detail.

Replication and Failover Process

- Primary Disaster Recovery Switch

- Secondary Disaster Recovery Switch
- Standby infrastructure in geographically diverse location
- Replication of database via Oracle Data Guard
- Replication of application information via rsync
- DNS update for CNAMEs
- Network connections and routing pre-established (VPN, backhaul connection)
- “Over and back” exercise requires make-up read
- Exercise is 12-16 hours in duration

DR Method of Procedure (MOP)

In collaboration with Customer

- Itron will create a MOP that outlines the environments, servers, connection points, and Itron and Customer points of contact.
- The MOP defines the failover process as well as the validation points post failover.
- Itron will provide Customer instructions to access MOP.
- Recovery Point Objective and the Recovery Time Objective...4-hour RPO/12-hour RTO as set forth in the Disaster Recovery Terms & Conditions.
- Failover procedure and validation points.

Declaration of a Disaster

- Itron will consult with Customer in the event of a disaster to discuss the failover and outline the expectations as the failover progresses.
- If a disaster is imminent, Itron will inform Customer that a DR failover will take place.
- In the event of a DR failover exercise, Itron and Customer will plan and schedule a failover exercise.
- DR failover is reserved for actual disaster events (loss of a datacenter, loss of communication with a datacenter for an indeterminate amount of time.)
- A corrupt database or the loss of a virtual machine would not be characterized as a DR failover event. Restoring from backup is characterized as Business Continuity and not Disaster Recovery.

1.6 Products Eligible for Disaster Recovery.

Production UIQ Suite

ATTACHMENT D
EXHIBIT D-4

Operations Optimizer Terms and Conditions

The following Special Terms and Conditions contained within this attachment apply to Itron's SaaS Service Offering for Operations Optimizer:

1. User IDs and Passwords

As it applies to these Special Terms and Conditions, the following shall replace Section 3.3 ("User IDs and Passwords") of the SaaS General Terms and Conditions in its entirety:

Itron shall provide Customer with an integration with Azure Active Directory for managing their user identifications and passwords ("User IDs") to access Itron's Operations Optimizer. Customer shall be solely responsible for all use of Customer's subscriptions and accounts. Customer shall maintain the confidentiality of all User IDs assigned to Customer. User IDs may not be shared or used by more than one user.

2. Roles and Responsibilities

As it applies to these Special Terms and Conditions, the table in Section 14 ("Roles and Responsibilities") of the SaaS General Terms and Conditions shall be replaced in its entirety with the following:

Description of service or deliverable	Itron	Customer
Manage user access according using Azure Active Directory to add new users and promptly remove users no longer involved with the Software as a Service.		P
Maintain skill sets necessary to properly support the SaaS.	P	
Administer and monitor Servers including but not limited to utilization of CPU, memory, IOPs, and disk space.	P	
Manage and troubleshoot the secure SaaS components and processes (if applicable).	P	
Administer associated Linux, Unix, and Windows operating systems.	P	
Apply operating system and other third-party security patches and critical updates as appropriate.	P	
Maintain and troubleshoot third-party software issues required for SaaS operations pursuant to this Addendum; work with third party to troubleshoot as required.	P	
Maintain anti-virus on all windows-based Servers if applicable to the SaaS platform.	P	
Monitor communications and support communications troubleshooting activities for the SaaS.	P	
Perform software upgrade activities if required.	P	
Maintain and administer the SaaS Server databases.	P	
Manage upload and submission of meter data files; work with Itron when problems are identified.		P
Provide and maintain a Secure FTP or equivalent if included in the SOW.	P	

Perform regular system, database, and custom component backups in accordance with selected service level.	P	
Maintain the applicable standard operating procedures and run books to maintain, monitor and operate the hosted environment.	P	

**ORDER DOCUMENT
ATTACHMENT E**

Itron is not a cellular carrier and relies on its contracted wireless carriers to provide Wireless Data Services. The delivery of these services is subject to the mandatory requirements set by the wireless carriers, which, among others, are influenced by a complex regulatory environment. As such, to ensure continuous compliance with these regulations and wireless carriers' requirements, Itron is limited in its ability to accommodate proposed changes to the terms below.

WIRELESS DATA SERVICE ADDENDUM

1. **Relationship to General Terms and Conditions.** This addendum is governed by the General Terms and Conditions and applicable Order Documents.
2. **Additional Definitions.** The following defined terms are in addition to those defined in the General Terms and Conditions:

Activated Device means a Network Device that has been activated on the Wireless Data Service Network by Itron.

End User means a user of Network Device.

Headend Software means Itron software licensed to Customer under the Software Addendum that communicates with Network Devices through the Wireless Data Service.

Network Device means any cellular-enabled device provided by or on behalf of Itron to Customer.

Wireless Carrier means a wireless carrier selected by Itron.

Wireless Data Service means wireless data telecommunication service purchased by Customer under this addendum that enables communication between a Network Device and the Headend Software.

Initial Activation Period is a period of provision of Wireless Data Service as agreed by the parties in the pricing summary.

3. **Ordering and Activation.** Customer will order Wireless Data Service by execution of the Contract and issuance of Notice to Proceed to Itron for the Initial Activation Period in accordance with this addendum. Itron shall procure Wireless Data Service from the Wireless Carrier and prepare each Network Device for Wireless Data Service.

5. **Line Term.** Each Activated Device comes with Wireless Data Service for the Initial Activation Period. At least 60 days in advance of the expiration of the Initial Activation Period for an Activated Device and for each annual period thereafter, Itron shall provide a quotation for renewal pricing for Wireless Data Service for successive one-year periods (each a **"Renewal Activation Period"**). Wireless Data Service will continue for a one-year renewal period at the then-quoted price unless Customer provides Itron with written notice of non-renewal no less than 120 days, or Itron provides Customer with written notice of non-renewal no less than 120 days, prior to the end of the Initial Activation Period or the then-current Renewal Activation

Period. In the case of a wide scale catastrophic event like a hurricane or act of God, that requires the majority of APs and Socket APs to be replaced outside of warranty, then Itron will agree to provide one time credits to customer for any unused portion of the prepaid cellular subscription, as a discount on the replacement purchase of Itron hardware and/or cellular services for the replacement device.

5. Invoicing. Itron will invoice Customer for Wireless Data Service fees as set forth in the applicable pricing summary for the Initial Activation Period upon shipment of the Activated Device. If monthly fees are established in the pricing summary, Itron will invoice Customer monthly for Wireless Data Service at the rates listed in the pricing summary. Itron also shall pass through to Customer, and Customer shall be responsible for, any tariffs, surcharges, duties or other charges, including government and regulatory fees, that are assessed directly or indirectly on Itron with respect to the provision of the Wireless Data Service.

6. Authorized Use.

6.1 The Wireless Data Service shall be used solely by Customer to establish a wireless data connectivity between the Headend Software and Network Devices or between CUSTOMER's SCADA and Network Devices and shall not be re-sold or otherwise provided to third parties by Customer. Except as otherwise stated in this addendum, Wireless Data Service is not transferrable.

6.2 Customer shall not, and shall not permit End Users to use the Wireless Data Service or Network Devices: (a) in an illegal or unauthorized manner; (b) in a manner prohibited by the applicable plan, option, feature or application not authorized hereunder or otherwise not in compliance with this addendum; (c) in a manner that has a material adverse impact on the Wireless Data Service or its operations.

6.3 Itron or the applicable Wireless Carrier may immediately suspend, limit, modify or terminate Wireless Data Service if: (a) Customer or End User is in violation of the above in sub-section 6.2 or Wireless Carrier's Requirements (defined below); (b) in the event of an emergency or in order to provide resources to emergency; (c) the provision or use of the Wireless Service is, or is likely to become unlawful; (d) the provision of Wireless Data Service or related infrastructure has, or is likely to cause death, personal injury or damage to property; (e) Wireless Carrier decided to withdraw Wireless Service from the market or modify Wireless Service due to its commercial considerations; (e) Customer or End User adversely interferes or prevents Itron's or Wireless Carrier's required updates, upgrades, modification of functionality, replacement or maintenance of Network Devices or infrastructure related to the provision of Wireless Data Service; (f) Itron is enabling a transition of Wireless Data Service from one Wireless Carrier to another. To the extent practical Itron shall attempt to give a timely notice to Customer prior to any suspension, limitation, modification or termination of the Wireless Data Service, however, due to the nature of the reasons which may necessitate such actions, neither Itron nor Wireless Data Service may be able to give such timely notice. Customer shall promptly inform Itron in writing of known instances of violation of section 6.2 or Wireless Carrier's Requirements. In the event of a violation of section 6.2 or Wireless Carrier's Requirements by Customer or End User, Customer shall promptly provide Itron with reasonable relevant information concerning such violation and reasonably cooperate with Itron or Wireless Carrier in investigation and resolution of such violation. If Customer or End User continues using the Wireless Data Service in a manner prohibited above, Itron may also deny activation to new lines or, upon written notice, may terminate this addendum for cause in accordance with the General Terms and Conditions.

6.4 Customer shall indemnify and defend Itron and Wireless Carrier from any costs, claims or liability assessed against Itron or Wireless Carrier arising from or relating to any violation of the section 6.2 or Wireless Carrier's Requirements (defined below) by Customer or End User.

7. Wireless Data Service Availability. Neither Itron nor Wireless Carrier guarantees permanent availability of Wireless Data Service as Wireless Data Service uses technologies which may be subject to service area limitations, interruptions and dropped transmissions caused by atmospheric, topographical, or environmental conditions, cell site availability, equipment or its installation, governmental regulations, system limitations, maintenance or other conditions or activities affecting Wireless Data Service operation. Wireless Data Service may not be available in all areas. Itron does not guarantee the availability of Wireless Carrier or that an alternative Wireless Carrier will be available to replace Wireless Carrier without any interruption to Wireless Data Service.

8. Itron Responsibilities. Itron's responsibilities are detailed in Attachment D- Managed Software as a Service Addendum

9. Enhancement of Wireless Data Service. Customer shall obtain Itron's prior approval and written agreement before it may install, deploy or use any regeneration equipment or similar mechanism (for example, a repeater) to originate, amplify, enhance, retransmit or regenerate Wireless Data Service.

10. Wireless Carrier's Requirements. Customer acknowledges that Itron is unable to provide any Wireless Data Service other than through a Wireless Carrier and Itron's ability to provide any goods or services in connection with this addendum is dependent on the enablement or availability of such goods or services from a Wireless Carrier. Wireless Carrier may require Itron to pass-through to Customer and, if applicable, to End Users its certain terms, conditions of provision of goods or services or other requirements (collectively, "**Wireless Carrier's Requirements**"). As examples and without limitation, such Wireless Carrier's Requirements may include End User license agreement and an acceptable use policy. Accordingly, Itron may communicate any Wireless Carrier's Requirements to Customer in writing and if Customer refuses to comply with the same, Itron may, notwithstanding anything to the contrary in this addendum or General Terms and Conditions and without any ensuing liability to Itron, immediately suspend, limit, modify or terminate any portion of Wireless Data Service that is not compliant with the latest Wireless Carrier's Requirements or if such suspension, limitation, modification or termination of Wireless Data Service is impractical, then Itron may immediately terminate this addendum.

11. Limitation of Liability. IN ADDITION TO THE LIMITATIONS ON LIABILITY SET FORTH IN THE GENERAL TERMS AND CONDITIONS, WITH RESPECT TO THE WIRELESS DATA SERVICE ONLY, ITRON AND ITS AFFILIATES WILL HAVE NO LIABILITY TO CUSTOMER AND END USERS FOR ANY CAUSES OF ACTION, LOSSES OR DAMAGES OF ANY KIND WHATSOEVER ARISING OUT OF THE ACTS OR OMISSIONS OF THE WIRELESS CARRIER OR ANY OTHER THIRD-PARTY INCLUDING, WITHOUT LIMITATION: (I) MISTAKES, OMISSIONS, INTERRUPTIONS, ERRORS, FAILURES OR DEFECTS IN FURNISHING WIRELESS DATA SERVICE, (II) DISCONTINUANCES OR CHANGES IN THE WIRELESS DATA SERVICE.

12. Disclaimer. Itron has entered into an agreement with Wireless Carrier relating to the provision of Wireless Data Service. Itron is willing to manage the Wireless Data Service to Customer pursuant to its agreement with Wireless Carrier, to comply with Itron's obligations under such agreement and to facilitate billing of Customer for the Wireless Data Service. ITRON IS NOT A TELECOMMUNICATIONS SERVICE PROVIDER OR WIRELESS CARRIER AND, EXCEPT AS EXPRESSLY SET FORTH IN THIS PARAGRAPH, ITRON MAKES NO WARRANTIES OR REPRESENTATIONS WHATSOEVER, DIRECTLY, OR INDIRECTLY, EXPRESS OR IMPLIED, AS TO THE DURABILITY, AVAILABILITY, SECURITY, FITNESS FOR USE, QUALITY, PERFORMANCE OR NON-INFRINGEMENT OF THE WIRELESS DATA SERVICE. ITRON SHALL HAVE NO OBLIGATION TO INDEMNIFY OR DEFEND CUSTOMER OR ANY INDEMNITEES UNDER THE INDEMNIFICATION SECTION OF THE GENERAL TERMS AND CONDITIONS OR OTHERWISE

FROM OR AGAINST ANY INFRINGEMENT CLAIMS RELATING TO THE WIRELESS DATA SERVICE.

13. No Third-Party Beneficiary. CUSTOMER AGREES THAT, AS IT RELATES TO THIS ADDENDUM, CUSTOMER AND ITS END USERS ARE NOT THIRD-PARTY BENEFICIARIES OF ANY AGREEMENT BETWEEN ITRON AND THE WIRELESS CARRIER OR ANY AGREEMENT A WIRELESS CARRIER MAY HAVE WITH ITS UNDERLYING CARRIER OR ANY OTHER THIRD PARTY. IN ADDITION, SUBJECT TO THE FOREGOING, CUSTOMER ACKNOWLEDGES AND AGREES THAT THE WIRELESS CARRIER AND ITS AFFILIATES, APPLICABLE UNDERLYING CARRIERS AND CONTRACTORS SHALL HAVE NO LIABILITY BASED IN CONTRACT TO CUSTOMER AND END USERS UNDER THE AGREEMENT BETWEEN ITRON AND SUCH PARTIES OR OTHERWISE IN CONNECTION WITH THIS ADDENDUM AND CUSTOMER, ON BEHALF OF ITSELF AND END USERS, HEREBY WAIVES ANY AND ALL CLAIMS OR DEMANDS THEREFOR.

14. Survival. The following sections of this addendum shall survive termination or expiration of this addendum, General Terms and Conditions or any Order Document or Statement of Work: 1 (“Relationship to General Terms and Conditions”), 2 (“Additional Definitions”), , 5 (“Invoicing”), 6 (“Authorized Use”), 7 (“Wireless Data Service Availability”), 9 (“Enhancement of Wireless Data Service”), 12 (“Limitation of Liability”), 12 (“Disclaimer”), 13 (“No Third Party Beneficiary”), and 14 (“Survival”).

ATTACHMENT F TO THE ORDER DOCUMENT

Maintenance and Support Addendum

1 Relationship to General Terms and Conditions

This Addendum is governed by the General Terms and Conditions and applicable Order Documents.

2 Additional Definitions

The following defined terms are in addition to those defined in the General Terms and Conditions:

Annual Adjustment means Itron's annual price increase.

Annual Fees means the annual Fees identified in an Order Document for each category of Covered Product, plus the Annual Adjustment, if any.

Client Services Guidelines Documents means the following documents as they may be updated by Itron from time to time: "Itron Equipment Repair Center Locations", and "Working Effectively with Itron Global Customer Support Services". Copies of the Client Services Guidelines Documents may be obtained by calling Itron Global Customer Support Service at (877) 487-6602 or such other number or process provided by Itron to Customer.

Covered Equipment means Itron Equipment identified in an Order Document for which Customer has purchased Maintenance Services.

Covered Firmware means Itron's network and application firmware embedded within a communicating device identified in an Order Document (e.g., network interface cards, meters, endpoints, network equipment, etc.) for which Customer has purchased Maintenance Services.

Covered Products mean Covered Firmware, Covered Software, Covered Equipment.

Covered Software means Itron software identified in an Order Document for which Customer is entitled to receive Maintenance Services to include the Middleware as defined in Attachment B - VIWAPA AMI Implementation SOW.

Error means a material failure of Covered Firmware or Covered Software to comply with applicable published Itron specifications.

Fix means a correction or workaround for an Error.

Global Support Services means those support services provided by Itron technical representatives via telephone, email, website or other means to assist Customer's Primary Service Contacts with questions or issues related to the operation of Covered Products.

Improvement means an update, modification, enhancement and/or extension to Covered Software functionality that is included in a Release.

M&S Commencement Date means the date upon and after which a Covered Product will be entitled to receive Maintenance Services, which unless otherwise provided in the applicable Order Document, will be as follows:

Covered Product	M&S Commencement Date
On premise Covered Software	Itron DI Applications: Date Itron DI Application is initially allocated in the DI Platform for Customer endpoint download following receipt of an accepted Purchase Order. Other Itron Software: First day of month following date Covered Software is made available to Customer
Covered Firmware	Date of shipment of the applicable communication device
Covered Software provided as Software-as-a-Service or Hybrid SaaS subscription	The validation of such Service Offering implementation by Itron pursuant to the applicable Statement of Work.
Covered Equipment	End of warranty period
Third-Party Covered Products	Per applicable third-party service provider terms and conditions

Maintenance Billing Cycle means a period of one (1) year beginning on January 1st of each calendar year. The first year and last year of Maintenance may be prorated as applicable.

Maintenance Services means services provided under this Addendum.

Operating Condition means performance in accordance with applicable published Itron specifications.

Primary Services Contacts means Customer's primary support staff who provides internal support to Customer's operations personnel and who are key interface to Itron for all Maintenance Services.

Release means a collection of Fixes and / or Improvements made available by Itron to Customer including major and minor releases.

Service Levels means the defined level of impact and associated response time, effort level, and escalation path procedures and guidelines described in Attachment 1 to this Addendum.

Service Offering has the meaning set forth in the Attachment D - Managed Software-as-a-Service Addendum.

Service Request means an Itron tracked Customer request for Global Support Services.

3 Principal Services Contacts

3.1 Designation by Customer

Customer shall designate a minimum of one (1) and not more than two (2) Primary Services Contacts for each Covered Product line, to serve as administrative liaisons for all matters pertaining to Maintenance Services for such Covered Product line and shall provide their contact information to Itron's customer account representative. Primary Services Contacts shall promptly report problems with Covered Products

by submitting a Service Request for entry into Itron's support tracking system. Although it is Customer's sole right to choose its Primary Services Contacts, Customer and Itron acknowledge that each Primary Services Contact must have the appropriate technical skills and training for the position. If Customer replaces a Primary Services Contact, Customer will provide updated contact information to Itron's customer account representative, and the new Primary Services Contact will be properly trained prior to interfacing with Itron support personnel.

3.2 Training of Principal Services Contacts

Before a Primary Services Contact interfaces with Itron support personnel, he/she will attend training sessions offered by Itron, an Itron-approved trainer, or Customer's training program supplied by Itron during this project to ensure that the Primary Services Contact is (i) knowledgeable about operation of the applicable Covered Products, and (ii) qualified to perform problem determination and remedial functions with respect to such Covered Products. Customer may perform Itron-approved training or may engage Itron to perform training of Primary Services Contacts at Itron's then current rates. Itron will make training sessions available by remote video conference or training will be made available at a location or in a manner mutually agreed by the Parties. Customer shall be responsible for all Customer's associated travel-related expenses and, if the Parties agree that training will be provided at a location other than an Itron-designated facility (e.g., at a Customer-proposed facility), Customer will also reimburse Itron's travel-related expenses. The Primary Services Contacts must have the skills and capabilities to train other Customer personnel on Covered Products. Itron may update Covered Product training from time to time and, upon receiving notice of such updates from Itron, Customer shall promptly provide such training to its Primary Services Contacts in accordance with this Section. For clarification on site training will be provided during the project. Global Support Services & Service Requests

3.3 Global Support Services

Itron will make support representatives available to provide technical support during its then current normal business hours as set forth in the Client Services Guidelines Document. Global Support Services include troubleshooting & problem diagnosis relating to Covered Products; release or system management consulting; and recommendations for fully utilizing Covered Products. Customer acknowledges and agrees that Global Support Services are not intended as a substitute for training of Customer personnel, field support, or Itron professional services. Nor will Customer use Global Support Services in lieu of having qualified and trained support personnel of its own.

3.4 Service Request Process

Customer shall submit Service Requests in the manner required by the Client Services Guidelines Documents and Service Levels. When Customer submits a Service Request, Customer will reasonably assess its business urgency according to the appropriate Severity Level in Attachment 1 to this Addendum. Itron will designate the initial Severity Level and the Parties will resolve any perceived gap regarding the Severity Level designation as soon as is reasonably practical. Customer may submit Service Requests on a 24/7/365 basis and Itron will respond to such Service Requests in accordance with the Service Levels.

3.5 Field Support

At Customer's request, and Itron's approval, Itron will dispatch support personnel to Customer's location to provide onsite Global Support Services ("Requested Field Support") related to a reported problem which cannot be addressed remotely. Requested Field Support will be billed at Itron's then-current rates, and Customer will reimburse Itron's travel-related expenses, unless the cause of the reported problem is found to be due to an error in the Itron product or service. For clarity, if the reported problem is found to be due to an error in the Itron product or service, Customer will not be billed for the Field Support rates, nor the travel-related expenses.

4 Itron Firmware and Software Maintenance

4.1 Scope

Firmware Maintenance Services covers its associated Covered Firmware embedded within the applicable communicating device and is provided as part of SaaS Hybrid subscription. Software Maintenance Services covers its associated Covered Software sold as: (i) on premise software license, or (ii) Software-as-a-Service or SaaS Hybrid subscription.

4.2 Modifications

Itron may modify or replace Covered Firmware and Covered Software so long as such modifications or replacements do not eliminate key, documented functionality provided by the most current System Release.

4.3 Fixes

Itron shall provide Fixes in accordance with the Service Levels. Itron's obligations with respect to Service Levels are contingent upon Customer (i) devoting the necessary resource effort required to support of Itron restoring the system and remediating the Error, (ii) responding to requests made by Itron within the applicable Response Time, (iii) assigning only qualified personnel to help Itron address the Error, and (iv) providing all information, access, and assistance reasonably requested by Itron to address the Error.

4.4 Improvements

Itron shall provide Improvements, if any, at no charge to Customer if such Improvements are made within the current product specifications and are made available to Itron customers at no charge. Improvements released as new add-on modules/features and not part of the product's original specifications, may require additional licensing and support fees and will be made available at Itron's then current rates.

4.5 Software Releases

4.5.1 Release Numbering Convention. Upgrades, Fixes and/or Improvements are made available to customers through periodic Software Releases. For informational purposes, Itron's current practice (which may vary and be changed by product, at any time in Itron's discretion) is to provide Software Releases using the numbering guideline, "X.X.X.X"

4.5.2 The first place, "X.X.X.X", in Itron's numbering convention refers to a "Major Release", or "System Release", which consists of a new version of Covered Software. A Major Release may include architectural changes, Improvements, Fixes and / or interfaces to new functional modules or platforms. A Major release may require infrastructure or component updates which affect compatibility with previous release versions.

4.5.3 The second place, "X.X.X.X", in Itron's numbering convention refers to a "Minor Release, which is an update to a current Major Release. A Minor Release may include consolidation of previous Service Packs, Improvements, Fixes, platform / 3rd party updates. Minor Release are provided to Itron customers on a regularly scheduled basis.

4.5.4 The third place, "X.X.X.X", in Itron's numbering convention refers to a "Service Pack, which is an update to specific modules found in a current Major Release. A Service Pack may include Fixes to Severity 1 - Severity 4 issues for a specified Minor or Major Release.

4.5.5 The fourth place, "X.X.X.X", in Itron's numbering convention refers to a "Hot Fix," which is an unscheduled release provided to one or more customers as a short-term, temporary fix to a critical Severity Level 1 Error. While not utilized by all Itron software product lines, Hot Fix releases are not made available to Itron customers generally but may be included in the next scheduled Minor Release or Service Pack for general release.

4.6 Support for Covered Firmware

Itron will only provide Maintenance Services for Covered Firmware if Customer (i) tests and approves installation of the latest Covered Firmware Fix within twelve (12) months of it being made available to

Customer, and (ii) tests and approves installation of the latest Covered Firmware Improvement within twenty-four (24) months of being made available by Itron.

4.7 Support for SaaS or IaaS

Itron will only provide Maintenance Services for Covered Software sold as a Software-as-a-Service or Hybrid SaaS subscription if Customer: (i) is current on all applicable fees for such Software-as-a-Service or SaaS Hybrid subscription and related Maintenance Services, and (ii) tests a Release as installed by Itron either in Customer's production Software-as-a-Service or Hybrid SaaS environment, or in Customer's funded non-production Software-as-a-Service or Hybrid SaaS environment, prior to Customer's full production use of the Release.

4.8 Support for Unsupported Itron Software and Firmware

At Customer's request, Itron may elect to provide Maintenance Services for an unsupported Release at Itron's then-current rates.

4.9 Mandatory Revisions

Customer must validate and approve the installation all software and firmware updates, patches, and service packages provided by, or as directed by, Itron from time to time and which may be required to correct errors, vulnerabilities, third-party concerns, or as otherwise necessary to ensure proper functioning of the Covered Software or to protect the interests of the Parties ("Mandatory Revisions"). ITRON IS NOT LIABLE FOR ANY CUSTOMER OR THIRD-PARTY DAMAGES RESULTING FROM CUSTOMER'S FAILURE TO INSTALL ANY MANDATORY REVISION IN A TIMELY MANNER.

4.10 Restoring Firmware or Software to Maintenance Services

If Customer declines or discontinues Maintenance Services for Covered Firmware or Covered Software and thereafter wishes to resume such Maintenance Services for the most recent Release of that Covered Firmware or Covered Software, Customer shall, prior to receiving Maintenance Services, notify Itron in writing of its request for Maintenance Services and pay Itron's then-current re-initiation fee, which shall not exceed an amount equal to all Annual Fees that would have been invoiced for the applicable Covered Firmware or Covered Software if Customer had not elected to decline or discontinue Maintenance Services for that Covered Firmware or Covered Software, plus a five percent (5%) markup, in addition to prorated Annual Fees for the then-current Maintenance Billing Cycle.

4.11 Exclusions

Itron shall have no obligation to provide Maintenance Services for, or liability to Customer for Covered Software adversely affected by (i) use of Covered Firmware or Covered Software by anyone other than Itron in combination with software, equipment, or communications networks not referenced in the Documentation as being compatible with the Covered Firmware or Covered Software; (ii) modification or recompiling of Covered Firmware or Covered Software or Covered Software installation instructions / installation scripts or database schema scripts, or improper installation of a Release, by anyone other than Itron, (iii) failure to perform customer responsibilities describe in this Addendum, (iv) use of an unsupported version of Covered Firmware or Covered Software by anyone other than Itron; (v) Customer's failure to implement a Mandatory Revision; (vi) maintenance and/or support of Covered Firmware or Covered Products other than by Itron; (vii) viruses introduced through no fault of Itron; or (viii) network or communication link failures.

4.12 Documentation and Backup

Itron will make an electronic copy of the Documentation as defined in Attachment J- Software Addendum available to Customer at no additional charge via physical media or download access. Itron will also maintain a copy of its most recent supported version of executable Covered Firmware and on premise Covered Software to be made available to Customer or installed by Itron as necessary in the event of

corrupted or inoperative Covered Firmware or on premise Covered Software. Said copy of executable Covered Firmware or on premise Covered Software or Third-Party software does not relieve Customer of its responsibility to backup and manage its Covered Firmware or on-premise software installation as part of ongoing system operation.

4.13 Customer Responsibilities

The provision of Maintenance Services for Covered Firmware or Covered Software by Itron assumes that Customer will facilitate such services as follows:

4.13.1 Service Requests

Customer will support Itron investigation and restoration efforts as defined in the Service Level table and will act upon / implement support solutions and workarounds recommended by Itron in a timely fashion. When escalating a Service Request with Itron, Customer's Primary Service Contact shall collect and provide all data logs, findings, analysis, and any relevant forensic information pertaining to the issue as outlined in Client Services Guideline Documents.

4.13.2 Data Review

If Itron determines that it is necessary to evaluate Customer data to reproduce error conditions not reproducible with Itron's standard test data sets, Customer will provide Itron with reasonable access to such data. Itron shall not be liable for any delay or failure to resolve the problem if access to such Customer data is denied to Itron.

4.13.3 Installation and Upgrades

Customer will engage Itron Global Support Services or their Itron account team for any Covered Firmware or on premise Covered Software installations and upgrades which require support beyond that provided herein. This applies to optional updates not affecting Business operations and will be provided at no additional cost.

5 Itron Equipment Maintenance

5.1 Maintenance Procedures

Customer shall initiate a request for Maintenance Services for Covered Equipment by delivering the Covered Equipment to the applicable Itron Certified Repair Center identified on the Itron Equipment Repair Location Table. Customer will return Covered Equipment at Customer's expense and in accordance with Itron's then-current Return Material Authorization ("RMA") procedures. Upon receipt of Covered Equipment (with the required information) under Itron's RMA procedures, Itron shall assess the item to determine (a) whether it is in fact Covered Equipment and (b) whether the maintenance requested is included within the Maintenance Services ordered by Customer and not otherwise excluded from coverage. If the returned equipment is determined to be Covered Equipment and the maintenance requested is included in the Maintenance Services ordered by Customer, Itron shall (i) perform preventative Maintenance Services necessary to maintain the Covered Equipment in Operating Condition, and (ii) diagnose and correct any failure in the Covered Equipment as necessary to meet Operating Condition, excluding minor cosmetic deficiencies such as blemishes, dents or scratches, and (iii) return the item of Covered Itron Equipment to Customer at Itron's expense within the applicable turnaround time identified on the Itron Equipment Repair Table. If Itron determines that returned equipment is not Covered Equipment or is excluded from the Maintenance Services ordered by Customer, then Itron will proceed in accordance with the estimation fees section below.

5.2 Exclusions

Itron is under no obligation to perform Covered Equipment Maintenance Services in circumstances where the failure or damage is due to: (i) accident, abuse, misuse, inadequate maintenance, problems caused by electrical power surges or acts of God outside of the tolerances set forth in the applicable published Itron

specifications; (ii) service or repair processes (including installation or de-installation of equipment, parts, or firmware/software) not performed or authorized by Itron; (iii) use of parts, configurations or repair depots not certified or authorized by Itron; or (iv) Customer's failure to perform material Customer responsibilities in accordance with this Addendum, including caring for Covered Equipment in accordance with applicable Documentation.

5.3 Estimated Fees

Itron will provide Customer with a price quote for the estimated cost (including current inspection fees), including labor, materials and shipping, for any repairs to equipment that are requested, which Itron determines are excluded from or not included within the Maintenance Services ordered by Customer. If Customer elects not to proceed with the requested repair, Itron will return the item of equipment at Customer's expense and Itron may charge Customer its then-current inspection fee.

5.4 Adding/Restoring Equipment to Maintenance Services

Following the Effective Date, additional Covered Equipment purchased by Customer, of a similar type and model already covered under this Addendum, shall automatically be deemed to be Covered Equipment following the M&S Commencement Date. If Customer declines or discontinues Maintenance Services for any Covered Equipment and thereafter wishes to add or restore such equipment as Covered Equipment, Itron may, prior to such equipment being included as Covered Equipment, inspect such equipment at Itron's then current rates to determine whether it is in Operating Condition and/or charge Itron's then current re-certification fee, in addition to prorated Annual Fees for the then-current Maintenance Billing Cycle (the "Re-initiation Costs"). At Customer's request, Itron will provide Customer with a quote for estimated Re-initiation Costs for equipment that Customer wishes to add or restore as Covered Equipment under this Section.

5.5 Equipment Responsibilities

Itron shall make available, and Customer shall obtain, a copy of the Documentation for Covered Equipment and Customer will be responsible to perform preventive maintenance for each such item in accordance with such Documentation. Customer shall also keep accurate records of Covered Equipment serial numbers and locations to assist Itron with performing Maintenance Services.

6 Fees and Invoicing

6.1 Annual Fees

Customer shall pay Annual Fees in advance of each Maintenance Billing Cycle in which it will receive Maintenance Services.

6.2 Invoicing

Itron will invoice Customer for the first Maintenance Billing Cycle upon User Acceptance Testing(UAT) completion. Itron may invoice Customer for Maintenance Services for a Covered Product that is added during any Maintenance Billing Cycle at a prorated amount. Otherwise, Itron will invoice Customer for each subsequent Maintenance Billing Cycle approximately twenty (20) days prior to the commencement of the following Maintenance Billing Cycle.

6.3 Renewal Notice

Itron will provide Customer a renewal notice for Itron Covered Products at least one hundred twenty (120) days prior to the commencement of each Maintenance Billing Cycle. Customer may discontinue Maintenance Services for any Covered Product(s) by providing Itron with written notice of non-renewal no less than ninety (90) days prior to the commencement of a Maintenance Billing Cycle.

6.4 Purchase Order

For items purchased outside of this agreement Customer shall submit a Purchase Order to Itron for the quoted amount of Itron Covered Products prior to the commencement of each Maintenance Billing Cycle.

7 Reserved

8 End of Support

Itron may discontinue Maintenance Services for any Covered Equipment, Covered Firmware or Covered Software, effective as of the end of the applicable Maintenance Billing Cycle, by giving Customer written notice of such discontinuance no less than one hundred eighty (180) days prior to the end of such Maintenance Billing Cycle. The end of support date for a Third Party Covered Product shall be the date specified by the applicable third-party service provider, which date will be promptly communicated by Itron to Customer following the date of receipt.

If the end of support date is scheduled within a subsequent Maintenance Billing Cycle, Annual Fees for that subsequent Maintenance Billing Cycle will be pro-rated through the end of support date. At Customer's request, or as defined in a related SaaS addendum / Order Document, Itron may elect to provide custom support for products for which Maintenance Services have been discontinued at Itron's then-current rates.

Periodically, Itron will make available product plan publications, including product information letters (PIL), product newsletters or written technology roadmaps which outline Itron's general plans for continued support and end of support of applicable Covered Products. Product publications are used as general guidelines for Customer communications and planning, which may be updated from time to time.

9 Survival

The following sections of this Addendum shall survive termination or expiration of this Agreement or any Order Document or Statement of Work: Section 5.14 (Exclusions), 6.2 (Exclusions), 7 (Fees and Invoicing), 9 (End of Support), and 10 (Survival).

Attachment 1 to Maintenance & Support Services Addendum
– Software Maintenance & Support Service Levels –

Severity Level	Response Times	Restoration Targets	Resolution Targets***	Escalation
<p>Severity Level 1*</p> <p>Business Impact: Critical Impact / System Down. A Production System Error for which there is no work-around, which causes Covered Firmware or Covered Software Product or a critical business function / process of said product to be unavailable such that system operation cannot continue.</p> <p>Example: a) Billing cannot be completed, b) Major documented function not working, c) System hung or completely down</p>	<p>During regular business-hours Itron will begin the Service Request process during Customer's initial call.</p> <p>During after-hour periods, Itron will respond to a critical support voice messages within 15 minutes by a return call to Customer, to validate receipt of the critical support call and begin the Service Request process.</p> <p>Following the start of the Service Request process Itron will respond to Customer's Service Request within two (3) hours with an investigation response.</p> <p>Itron will update Customer at three (3) hour intervals during each day the Service Request remains unresolved, or as otherwise agreed by the Parties.</p> <p>Customer will respond to an Itron inquiry or request within three (3) hours.</p>	<p>Itron will make diligent efforts on a 24x7 basis, or as otherwise agreed by the Parties, to:</p> <p>i) restore Covered Firmware or Covered Software with a change to eliminate root cause, ii) provide a workaround that restores Covered Firmware or Covered Software and downgrades the Severity Level to S2, S3, or S4.</p> <p>Customer's Support Staff must be available 24x7 to work cooperatively with Itron continuously until restoration is achieved.</p> <p>Restoration Target:</p> <p>4 hours if Itron SaaS.</p>	<p>5 business days (for non-bug fixes)</p> <p>Root Cause Analysis (RCA): 30 business days</p>	<p>An unresolved Service Request shall be escalated to Itron management as follows:</p> <p>After 30 minutes: Technical Customer Support Team Lead</p> <p>After 8 hours: Manager, Technical Client Services</p> <p>After 16 hours: Director, Global Support Services</p> <p>After 48 hours: Service Request. Vice President, Services and Delivery</p> <p>After 72 hours: President, Itron</p>

Severity Level	Response Times	Restoration Targets	Resolution Targets***	Escalation
<p>Severity Level 2*</p> <p>Business Impact: Major impact, degraded Operation. An Error other than a Severity Level 1 Error, for which there is no work-around, which degrades or limits operation of major system functions causing Covered Firmware or Covered Software to miss required business interface or deadlines. Covered Firmware or Covered Software remains available for operation but in a highly restricted fashion.</p> <p>Example: a) Billing cannot be completed on time, b) Major function is operating outside documented timing / term, c) Covered Firmware or Covered Software operating slow, missing data, data delivery, daily mission.</p>	<p>During regular business-hours Itron will respond to Customer regarding Service Request within one (1) business day.</p> <p>While Service Request remains unresolved, Itron will update the Customer and the Service Request at least every other business day, or as otherwise agreed by the parties.</p> <p>Customer will respond to an Itron inquiry or request within one (1) business day.</p>	<p>Itron will make diligent efforts during normal business hours to:</p> <p>i) restore Covered Firmware or Covered Software with a change to eliminate root cause, ii) provide a workaround that restores Covered Firmware or Covered Software and downgrades the Severity Level to S3 or S4.</p> <p>Restoration Target:</p> <p>5 business days if Itron SaaS.</p>	<p>15 business days (for non-bug fixes)</p> <p>Root Cause Analysis (RCA): Not Available</p>	<p>An unresolved Service Request shall be escalated to Itron management as follows:</p> <p>After 1 hours: Technical Customer Support Team Lead</p> <p>After 8 hours: Manager, Technical Client Services</p> <p>After 24 hours: Director, Global Support Services</p> <p>After 30 Days: Vice President, Services and Delivery</p>

Severity Level	Response Times	Restoration Targets	Resolution Targets***	Escalation
<p>Severity Level 3**</p> <p>Business Impact: Minor Business Impact, compromised operations. An Error other than a Severity Level 1 or Severity Level 2 Error that has moderate impact on use of or access, with low business impact, but not preventing Customer from performing daily activities.</p> <p>Example: The Service Request affects use by Covered Firmware or Covered Software users, allowing Customer's functions to continue to meet daily business needs.</p>	<p>During regular business-hours Itron will respond to Customer regarding Service Request within two (2) business days.</p> <p>While Service Request remains unresolved, Itron will update the Service Request weekly, or as otherwise agreed by the parties.</p> <p>Customer will respond to an Itron inquiry or request within two (2) business days.</p>	<p>Itron will work during normal business hours to:</p> <p>i) restore Covered Firmware or Covered Software with a change to eliminate root cause, ii) provide a workaround that restores Covered Firmware or Covered Software and downgrades the Severity Level to S4.</p> <p>Restoration Target:</p> <p>45 business days if Itron SaaS.</p>	<p>90 business days (for non-bug fixes)</p> <p>Root Cause Analysis (RCA): Not Available</p>	

Severity Level	Response Times	Restoration Targets	Resolution Targets***	Escalation
<p>Severity Level 4</p> <p>Business Impact: Standard Operations intact. A low or no-impact Error other than a Severity Level 1, Severity Level 2 or Severity Level 3 Error, or a request for enhancement / new functionality</p> <p>Example:</p> <p>Generally, a cosmetic Error or an Error which does not degrade Customer's use of the product or system.</p>	<p>During regular business-hours Itron will respond to Customer regarding Service Request within three (3) business days.</p>	<p>Itron GSS Management Team will make commercially reasonable efforts during normal business hours to understand the Service Request and provide applicable recommendations as to when a Fix may be schedule in a future release, or how to proceed with a formal enhancement request to Itron's product and delivery teams.</p> <p>Restoration Target:</p> <p>There is no restoration target for Severity Level 4 Issues.</p>	<p>There is no resolution target for Severity Level 4 Issues.</p> <p>Root Cause Analysis (RCA): Not Available</p>	

* Severity Level 1 and Severity Level 2 must be reported by phone to ensure they are addressed under the appropriate severity level response process. Service Requests entered by email or Web access are generally addressed as a Severity Level 3.

** Service Request opened on non-production servers / environments are entered as a Severity Level 3.

*** Issue must be repeatable before Resolution Target Time begins barring no software application bugs.

ATTACHMENT G TO THE ORDER DOCUMENT

Data Processing Addendum

This Data Processing Addendum (“DPA”) supplements and forms part of the agreement (“Agreement”) entered into by Itron and Customer, collectively, herein referred to as “Parties” and each individually as a “Party.”

PURPOSE

Pursuant to the Agreement, Itron may Process Controller Personal Data in the context of providing Services to Controller.

The provisions laid out by this DPA shall be applicable to all activities that are performed in connection with the Agreement and by Itron, their employees or agents when encountering Controller Personal Data originating from, collected for, or otherwise Processed on behalf of Controller.

With respect to the Processing of Controller Personal Data, Itron is subject to the Data Protection Laws, the Agreement, and Controller Instructions.

This DPA sets out the terms and conditions for the Processing of Controller Personal Data by Itron. Further details on scope, duration, and purposes for the Processing as well as categories of Controller Personal Data and Data Subjects are set forth in the Agreement and in Exhibit G-1 to this DPA.

Controller shall ensure that it is authorized to transfer the relevant Personal Data to Itron for the purposes of providing Services under the Agreement (including any amendments thereof).

DEFINITIONS

“**Affiliate**” means any legal entity that directly or indirectly controls, is controlled by, or is under common control with, a Party to this Agreement, where “control” means ownership of at least fifty (50) percent of the equity having the power to vote on or direct the affairs of the entity.

“**Controller Information**” means any operational, confidential, or employee data, including Controller Personal Data, exchanged between the parties in connection with the Agreement and the Services provided thereunder. Such information is agreed to be Processed for the business purpose of contracting.

“**Controller**” means the Customer, to the extent that it, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“**Controller Personal Data**” means any Personal Data originating in the sphere of the Controller and Processed by Processor in connection with the Services. Controller Personal Data does not include data that has been anonymized.

“**Data Protection Laws**” means any regulation, law, or legislation relating to data protection and privacy that applies to a Party with respect to the Processing of Controller Personal Data pursuant to the Agreement, including without limitation, the European Data Protection Laws, United States’ federal and state laws such as the California Consumer Privacy Act (“CCPA”) and the Connecticut Consumer Data Protection Act (“CTDPA”), in each case as amended, repealed, consolidated or replaced from time to time and as applicable to each Party and the Controller Personal Data.

“Data Subject” means the individual who is the subject of the Personal Data and to whom Personal Data relates, directly or indirectly.

"Europe" means the European Union, the European Economic Area, and/or their member states, Switzerland, and the United Kingdom.

“European Data” means Controller Personal Data that is subject to the protection of European Data Protection Laws.

"European Data Protection Laws" means Data Protection Laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); (ii) applicable national implementations of the GDPR; (iii) UK General Data Protection Regulation ("UK GDPR"); and (iv) Swiss Federal Data Protection (FADP) of 19 June 1992 and its Ordinance; in each case, as may be amended, superseded or replaced.

“Instructions” means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action regarding Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available). The terms “Instruct,” “Instructed,” and “Instruction” will be construed accordingly.

“Personal Data” shall have the meaning as defined by the Data Protection Laws; unless otherwise defined by the Data Protection Laws or in case of conflict of interpretation, means any information about an individual, *inter alia*, an employee, customer, or potential customer of a Party, including, without limitation: (1) any information that directly or indirectly identifies, or relates to an individual; or (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information, as well as website tracking or analytic “cookie” information, usage and traffic data or profiles, meter location, or other usage data when combined with any of the information specified in (1). Personal Data includes, but is not limited to name, social security number, date and place of birth, mother’s maiden name, biometric records, personal electronic mail address, internet identification name, network, or internet password.

“Personal Data Breach” means breach of security leading to the unauthorized destruction, loss, alteration, disclosure of, or access to, Controller Personal Data. Personal Data Breach shall not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems. If the Data Protection Laws define “Personal Data Breach” or a similar term in a substantially different manner, the definition in the Data Protection Laws shall take precedence.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise, alignment or combination, restriction, or erasure of Personal Data. The terms “Process,” “Processes” and “Processed” will be construed accordingly.

“Processor” means Itron, to the extent that it Processes Personal Data on behalf of the Controller.

"Restricted Transfer" means (i) a transfer of Controller Personal Data from Controller to Processor; or (ii) an onward transfer of Controller Personal Data from Processor to a Sub-Processor or among two or more Sub-Processors, that would be prohibited by Data Protection Laws or by the terms of any applicable data transfer agreements addressing data transfer restrictions arising under Data Protection Laws in the absence of appropriate safeguards.

"Services" means the services and other activities to be supplied to or carried out by or on behalf of Processor for Controller pursuant to the Agreement.

"Standard Contractual Clauses" ("SCCs") means the standard contractual clauses for the transfer of personal data to processors approved pursuant to the European Commission's Decision (EU) 2021/914 of June 4, 2021, the text of which is available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

"Sub-Processor" means any processor engaged by Processor to assist in fulfilling Processor's obligations with respect to the AGREEMENT and who may Process Controller Personal Data.

"Technical and Organizational Measures" ("TOMs") means those security measures aimed at protecting personal data against Personal Data Breach.

Any capitalized term used in this DPA that is not otherwise defined in this DPA shall have the meaning ascribed to it in the Agreement.

TERMS

1. CONTROLLER OBLIGATIONS

- 1.1. Within the scope of the Agreement and in its use of Services, the Controller shall be responsible for complying with all requirements that apply to it under Data Protection Laws with respect to its own Processing of the Controller Personal Data and the Instructions it issues to Processor.
- 1.2. Controller acknowledges and agrees that it is solely responsible for: (i) the accuracy, quality, and legality of Controller Personal Data and the means by which Controller acquired Controller Personal Data; (ii) complying with all necessary transparency, lawfulness, and other requirements under Data Protection Laws that apply to its collection and use of the Controller Personal Data, including all obligations to provide notice and obtain consents and authorizations; (iii) ensuring it has the right to transfer Controller Personal Data to the Processor or provide the Processor with access to the Controller Personal Data for Processing in connection with the Services provided under the Agreement; and (iv) ensuring that its Instructions to Processor comply with applicable laws, including Data Protection Laws.
- 1.3. The parties agree that the Agreement, including this DPA, together with Controller's use of Processor's Services in accordance with the Agreement, constitute Controller's Instructions to Processor for the Processing of Controller Personal Data. Modifications and additions to these Instructions must be proposed in writing with at least seven days' prior notice to the receiving Party and must comply with all applicable requirements defined in the Agreement.
- 1.4. Controller agrees that the Technical and Organizational Measures ("TOMs") specified in Appendix B hereunder provides a reasonable level of security appropriate to the risks inherent to the Processor's Services and the nature of the Controller's Personal Data to be Processed.
- 1.5. Controller hereby consents to Processor's use and appointment of Sub-Processors, in consideration of Processor's compliance with section 2.1h hereunder.

2. PROCESSOR OBLIGATIONS

2.1. Processor shall:

- a) Process the Controller Personal Data only for the purpose of providing Services consistent with the Agreement and as otherwise instructed by Controller.
- b) Process the Controller Personal Data in accordance with Controller's documented Instructions; including transfer of personal data to a Third country or to an international organization unless required to do so by applicable law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless prohibited by that law. If Processor considers the Instructions given by the Controller to infringe upon any Data Protection Law or other applicable law, Processor shall promptly inform the Controller in writing, unless applicable laws or a substantial public interest prohibit such notice. Processor is entitled to suspend without penalty its execution of the Instruction in question while the Instruction remains in dispute, and to refuse to perform any evidently unlawful Instruction.
- c) Provide the Controller with contact information for its data protection advisor or Data Protection Officer ("DPO") pursuant to Data Protection Laws and, without undue delay, notify the Controller when such information changes.
- d) Notify the Controller promptly of any request to access the Controller Personal Data by a Data Subject or supervisory authority, unless prohibited by applicable law.
- e) Assist the Controller in responding to requests by Data Subjects regarding their rights under Data Protection Laws.
- f) Maintain records of the Processing of Controller Personal Data as required by Data Protection Laws.
- g) Ensure that Sub-Processors are bound, in substance, by obligations equivalent to the data protection obligations that are binding on the Processor under this DPA. The Processor has the Controller's general authorization for the engagement of Sub-Processors identified in Exhibit G-3 below accessible online at <https://www.itron.com/legal/privacy/contract-templates>. Processor will inform Controller of any intended changes of that list through the addition or replacement of Sub-Processors from time to time, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the concerned Sub-Processor(s). Controller may, within thirty (30) days after notice of the engagement of a new Sub-Processor, object to the use of new Sub-Processor if Controller reasonably believes that the new Sub-Processor raises a material risk of failing to comply with data protection law.
- h) Ensure that Processor's employees and other persons authorized to Process the Controller Personal Data (i) are bound by confidentiality, (ii) access Controller Personal Data only on a need-to-know basis, and (iii) are appropriately trained regarding confidentiality and Data Protection Laws.
- i) Assist the Controller in responding to requests from supervisory authorities.

- j) Assist the Controller in complying with its obligations under Data Protection Laws, including assisting Controller in conducting data protection impact assessments when required.
 - k) Processor shall remain fully responsible to Controller for the performance of the Sub-Processor's obligations in accordance with its contract with the Processor. When requested in writing by Controller, Processor shall provide information necessary to demonstrate Processor's and Sub-Processor's compliance with the Data Protection Laws
 - l) Allow for and contribute to (1) mandatory audits carried out by competent data protection authorities under Data Protection Laws and (2) audits conducted and paid for by the Controller, subject to the terms of this subsection (l). Controller agrees that Processor satisfies its obligation under Section 2.2(l)(2) by providing summaries of third-party audits undertaken by Processor relating to ISO 27001, SOC 2 Type 1, SOC 2 Type 2, and SSAE 16/SSAE 18 standards, which will be provided to Controller if requested by Controller no more frequently than once per 12-month period. Controller may further request an on-site audit for the 6-month period immediately following a Personal Data Breach caused by Processor's failure to implement appropriate security measures. If connection with any on-site audit permitted by this section, Controller may choose to conduct the audit by itself or mandate an independent auditor. Such on-site audits shall be carried out on pre-agreed dates, during normal business hours and no more than once per year, unless required more frequently by a supervisory authority pursuant to Data Protection Laws. On-site audits may include access to the physical facilities of the Processor provided there is no unnecessary disturbance to business operations. The Parties shall make the information referred to in this clause, including the results of any audits, available to the competent supervisory authority/ies pursuant to applicable law. Any information discovered pursuant to an on-site audit will be the confidential information of Processor. Controller will ensure that it or any independent auditor it engages complies with all Processor policies and procedures if accessing Processor's physical facilities.
- 2.2. To the extent this DPA is subject to European Data Protection Laws, Controller grants Processor general authorization to conduct, any transfer or Restricted Transfer of Controller Personal Data to a third country or an international organization outside the European Economic Area, including where such transfer is made to a Sub-Processor. Such transfer will be conducted pursuant to the EU-U.S. Data Privacy Framework, and/or the UK Extension to the EU-U.S. Data Privacy Framework, (or such successor framework that is approved or otherwise validated by relevant data protection authorities ("Framework")) while such Framework is in effect and during which time Processor maintains an active certification for such Framework that allows it to rely on the Framework for such transfers. If the Framework is determined to be invalid by relevant data protection authorities, the Parties agree that such Restricted Transfers shall be conducted pursuant to the SCCs as follows:
- a) If there is any conflict between this DPA or the Agreement and SCCs, the SCCs will prevail;
 - b) Controller will be referred to as the "Data Exporter" and Vendor will be referred to as the "Data Importer" in the SCCs with relevant company name, contact person details, address details, and activities related to the transferred Controller Personal Data from this DPA and the Agreement being used accordingly;
 - c) Details in Exhibit G-1 of this DPA will be used to complete Annex I and III of the SCCs;

d) Details in Section 2.1 and Exhibit G-2 of this DPA will be used to complete Annex II of the SCCs;

e) For the purposes of the Standard Contractual Clauses:

- i. The Parties agree to retain Clause 7;
- ii. The Parties select option 1 in Clause 9 and agree on fifteen (15) business days as the notice period for additions or replacements of new Subprocessors;
- iii. The optional language in Class 11(a) is omitted;
- iv. Clause 13(a) reads as follows “The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority,” which shall be as specified in Exhibit G-1;
- v. The Parties select option 1 of Clause 17 and specify the jurisdiction stated in the Agreement; and
- vi. The Parties select the courts of forum consistent with the jurisdiction within the Agreement.

f) In addition to the SCCs, the Parties agree that any Controller Personal Data subject to the UK GDPR that is a Restricted Transfer will be subject to the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses Version B1.0, in force 21 March 2022 (the “UK Addendum”) (the text of which is available at <https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf>). The UK Addendum will be deemed executed by the Parties as of the effective date of this DPA, and the information in Exhibit G-1 and Exhibit G-2 to this DPA and this Section 2.2 will be used to fill out the relevant sections of the UK Addendum.

- g) The Parties agree to complete the Standard Contractual Clauses as follows for Controller Personal Data subject to the FADP that is a Restricted Transfer: (i) the Parties agree to abide by the GDPR standard in relation to all Processing of Controller Personal Data that is governed by the FADP; (ii) the term ‘Member State’ in the Standard Contractual Clauses will not be interpreted to exclude Data Subjects who habitually reside in Switzerland from initiating legal proceedings in Switzerland in accordance with Clause 18© of the SCCs and until the revised FADP enters into force, the SCCs will also protect the data of legal entities in Switzerland; and (iii) references to the ‘GDPR’ in the SCCs will be understood as references to the FADP insofar as the transfer of Controller Personal Data is subject to the FADP.

2.3. To the extent any Controller Personal Data is subject to the CCPA or the CTDPA,

- a) Processor will not:
 - i. Process such Controller Personal Data other than for the specific purpose of performing the Services for Controller in accordance with this DPA;
 - ii. Process such Controller Personal Data for a commercial purpose other than as necessary to provide the Services to Controller;
 - iii. “sell” or “share” (each as defined by CCPA or CTDPA) such Controller Personal Data;
 - iv. Process such Controller Personal Data outside of the direct business relationship between Processor and Controller; or
 - v. combine such Controller Personal Data with any other Personal Data or information Processor collects (directly or via any third party) other than as expressly permitted under the CCPA or CTDPA for service providers;
- b) Processor will comply with all obligations applicable to it as a “service provider” under the CCPA or CTDPA and provide the same level of privacy protection as is required by the CCPA or CTDPA ;
- c) Processor will promptly notify Controller if Processor determines it can no longer meet its obligations under this Section 2.3; and
- d) Processor permits Controller, upon notice to Processor, to take reasonable and appropriate steps to stop and remediate unauthorized use of Controller Personal Data

2.4. Processor agrees to notify the Controller of any Personal Data Breach without undue delay after its discovery, as follows:

- a) The notification will include a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of potentially affected Data Subjects and the categories and approximate number of personal data records concerned, the name and contact details of the Processor's data protection advisor or DPO from whom information can be obtained, the likely consequences of the Personal Data Breach, the measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.
- b) If it is not possible to provide the information at the same time, Processor may provide information in phases.
- c) Processor shall assist Controller with notifying the supervisory authorities and the Data Subjects concerned, if required by Data Protection Laws, and
 - (i) the Processor shall promptly take all commercially reasonable measures it deems necessary to secure the data and mitigate possible adverse effects on the affected Data Subject(s);
 - (ii) the Processor shall inform the Controller of the measures it has taken; and
 - (iii) the Processor shall not notify the competent data protection authorities or affected Data Subject(s) on behalf of the Controller unless instructed to do so by the Controller.

2.5. Processor shall inform the Controller if there is a substantial change in the security procedures described in the TOMs.

2.6. Processor acknowledges that Controller is subject to the laws of the United States Virgin Islands and agrees to comply with all applicable local data protection and breach notification laws, including but not limited to 14 V.I.C. § 2208. Specifically, Processor shall notify Controller without unreasonable delay following the discovery of any breach of security involving unencrypted personal information of a Virgin Islands resident and shall assist Controller in meeting its obligations under Virgin Islands law, including those relating to the timing, content, and method of notification. This obligation is in addition to, and not in limitation of, any other applicable breach notification or data security requirements under this DPA or applicable law.

3. LIABILITY AND INDEMNIFICATION

Controller and Processor shall be liable to Data Subjects only to the extent mandated by Data Protection Laws or the Agreement. The Parties shall coordinate regarding any liability claims. If a Data Subject is addressing a claim against the Controller due to Processor's Processing of Controller Personal Data under this DPA and/or the Agreement, Processor shall indemnify the Controller against any costs, claims and damages arising out of Processor's non-compliance with this DPA or the relevant terms of the Agreement, Data Protection Laws or any other applicable Instructions, rules or policies relating to Processing of Controller Personal Data under the Agreement. Any such liability for Processor under this DPA shall be subject to the requirements for statutory liability under the applicable legislation and to the limitation and cap of liability set forth in the provisions of the Agreement.

The Controller will indemnify Processor and hold Processor harmless against all claims, actions, third party claims, losses, damages, and expenses incurred by Processor and arising directly or indirectly from or in connection with Controller's breach of this DPA and/or Data Protection Laws.

4. TERM AND TERMINATION

- 4.1. This DPA shall continue to be in effect until terminated pursuant to Section 4.2 or 4.3 below.
- 4.2. This DPA shall automatically terminate upon any termination or expiration of the Agreement, provided no separate assignments for Processing of Controller Personal Data independent of the Agreement have been concluded by and between the Parties. In case such separate assignments have been made, this DPA shall automatically terminate when the Agreement and all such separate assignments have terminated or expired.
- 4.3. Controller shall properly notify and grant Processor a forty-five (45) day period to remedy any suspected or actual breach of this DPA before invoking any action relating to early termination pursuant to the Agreement.
- 4.4. Termination or expiration of this DPA shall not discharge Processor from its confidentiality or other obligations pursuant to the Agreement and Data Protection Laws. Processor agrees, even after the termination or expiry of this DPA, to perform its legal obligations as Processor and to assist the Controller in performance of its legal obligations pursuant to Data Protection Laws, and to demonstrate compliance with the Data Protection Laws.
- 4.5. Upon termination of the Agreement or cessation of Processor's provision of Services, Processor shall send all data to a new processor or to the Controller as instructed by the Controller in writing. Thereafter, Processor shall destroy all other copies of the data unless otherwise instructed in writing by Controller or Data Protection Laws or other applicable laws a retention or Data Protection Laws or as required under applicable law.

5. UPDATES TO THIS DPA

5.1. Changes to this Addendum. Itron may change the provisions of the DPA if the change:

- b) reflects a change in the name or form of a legal entity;
- c) is required to comply with applicable law, regulation, a court order, or guidance issued by a governmental regulator or agency; or
- d) does not:
 - (i) result in a degradation of the overall security of the Services;
 - (ii) expand the scope of, or remove any restrictions on Itron's Processing of Customer Personal Data; and
 - (iii) otherwise have a material adverse impact on Controller's rights under the DPA, as reasonably determined by Itron.

5.2. Notification of Changes. Any changes Itron makes to this DPA pursuant to Section 5.1, will be reflected at our webpage here <https://www.itron.com/legal/privacy/contract-templates>. We encourage you to periodically review our webpage for the current version of this addendum.

ATTACHMENT G EXHIBIT G-1

Description of Processing

This Exhibit G-1 includes certain details of the Processing of Controller Personal Data.

Nature, purpose, and legal basis of Processing

Processor will Process Controller Personal Data as necessary to provide the Services pursuant to the Agreement, as further specified in any additional Purchase Orders, and as further Instructed by Controller in its use of the Services and may be subject to the following Processing activities, including but not limited to:

- Storage, hosting, and other Processing necessary to provide, maintain and improve the Services provided to Controller; and/or disclosure in accordance with the Agreement and this DPA, and/or as required by applicable laws.
- Customer Support

The legal basis for the transfer is the performance of the Agreement between the Parties.

Duration of Processing

Subject to Section 4.5 of this DPA, Processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

Frequency of Transfer

Ongoing

Categories of Data Subjects

Processor may have access to or receive from Controller or its agents, employees, advisors, contractors, or subcontractors Controller Personal Data which may include, but is not limited to the following categories of Data Subjects who are natural persons:

- Controller's business partners, vendors, and subcontractors of Controller;
- Employees or contact persons of Controller's end customers, partners, vendors, and Subcontractors;
- Employees, agents, advisors, contractors, and freelancers of Controller; and
- Controller's users authorized by Controller to use the services of Processor.

Types of Personal Data

Processor may have access to or receive from Controller or its agents, employees, advisors, contractors, or subcontractors Controller Personal Data which may include, but is not limited to the following categories:

- First and last name
- Title and Position
- Employer
- Contact information (email, phone, physical address)
- Account number
- ID Card number
- Equipment-specific information, including serial number and location.
- Consumption data

The parties do not anticipate the transfer of special categories of data or sensitive data.

Retention Period

The Controller Personal Data will be retained for the period of time needed for Processor to complete its obligations under the Agreement.

Competent Supervisory Authority:

The competent supervisory authority shall be the data protection authority where Controller is established. If Controller does not have an establishment in Europe, the competent supervisory authority shall be the data protection authority of one of the member states in which the Data Subjects whose Personal Data is Processed by Processor under the DPA. Except that: (a) the Swiss Federal Data Protection and Information Commission will act as the competent supervisory authority for transferred Personal Data subject to the FADP; and (b) the Information Commissioner's Office will be the competent supervisory authority for transferred Personal Data subject to the UK GDPR.

Table 4 of the UK Addendum:

Ending This Addendum When the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19:
	<input type="checkbox"/> Data Importer
	<input checked="" type="checkbox"/> Data Exporter
	<input type="checkbox"/> Neither Party

ATTACHMENT G
EXHIBIT G-2

Technical and Organizational Measures

This document outlines the technical and organizational security measures (“TOMs”) and controls implemented by Itron, Inc., its subsidiaries, and affiliated companies, “Itron” designed to protect Controller Personal Data.

Itron will maintain these or similar controls for data protection but reserves the right to make changes to these controls, so long as such changes do not materially weaken the controls or data security for the data Itron is responsible for across its various services and processes.

1. Information Security Governance
 - A. Itron maintains dedicated staff responsible for the development, implementation, and maintenance of Itron’s information security program.
 - B. Itron implements a set of policies for information security that are defined, approved by management, published, and communicated to personnel and relevant external parties.
 - C. Itron regularly reviews the policies for information security at planned intervals at least annually or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.
 - D. Itron implements audit and risk assessment procedures for the purposes of periodic review and assessment of risks at least annually to the Itron organization, monitoring and maintaining compliance with Itron policies and procedures, and reporting the condition of its information security and compliance to executive management.
 - E. Itron values the confidentiality of information and adheres to requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of such information are identified, regularly reviewed, documented, and enforced.
2. Information Security Training
 - A. Itron requires that new personnel complete security awareness training as part of the onboarding process.
 - B. Itron ensures that all employees of the organization and, where relevant, contractors receive regular, but at least annually, and appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
 - C. Itron regularly tests all employees and contractors of the organization, who have access to external emails, to detect and report malicious and phishing emails.
 - D. Employees and, where relevant, contractors complete regular, but at least annually, data protection and security training as relevant for their job function.
3. Data Protection
 - A. Itron engages in information assets classification to classify information in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.
 - B. Itron maintains identified, documented, and implemented acceptable use standards of information, the assets associated with the information, and information processing facilities.
 - C. Itron storage media is disposed of securely, ensuring data is rendered unrecoverable, when no longer required or prior to reuse, using formal procedures.
 - D. Itron has an established access control policy which is documented and reviewed based on business and information security requirements and limits access to extent required and necessary. The controls include:
 - Access controls for workspaces,
 - Access controls for IT systems including IT Systems being managed for the benefit of Customer, and

- Access controls for apps and data, including Customer data.
 - E. Itron actively engages in security controls that include logical segregation of data, restricted (e.g., role-based) access, monitoring, and where applicable and required, utilization of industry-standard encryption technologies.
 - F. Itron actively engages in data security controls for requesting, approving, revoking, and revalidating user access to systems and applications. Only personnel with clear business need will be provided with access to systems and applications with Personal Data.
 - G. Itron has a designated Global Privacy Officer.
 - H. Employees receive work instructions and guidelines regarding confidentiality and data protection as relevant for their job, to ensure compliant handling of Personal Data.
 - I. Sub-Processors and service providers are carefully selected and are bound to Itron's Processing restrictions. Incidents are notified to Itron without undue delay.
4. Technical Security Controls
- A. Itron implements detection, prevention, and recovery controls to protect against malware, combined with appropriate user awareness.
 - B. Itron regularly scans on monthly basis to detect technical vulnerabilities and apply appropriate mitigation actions to reduce the associate risk and exposure to such vulnerabilities.
 - C. Itron regularly patches and updates, in a timely manner, systems and applications based on the severity of identified vulnerabilities.
 - D. Itron monitors various information sources to ensure knowledge of and response to relevant threats, including industry specific sources.
 - E. Itron networks are managed and controlled to protect information in systems and applications and segregates groups of information services, users, and information systems as appropriate. This includes separation of networks for processing, administration and supporting services in case of high protection requirements.
 - F. Itron applies appropriate protections at the network edge, including stateful firewalls to filter attacks.
 - G. Itron ensures information involved in electronic messaging will be appropriately protected, including encryption as required.
 - H. Itron information involved in application services passing over public networks is actively protected from fraudulent activity and unauthorized visibility. No Customer information shall pass over public networks unless encrypted.
 - I. Itron implements password controls designed to manage and control password strength and usage. Itron prohibits users from sharing passwords and accounts.
 - J. Itron ensures that all remote access to internal networks, systems and applications are protected by multi-factor authentication.
 - K. Itron protects internal devices utilizing security controls including automated locking screen saver, antivirus software, firewall software, hard disk encryption and appropriate patch levels.
5. Physical Security
- A. Itron ensures physical security perimeters are defined and used to protect areas that contain either sensitive or critical systems and information.
 - B. Itron ensures secure areas are protected by appropriate entry controls to ensure that only authorized personnel, based on job role, are allowed access.
 - C. Itron ensures that non-authorized personnel are logged and escorted in areas that contain either sensitive or critical systems and information.
 - D. Itron ensures that secure areas containing sensitive or critical systems and information monitor for environmental hazards such as heat, fire, and water damage.
6. Secure Software Development Lifecycle

- A. Itron ensures principles, including Privacy by Design, for engineering secure systems are established, documented, maintained, and applied to any information system implementation efforts.
 - B. Itron ensures testing of security functionality is carried out during development and that acceptance testing programs and related criteria are established for new information systems, upgrades, and new versions.
 - C. Itron ensures test data does not include production data unless fully anonymized and is selected carefully, protected, and controlled.
 - D. Itron ensures that changes to systems and applications undergo an appropriate change management procedure designed to test, approve, and monitor changes to the Itron environment.
- 7. Logging and Monitoring
 - A. Itron maintains a central repository of security records and ensures collection of such records from all relevant information technology infrastructure. These logs will be maintained for a minimum of one year.
 - B. Itron ensures all user access activities, including successful and failed logins, are maintained in the central repository.
 - C. Itron ensures information security logs are actively monitored and events are reported through appropriate management channels as quickly as possible and will ensure information security incidents are responded to in accordance with the documented procedures.
 - D. As to systems managed by Itron for Customer, Customer shall, upon request, have access to such security records and access activities and logs as applicable. For the avoidance of doubt, this access does not include automated, electronic transfer of records to Customer, which may be available as a separate project at an additional cost.
- 8. Incident Response
 - A. Itron has an established, documented Information security event response program. Events are reported through appropriate management channels and reported to Customer as to systems managed by Itron for Customer as quickly as possible.
 - B. Itron ensures information security incidents, including privacy related incidents, are responded to in accordance with documented procedures and compliance requirements. Itron will follow documented incident response processes, including notification to the impacted parties without undue delay. Business continuity and disaster recovery services are available to Customer at an additional cost or as are outlined in other sections of the Order Document.
 - C. Itron ensures the Incident Response process includes a detailed investigation to identify root cause of the event, incident response plan and to document and incorporate lessons learned.
- 9. Disaster Recovery and Business Continuity
 - A. Itron determines its requirements for information security and the continuity of information security management in adverse situations, e.g., during a crisis or disaster.
 - B. Itron documents and maintains procedures to maintain business continuity and recover from a disaster.
 - C. Itron maintains a backup policy to define the organization's requirements for backup of information, software, and systems.

ATTACHMENT G EXHIBIT G-3

List of Sub-Processors

Sub-Processors that may be involved with providing the Services are described below.

For more information about Itron's Partners, please visit <https://www.itron.com/na/partners-landing-page/partner-directory>.

<i>Processor's Affiliates</i>		
Name of Sub-Processor	Location of Sub-Processor	Purpose
Allmess GmbH	Germany	Itron entity used to contract with a specific customer base
Itron Australasia Pty Ltd	Australia	Itron entity used to contract with customers in Australia
Itron Austria GmbH	Austria	Itron entity used to contract with customers in Austria
Itron Belgium SA	Belgium	Itron entity used to contract with customers in Belgium
Itron Canada, Inc.	Canada	Itron entity used to contract with customers in Canada
Itron Czech Republic s.r.o.	Czech Republic	Itron entity used to contract with customers in Czech Republic
Itron France S. A. S	France	Itron entity used to contract with customers in France
Itron Global LLC dba Itron Global Trading		Itron entity used to contract with customers outside NAM where a local in-country Itron entity is not available
Itron International LLC	Luxembourg	Itron entity used to contract with customers outside NAM if an in-country Itron entity is unavailable
Itron GmbH	Germany	Itron entity used to contract with customers in Germany, unless customer is from Zahler or Allmess region
Itron India Private Limited	India	Itron entity used to contract with customers in India
Itron Italia SpA	Italy	Itron entity used to contract with customers in Italy
Itron Japan Co., Ltd.	Japan	Itron entity used to contract with customers in Japan
Itron Labs KFT	Hungary	Itron entity
Itron Management Services Ireland, Limited	Ireland	Itron entity
Itron Metering Solutions (Suzhou) Co., Ltd.	China	Itron entity

<i>Processor's Affiliates</i>		
Name of Sub-Processor	Location of Sub-Processor	Purpose
Itron Metering Solutions Co. Ltd. fka Silver Spring Networks	Thailand	Itron entity used to contract with customers in Thailand
Itron Metering Solutions UK Ltd.	UK	Itron entity used to contract with customers in UK
Itron Metering Systems Co., Ltd.	China	Itron entity used to contract with customers in China
Itron Metering Systems Singapore Pte Ltd (fka Actaris Singapore Pte. Ltd) (fka Kimford Pte Ltd)	Singapore	Itron entity used to contract with customers in Singapore
Itron Nederland B. V.	Netherlands	Itron entity used to contract with customers in the Netherlands
Itron Networked Solutions, Inc.	United States	Itron entity
Itron New Zealand Limited	New Zealand	Itron entity used to contract with customers in New Zealand
Itron Polska SP Zoo	Poland	Itron entity used to contract with customers in Poland
Itron Sistemas de Medicao Lda.	Portugal	Itron entity used to contract with customers in Portugal
Itron Spain SLU	Spain	Itron entity used to contract with customers in Spain
Itron Sweden AB	Sweden	Itron entity used to contract with customers in Sweden
Itron Ukraine	Ukraine	Itron entity used to contract with customers in Ukraine
Itron Zähler & Systemtechnik GmbH	Germany	Itron entity used to contract with specific customer base
Metertek Sdn. Bhd. (fka Metertek Schlumberger Sdn. Bhd. 2001- 1119)	Malaysia	Itron entity used to contract with customers in Malaysia
PT Mecoindo	Indonesia	Itron entity used to contract with customers in Indonesia
Temetra Limited	Ireland	Itron entity

<i>Processor's Third-Party Sub-Processors</i>		
Name	Location of Sub-Processor	Purpose
ABB Tropos Wireless Communications Systems	Switzerland	Vendor
Accenture LLP	United States	Vendor
Aclara Technologies LLC	United States	Vendor
Acuity Brands, Inc.	United States	Vendor
Advanced Control Systems (ACS)	United States	Vendor

Processor's Third-Party Sub-Processors

Name	Location of Sub-Processor	Purpose
Aeroqual, Inc.	New Zealand	Vendor
Amazon Web Services, Inc.		Hosting of Data
Ameresco, Inc.	United States	Vendor
APANET	Poland	Vendor
AT&T	United States	Vendor
Athena Computer Power Corp	United States	Vendor
AutoGrid	United States	Vendor
Aztech Associates Inc.	Canada	Vendor
Beckwith Electric Co.	United States	Vendor
Beonic	Australia	Vendor
Bidgely	United States	Vendor
Bouygues Energies & Services	France	Vendor
Capgemini	France	Vendor
Carrier	United States	Vendor
CEIVA Energy	United States	Vendor
Choice	Australia	Vendor
CIMCON	United States	Vendor
Cisco	United States	Vendor
Citelum	France	Vendor
Citylone	France	Vendor
Cleverciti	Germany	Vendor
ClipperCreek	United States	Vendor
CNIguard	United States	Vendor
Communitings	Belgium	Vendor
Comtrade Digital Services	United States	Vendor
Connect Intwine	United States	Vendor
ConnectDER	United States	Vendor
Corporate Systems Engineering	United States	Vendor
Cyient	India	Vendor
Dynamic Digital Displays	United States	Vendor
Databuoy	United States	Vendor
DC Systems	United States	Vendor
Diaglogic	Canada	Vendor
Digi International Inc.	United States	Vendor
Guangdong Rongwen Energy Technology Group	China	Vendor
Dresser Natural Gas Solutions	United States	Vendor
Dropcountr	United States	Vendor
D-tect Systems	United States	Vendor
DVI	United States	Vendor
Eagle Research Corporation	United States	Vendor
Eaton	United States	Vendor
EC Infosystems	United States	Vendor
Ecobee	Canada	Vendor

Processor's Third-Party Sub-Processors

Name	Location of Sub-Processor	Purpose
EDMI Limited	Singapore	Vendor
Efacec Power Solutions	Portugal	Vendor
Efergy	China	Vendor
Elektron	Sweden	Vendor
Eletra Energy Solutions	Brazil	Vendor
Elichens	France	Vendor
Emerson	United States	Vendor
Energate	Canada	Vendor
Tecnologias EOS Medical	Mexico	Vendor
Esri	United States	Vendor
Estuate	United States	Vendor
Exceleron	United States	Vendor
Exegin Technologies Limited	Canada	Vendor
Fairway Electrical Services Inc.	Canada	Vendor
G&W Electric	United States	Vendor
Genus Power Infrastructures Limited	India	Vendor
Gerard Professional Solutions Pty Ltd (GPS)	Australia	Vendor
Google	United States	Vendor
Graybar	United States	Vendor
GreenBe Software	Australia	Vendor
Grid4C	United States	Vendor
Harris Utilities	Canada	Vendor
HD Electric Company	United States	Vendor
Holophane	United States	Vendor
Honeywell	United States	Vendor
Horstmann	Germany	Vendor
Houston Radar	United States	Vendor
I20	United Kingdom	Vendor
IBM	United States	Vendor
Infosys	India	Vendor
Instrumentation Technologies		Vendor
iUS Technologies	United States	Vendor
Jetlun Corporation	United States	Vendor
Kamstrup	Denmark	Vendor
Kitu Systems	United States	Vendor
Landis Gyr	Switzerland	Vendor
LED Roadway Lighting	Canada	Vendor
LG Electronics USA, Inc.	United States	Vendor
LightSmart Energy Consulting, LLC	United States	Vendor
Lockheed Martin	United States	Vendor
Lumnex	United States	Vendor
Master Meter	United States	Vendor
Metrix	New Zealand	Vendor

Processor's Third-Party Sub-Processors

Name	Location of Sub-Processor	Purpose
Microsoft	United States	Vendor
Mirai	Japan	Vendor
MMB Research	Canada	Vendor
Nansen	Brazil	Vendor
New Cosmos Electric Co., Ltd.	Japan	Vendor
Nighthawk Total Control	United States	Vendor
NovaTech	United States	Vendor
OMRON Electronic Components	United States	Vendor
Operational Technology Solutions (OTS)	United States	Vendor
Oracle	United States	Vendor
OSIsoft	United States	Vendor
OSRAM	Germany	Vendor
OWON Technology Inc.	China	Vendor
PayGo Electric	Kenya	Vendor
Power Systems Integrity, Inc.	United States	Vendor
Powerley	United States	Vendor
Qinetiq	United Kingdom	Vendor
Qualcomm	United States	Vendor
Rainforest Automation	United States	Vendor
RouteSmart Technologies	United States	Vendor
S&C Electric Company	United States	Vendor
SafePlug Smart Energy	United States	Vendor
Secure		Vendor
SELC	United States	Vendor
Sentient Energy, Inc.	United States	Vendor
Siemens Corporation	Germany	Vendor
Sierra Wireless	Canada	Vendor
Smart Energy Water	Canada	Vendor
Smartenit	United States	Vendor
SmartGridCIS	United States	Vendor
Sonnen	Germany	Vendor
SPIE	United States	Vendor
Sprint	United States	Vendor
Sumeru Verde P. L.	India	Vendor
Sunrise Technologies, Inc.	United States	Vendor
Tantalus	United States	Vendor
TCAM Technology Pte Ltd	Singapore	Vendor
Telematics Wireless	United States	Vendor
Telescada	United States	Vendor
Tendril	United States	Vendor
Terrago	United States	Vendor
ThinkEco	United States	Vendor
Trilliant	United States	Vendor

Processor's Third-Party Sub-Processors

Name	Location of Sub-Processor	Purpose
Universal Devices	United States	Vendor
Urbancontrol	United Kingdom	Vendor
Utilidata	United States	Vendor
US3	United States	Vendor
V2COM	United States	Vendor
Varentec	United States	Vendor
Verizon	United States	Vendor
WaterSmart	United States	Vendor
Whirlpool	United States	Vendor
Wireless Glue	United States	Vendor
ZH Technologies International	United States	Vendor

ATTACHMENT H TO THE ORDER DOCUMENT

Network Coverage Addendum

1. Additional Definitions.

The following defined terms are in addition to those defined in the Agreement General Terms and Conditions of the Agreement and the Additional Definitions in this Section 1 of the Equipment Addendum for this Attachment H.

Alternative Backhaul means alternative CUSTOMER provided network connectivity between Itron data center and Network Devices which is approved by both parties. For example, fiber backhaul, point to point wireless or satellite communications provided by CUSTOMER and approved by SUPPLIER would be Alternative Backhaul.

Alternative Network Devices means new types of Network Devices which have been or may be developed by SUPPLIER to provide additional alternatives to APs, Socket-APs and Relays. For example, a new type of AP that can be mounted on a streetlight socket which enables installation in areas where no poles are present.

Deployment Period is defined in the Equipment Addendum Attachment C.

Network Device is defined in the Equipment Addendum Attachment C.

Network Coverage Commitment is defined in Section X of this Attachment H.

No Meter Left Behind Commitment is defined in Section 10 of this Attachment H.

Optimized Endpoint means an endpoint that has been subject to Optimization.

Read State means meters identified in UIQ as “Active,” “Inactive” or “Disconnected”.

Total VIWAPA Population means the ~57,000 electric meters as provided during the RFP and any additional devices installed during the deployment period that are within 200 linear meters of a meter in the RFP list.

The following defined terms are duplicated from the Statement of Work (Attachment B) for purposes of this Attachment H.

AMI	Advanced Metering Infrastructure
Commissioned AMI Meter	Means AMI meters that have been installed and communicating on the AMI network at 95% or better and providing read data for 5 (five) consecutive days. Once a device is commissioned it remains in the state until Optimization is complete. At that point it becomes Provisioned and Optimized as defined in this document.
Commissioned Network Device	Means any Access Point, Relay or Socket Access Point (SAP) that has been installed and Active for 5 (five) consecutive days as evidenced by the Device Ping Report from AMM. Once a device is commissioned it remains in the state.

Enhanced Field Network Design (EFND)	Means SUPPLIER's modifications to the Initial Field Network Design that will be performed after SUPPLIER performs Site Surveys of the field network locations and conditions.
Final Field Network Design (FFND)	Means SUPPLIER's final "as built" inventory of Network Devices at the end of deployment and Optimization.
Initial Field Network Design (IFND)	Update to the Preliminary Network Design using the most recent AUTHORITY information. Site Surveys are performed to validate the suitability and feasibility of building the network according to the IFND. Results of site surveys are incorporated in the EFND.
Optimization	An iterative process in which the performance of the network within a defined region is evaluated against Service Levels upon which the Parties have agreed. Optimization will be performed in an Optimization Area after Meter installation reaches a to be agreed upon saturation percentage and all Network Devices required by the Enhanced Field Network Design for the area have been installed and validated. At the conclusion of optimization, Service Points that meet SLAs are marked "Optimized". Optimization may result in the placement of additional, or relocation of existing, Network Devices in the area, to meet Service Level Agreements. Service Points that do not meet Service Levels will not be considered "Optimized".
Optimization Area	Means a contiguous area agreed to by SUPPLIER and the AUTHORITY used for Optimization.
Wide Area Network (WAN)	A geographically dispersed communications network with a specific user group; that is, any network that links across metropolitan, regional, or national boundaries. A WAN may be privately owned or rented, but the term usually implies the inclusion of public (shared user) networks.

2. Warrants and Representations

SUPPLIER represents that it also has enough network capacity built into the network to support up to 60,000 electric meters assuming that any additional electric meters ("Not Provided Locations") are within the coverage area of the "Initial Network Design" i.e. latitude and longitude coordinate pairs within this Initial Network Design Coverage Area, regardless of the physical installation location (e.g. inside, outside, etc.), and upon completion of the system acceptance test, will have an average daily communication performance of 99.5% or better and an average near real time data collection and delivery interval reads every 15 minutes of 95% (collectively, the "Performance Requirements"). SUPPLIER warrants that the Total VIWAPA Population is included in the Initial Network Design Coverage Area.

SUPPLIER agrees that the Final Field Network Design of surveyed and installed Network Devices will provide the necessary RF communications to meet the Performance Requirements for the Total VIWAPA Population. Provided that any electric meter strictly within the boundaries of the Initial Network Design Coverage Area, SUPPLIER warrants that the Final Field Network Design will meet the Performance Requirements for the Total VIWAPA Population proposed for the AMI solution. If additional Network Devices or Remote Antenna are required to meet the Performance Requirements during the deployment period, VIWAPA will purchase and pay SUPPLIER to install such Network Devices or Remote Antenna, up to 5% of the total cost of the Network Equipment. This 5% limit shall be calculated using total cost of network devices and installation. SUPPLIER shall provide all survey services for additional devices at no charge.

3. Data Set and IFND.

CUSTOMER will provide SUPPLIER with a revised data set of meter locations and mounting asset locations (“**Data Set**”) that will be used as the basis for SUPPLIER to develop an IFND. The Data Set will be in WGS84 decimal degree latitude / longitude format. If CUSTOMER does not provide a complete Data Set for at least 95% of the meter locations to SUPPLIER prior to the Order Document Effective Date, the Network Coverage Commitment shall cover 100% of Meter service point locations latitude/longitude data set provided by CUSTOMER as part of the RFP.

- a. SUPPLIER will provide CUSTOMER with an IFND that lists:
 - i. Number of APs and Socket APs for initial deployment and their intended deployment location.
 - ii. Number of Relays for initial deployment and their intended deployment location.
- b. The IFND as described above will contain fewer devices than the device counts provided as Equipment quantities per Section 4 below, because SUPPLIER will hold off some number of devices to be used to provide:
 - i. Coverage in areas where the IFND did not successfully cover some meters.
 - ii. Redundancy in areas where meters can only register with a single AP.
 - iii. Load balance for APs and Socket APs with an excessive number of meters which cannot be read according to the performance SLAs.
 - iv. Coverage to “hard-to-hear” locations (e.g., below grade meters, meter cabinets, in building meter rooms) subject to the exclusions below.

4. Equipment Quantities.

SUPPLIER will provide CUSTOMER the expected total count of Network Devices required to meet the Network Coverage Commitment in Section 6 of this Attachment H based on the Data Set provided by CUSTOMER. Network Devices will be quantified by device type (i.e., Access Points, Socket Aps and Relays) that are expected to be required during the Deployment Period to provide 100% coverage for the Electric Meters provided in the data Set.

5. Network Equipment Budget.

The total cost of the expected Network Devices (8 ethernet AP, 59 Cellular AP, 66 Relays and 21 Socket AP) will be used to determine the Network Equipment Budget. Note that this is the total cost of Network Devices that are expected to be required by the end of the project to provide 100% coverage to the meters in the Total VIWAPA Population. The Network Equipment budget does not include the 5% cap if additional equipment is required.

- c. SUPPLIER will select the most cost-effective Network Device to meet the Network Coverage Commitment. In general, SUPPLIER shall select from the available Network Device options the device(s) that minimizes total cost (hardware, mounting, and operational). If CUSTOMER directs SUPPLIER to use a different Network Device, the difference in cost (including installation) between CUSTOMER’s chosen solution and the SUPPLIER proposed solution will not count towards the Network Equipment Budget.
- d. the difference in cost (including installation) between the proposed solution and the solution chosen by CUSTOMER will be the responsibility of CUSTOMER and are excluded from the Network Equipment Budget calculation.
- e. If the total Equipment cost of the FFND exceeds the Network Equipment Budget plus 5%, SUPPLIER will bear the cost of additional Equipment as needed to meet the Network Coverage Commitment. For clarity:
 - i. Cost of equipment will be covered by SUPPLIER

- ii. Cost of device installation will be covered by SUPPLIER
- iii. Cost of Make Ready work will be covered by CUSTOMER
- iv. Cost of pole installation will be covered by CUSTOMER

6. Geocoded Locations.

The IFND will only include AMI electric meters within 200 linear meters of AMI electric meters provided with geocoded locations. SUPPLIER expects meters without a geocoded location to be able to connect without additional Equipment if such deployed meters fall within the footprint of the geocoded meters. If an endpoint without an initial geocoded location is excluded from the Coverage Commitment in this Attachment H and additional Network Devices are required, the additional Network Devices deployed to connect these endpoints will not count towards the Network Equipment Budget.

7. Network Coverage Commitment

The FFND provided to CUSTOMER will provide RF coverage to 100% of Meters provided for in the IFND (“**Network Coverage Commitment**”), calculated as the number of Meters able to communicate with AMI system within the Performance Requirements over the total number of Meters deployed under the SOW and not excluded by Section 7.1 of this Attachment H. A meter’s ability to communicate with AMI system will be considered confirmed once a Meter transitions to a Commissioned State (as defined above). The Network Coverage Commitment shall be measured one time only after Optimization is completed. Should the Network Coverage Commitment not be met at the conclusion of Final Optimization, SUPPLIER will remediate the network and retest. All remediations will be subject to the terms in Section 5 of this Addendum H.

For areas requiring additional Network Devices above the Network Equipment Budget, SUPPLIER shall use the best option to provide mesh coverage, e.g., AP’s, Socket APs, Relays, Photocell APs, or Alternative Network Device while still meeting the Performance Requirements. For example, Alternative Network Device could be a new type of AP that can be mounted on a streetlight socket which enables installation in areas where no poles are present. As another example, mounting a socket AP on a pole or another alternative mounting option if available. Any make ready work needed for these additional devices would be subject to the terms set forth in Section 5 of this addendum H.

8. Exclusions.

The Network Coverage Commitment does not apply to Meters that are not Commissioned due to:

- A lack of wide area network (WAN) backhaul connectivity for the associated Network Device unless such lack can be addressed by use of Alternative Network Equipment or Alternative Backhaul. Network Device may be added to the design to provide an alternative method to cover downstream meters from lack of WAN coverage affected Network Device. However, excessive chains of relays (4 or more) linking meter clusters back to areas of active mesh or backhaul are excluded.
- Inability to mount Network Device antenna (except for Socket APs) a minimum of 7m above ground level (AGL) due to local ordinance preventing it;
- Radio frequency opt-out customers leading to material gaps in mesh coverage (cases would be mutually agreed upon by the Parties, acting reasonably and in good faith, during the Deployment Period);
- Illegal radio frequency interference from transmitters operating within the solution frequency spectrum of 902 to 928 MHz that cannot be resolved by CUSTOMER;

- Failure of CUSTOMER to perform required preparatory work, or CUSTOMER pays SUPPLIER to perform required preparatory work, associated with remediating hard to reach indoor or below grade meter locations requiring external antennas (such as drilling, conduit runs, building / customer approvals); This applies to individual Meters located inside built structures (meter rooms, cabinets, etc) or below grade that do not match the meters that were identified by CUSTOMER as being built inside structures or below grade. This exclusion is based on SUPPLIER and CUSTOMER periodic review and mutual agreement.
- If applicable, discontinuance by CUSTOMER of Maintenance and Support Services or failure of CUSTOMER to implement updates provided by SUPPLIER;
- Note that design and Network Device counts are scoped assuming CUSTOMER provided location data was reasonably accurate and only covers Meters in the Total VIWAPA Population provided as an input to the IFND. Meters added outside of the designed coverage area as reviewed and mutually agreed to are not covered by this SOW.

9. Network Equipment Deployment

SUPPLIER will deploy the Network Equipment specified in the EFND in a geographical area at least 4 weeks before meter installation begins.

These devices will be imported into UIQ by SUPPLIER so that SUPPLIER's NOC monitoring can commence and the health of the communications to these devices be assessed prior to meter installation. Devices that do not meet the NOC performance metrics will be ticketed and where appropriate assigned to SUPPLIER for field investigation (e.g., vandalism, downed pole).

Any installed network device that fails to Commission will be investigated and remediated by the SUPPLIER prior to scheduled meter installations in the affected deployment area.

10. Meter Deployment and No Meter Left Behind

SUPPLIER will provide AUTHORITY every month with the expected meter deployment for the following month. The deployment plan will be as specific as possible, for example by endpoint, Service Point ID, latitude, longitude, and expected deployment date.

SUPPLIER will follow the installation plan and on a timely basis load location information into UIQ. SUPPLIER's installer should be directed to prioritize deployment in the following manner:

- Deploy only in areas where Network Infrastructure has been deployed.
- Deploy from Network Devices outward if possible.
- Deploy in a manner to saturate geographic areas under network infrastructure as opposed to completing long routes that extend in a single direction (as an example).
- Address skipped meters in a timely manner.

SUPPLIER will monitor the deployment for those meters in:

- "Installed" state (where the location information has been loaded in UIQ but the meter has not made contact with the mesh and/or the back office).
- "Unreachable" state (meters that were in "Active" "Inactive" or "Disconnected" which have not communicated for 24-48 hours.
- "Discovered" state (where meter has made contact with the mesh and no location information has been loaded in UIQ within 72 hours of installation).

SUPPLIER will perform an analysis of the possible reasons for meters being in the above states leveraging the deployment schedule as well as metrics exposed by UIQ, the SUPPLIER reporting server, field notes, and other sources.

- For “Installed” meters, SUPPLIER will examine those meters which have been in that state for longer than 5 days.
- For “Unreachable” meters, SUPPLIER will investigate “lack of RF coverage” of devices that are not communicating normally, SUPPLIER will lead the troubleshooting focusing on the endpoints.
- For “Discovered” meters, SUPPLIER will review installation logs to verify that the meter was installed and the installation records was provided to CUSTOMER’s CIS for processing. SUPPLIER will correct any errors in the installation and repost the installation to CUSTOMER’s CIS. Where the meter was properly installed and reported to VIWAPA’s CIS, SUPPLIER will notify CUSTOMER for investigation and correction of the update to UIQ.

Upon this analysis SUPPLIER will:

- Identify areas which require additional meter deployment, or relocation of network device, of network devices or installation of remote antenna and will schedule these to be deployed within a mutually agreed timeline. SUPPLIER will provide for all the field services without cost to the CUSTOMER. If the Equipment costs for this additional deployment exceeds the Network Budget of Equipment identified in the IFND, SUPPLIER will provide such Equipment without cost to the CUSTOMER.
- Identify areas which require additional deployment where meters are still thinly deployed and additional meter deployment will strengthen the RF mesh and provide coverage and schedule these meters to be deployed within a mutually agreed timeline.
- Perform a field visit to examine local conditions and propose a solution such as installing an external antenna, installing an additional Network Device (e.g., an isolated meter room, meters below grade) or other solution.
- Perform a field visit to ensure meters are deployed, recorded and/or operating correctly.
- Determine that the meter(s) are located in an area where the designed AP or Socket-AP does not have cellular backhaul of sufficient quality to maintain consistent communications. SUPPLIER will identify alternative locations for mounting APs or Socket-APs and connect to the affected meters with Relays subject to the exclusions detailed in Section 7.1 of this document. If these solutions do not suffice CUSTOMER and SUPPLIER will identify alternate backhaul solutions (e.g., fiber AP, satellite AP, etc) and CUSTOMER will provide Alternate Backhaul..

SUPPLIER and CUSTOMER will hold a weekly meeting to review the counts, aging, and status of meters in these states as well as solution options, and logistics of field visits and remediation.

SUPPLIER will ensure that any deployed meter becomes Commissioned per the below prescribed timelines. SUPPLIER will attempt to remediate 100% of deployed meters that fail to become Commissioned prior to the 3rd read date from installation.

- >80% of meters should Commission before 1st read date and VIWAPA will manually read up to 20% of installed meters on route without penalty.
- >95% of meters should Commission before 2nd read date and VIWAPA will manually read up to 5% of installed meters on route without penalty.
- >99.5% of meters should Commission before 3rd read date and VIWAPA will manually read up to 0.5% of installed meters on route without penalty

Upon meters meeting the minimum performance threshold for 5 consecutive days, they will be Commissioned and eligible for the Pre-Optimization SLAs.

For any meter which fails to Commission within the timelines above and requires VIWAPA to manually read more meters than allowed, SUPPLIER will credit CUSTOMER \$75 per month for each manual read above the threshold until such meter becomes Commissioned.

11. Meter Saturation and Optimization

SUPPLIER will conduct Optimization for St. John before IDA approximately every 3 months for St. Croix and St. Thomas (including Water and Hassel islands). No area will be optimized where less than 98% of installed meters are Commissioned.

This process examines a variety of metrics such as meter loading on Access Points, meters without a secondary Access Point, and meters that do not read consistently in the 15-minute read jobs.

The process might recommend the addition of Access Points, Socket-APs, or other suitable mitigation methods to remediate RF coverage, redundancy, or AP loading issues.

At the end of each Optimization, the analysis and the list of Service Point IDs that are considered Optimized will be reviewed with CUSTOMER. Any meter within an Optimization Area which fails to be Optimized will be identified and will have a mitigation plan such that such meter will be Optimized with the next planned Optimization.

Upon being marked Optimized, these meters will be extracted from the list of meters under “Pre-Optimization” SLAs and will be added to the list of Optimized meters used to compute the SaaS SLAs.

Thereafter, if a meter in an Optimized Service Point ID is replaced by another meter, the new meter installed in the same Service Point is automatically considered for the SLA calculation. Any new Service Point added to an Optimized Area after SAT will be Optimized periodically (no less than every 6 months) when SUPPLIER is notified that such Service Point has been added, a new AMI meter has been installed and such meter becomes Commissioned.

SUPPLIER will complete Optimization for all Commissioned meters prior to beginning SAT.

ATTACHMENT I TO THE ORDER DOCUMENT

Security Addendum

This Security Addendum (“**Security Addendum**”) supplements and forms part of the Agreement and shall be applied to the Order Document. Any capitalized term used but not defined in this Security Addendum shall have the meaning given in the Agreement and/or in the Order Document. If there is a conflict or inconsistency between this Security Addendum and any other part of the Agreement or Order Document, the term that affords greater protection for Customer Data will control.

1. **Information Security Program.** Itron shall maintain a comprehensive documented security program that is based on industry standard security frameworks, including NIST 800-53 and ISO 27001 (the “Security Program”). Pursuant to the Security Program, Itron shall maintain administrative, physical, and technical security measures to protect the Service Offerings, Maintenance and Support Services, and the security and confidentiality of Customer’s Data.
2. **Network, Application, and Infrastructure.** Itron shall maintain information security controls to protect Customer Data that is received, processed, or stored by Itron or its cloud providers in connection with Customer’s use of the Service Offerings and Maintenance and Support Services. These controls will be designed to ensure the confidentiality, integrity, and availability of Customer Data, the Itron network, and information technology assets used by Itron to deliver Service Offerings. They will include technical and organizational measures and other safeguards to (i) secure Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access; (ii) mitigate reasonably foreseeable external and internal risks to the Itron network and Service Offerings, including risks of unauthorized access to facilities, systems, and information assets storing or processing Customer Data; and (iii) enable Itron and Customer to comply with their respective obligations under applicable data privacy and data protection laws and regulations (collectively, “**Data Protection Laws**”). All controls will be governed by written policies and procedures under Itron’s Security Program. All policies and procedures will be reviewed and approved annually by appropriate management-level Itron Personnel.
3. **Specific Technical Controls.** Itron will employ defenses such as encryption, log monitoring, endpoint protection, and firewalls to protect the Itron network, Service Offerings and Customer Data, including the following, consistent with industry standards:
 - a. Encryption of Customer Data processed and stored in the Service Offerings (including Customer user passwords) leveraging at least AES 256-bit encryption for data at rest and in transit.
 - b. Strong authentication in compliance with industry standards, such as multi factor authentication; strong complex passwords, or certificate based authentication. Passwords shall not be stored or transmitted in a human readable format.
 - c. Network-based vulnerability scanning for Itron network and Service Offerings, with regular application of patches and security updates to the Itron network, Service Offerings, and associated information assets;
 - d. Intrusion prevention and intrusion detection systems (IPS/IDS), with secure storage and regular monitoring of logs;
 - e. Firewalls to control traffic to and from the Itron network and Service Offerings, with network perimeter monitoring, automated notification of suspicious activity, and rule set validation reviewed annually;

- f. Secure by design, defense in depth approach to development and maintenance of Itron Software incorporated in Service Offerings in accordance with a defined software development life cycle framework, including regular code review using application security and code analysis tools;
 - g. External and internal vulnerability testing for the Service Offerings, including annual penetration testing;
 - h. Hardening practices to protect the Itron network and Service Offerings from vulnerabilities;
 - i. Remediation of vulnerabilities with appropriate timelines based on severity.
- 4. **User Access Management.** Itron will ensure that all access to the Itron network and Service Offerings is restricted to authorized individuals and Itron will enable Customer to restrict Customer users' access to the Service Offerings. These restrictions will be supported by authentication controls, including enforcement of complex password rules, consistent with industry standards, and account lockouts in all environments as well as procedures such as encryption, masking, and expiration rules to maintain security of passwords.
- 5. **Network and Data Separation.** Itron will maintain logical or physical separation between the Itron network and the cloud provider environments where Customer Data is processed and stored. Itron's application and database security frameworks will ensure that Customer Data is logically separated from Itron data and third-party data. Itron will also maintain logical separation of production and non-production environments within the Itron network and within the Service Offerings.
- 6. **Physical and Environmental Controls.** Itron will employ industry standard measures to manage physical security, mitigate security risks, and prevent and detect unauthorized access to Itron facilities, systems, and assets. Itron will equip its corporate buildings with physical access control systems such as access badge readers and monitoring, and registration systems for visitors that restrict access and track information about individuals. Itron will also implement and regularly test fire suppression measures and environmental controls, where required for systems performance. To protect Customer Data while stored or processed using Services Offerings, Itron will ensure cloud providers maintain physical security for their data centers using state-of-the-art controls and equipment to protect their data centers from threats and unauthorized access. Itron will also ensure cloud providers enforce other controls designed to ensure redundant operations during environmental incidents, including continuity of electrical power, fire suppression, and humidity and temperature controls.
- 7. **Change Management.** Itron will implement and follow formal change management processes that require software and infrastructure changes affecting the Service Offerings or the Itron network to be formally documented, tested, reviewed, and approved prior to migration to the production environment. Infrastructure and software changes are managed and tracked using work management systems. The change management processes are appropriately segregated, and access to migrate changes to production is restricted to authorized Itron Personnel. This clause requires Customer to maintain non-production environments as part of their deployment. Should Customer elect to remove non-production environments, this paragraph is void.
- 8. **Vendor Management.** Itron will implement and follow formal vendor risk management processes that require documented risk assessment, with scrutiny and mitigation commensurate with the level of risk. Itron's agreements with cloud providers and other key vendors involved in provisioning the

Service Offerings or the Itron network will include information security and protection commitments, including where appropriate requirements to conduct, maintain, and provide on request evidence of third-party audit and/or certification according to the Service Organization Controls (SOC) reporting framework, ISO/IEC, or other similar framework or standard.

9. Breach Notification and Incident Response.

(a) Notification. If Itron becomes aware of a breach of security or a potential breach of security, impacting Customer Data or systems Itron manages to deliver Service Offerings, leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data (a “Security Incident”), Itron shall immediately notify Customer as follows:

Itron shall IMMEDIATELY CALL, regardless of the day or time the Customer’s ITS Support Center at (860) 665 - 4357 (24x7); ALSO julius.aubain@viwapa.vi, communications@viwapa.vi with details of the Security Incident.

(b) Initial Notification. The initial notification shall include the date and time of the Security Incident occurrence (or the approximate date and time of the occurrence if the actual date and time of the occurrence is not precisely known) and a detailed summary of the facts and circumstances of the Security Incident, to the extent that they are known to Itron, including a description of (a) why the Security Incident occurred (e.g., a precise description of the reason for the system failure), (b) the amount of Customer Data known or reasonably believed to have been disclosed without authorization, and (c) the measures being taken to address and remedy the occurrence to prevent the same or a similar event from occurring in the future.

(c) Notice Updates. Itron shall provide written updates of the Security Incident notice to Customer addressing any new facts and circumstances learned after the initial written notice is provided and shall provide such updates within a reasonable time after learning of those new facts and circumstances. Itron shall cooperate with Customer to determine the risk posed by the Security Incident, including providing additional information regarding the Security Incident upon request from Customer to the extent such information is available to Itron and to the extent the Security Incident is caused by Itron’s errors or omissions.

(d) Incident Response Plan. Itron shall have in place a written Response Plan with requirements and procedures to respond to and address Security Incidents caused by Itron’s errors or omissions (“Response Plan”), including measures to notify Customer, mitigate impacts of Security Incidents and procedures and actions to be taken to assess Security Incident and mitigate the risk of occurrence of such Security Incidents in the future, as described below. Upon request, Itron shall provide the Response Plan to Customer or make its Response Plan accessible for review. The Response Plan and its implementation shall follow best practices that at a minimum are consistent with the contingency planning requirements of NIST Special Publication 800-61 Rev. 2, NIST Special Publication 800-53 Rev. 4, CP-1 through CP-13 and the incident response requirements of NIST Special Publication 800-53 Rev. 4, IR-1 through IR-10 as those standards may be amended.

Itron will, for Security Incidents on Itron network, the Service Offerings or affecting Customer Data under Itron’s responsibility, promptly take all reasonable steps to contain or mitigate the effects of the Security Incident and implement appropriate controls to prevent its recurrence. Itron will comply with applicable law in its response to the Security Incident. Itron will be responsible for any Security Incident response and investigation and will cooperate with and assist Customer, to the extent such cooperation does not impact Itron’s confidentiality obligations to other parties, including other Itron customers, and its representatives, law enforcement, and any data protection authority or other appropriate governmental or regulatory body in connection with Itron’s response and investigation.

- 10. Audit.** Itron undergoes external audits and has completed a SOC 1 Type II attestation, and a SOC 2 Type II attestation. These reports are available upon request and Itron will provide the SOC 2 Report to CUSTOMER within 30 days of execution of Contract and upon completion of the annual audit. Itron will also provide written responses to all reasonable requests made by Customer for information relating to Itron's processing of Customer Data, including responses to information and security audit questionnaires submitted by Customer and that are necessary to confirm Itron's compliance with this Security Addendum, provided Customer shall not exercise this right more than once per calendar year or when Customer is expressly requested or required to provide this information to a protection authority. Notwithstanding the foregoing, Customer may provide Itron with thirty (30) days' prior written notice requesting that a third party conduct an audit of Itron's facilities, equipment, documents and electronic data relating to the processing of Customer Data under the Agreement ("Audit"), provided that: (a) the Audit shall be conducted at Customer's expense; (b) the parties shall mutually agree upon the scope, timing and duration of the Audit; (c) the Audit shall not unreasonably impact Itron's regular operations; and (d) such Audit shall not occur more than once per calendar year. Customer acknowledges that any audit report, written responses, or Audit described in this section shall be subject to the confidentiality provisions of the Agreement.
- 11. Third-Party Data Security Assessments.** Prior to engaging with a new third party that may have access to Customer Data, Itron shall evaluate such third party's data security standards using a qualification risk assessment.
- 12. Bill of Materials.** Upon request by Customer, Itron shall provide a software bill of materials in an industry standard format that identifies the major components and versions used in the software that is incorporated into the Service Offerings. Itron will make available a statement of verification that the hardware components used are not sourced from embargoed countries or US Trade Restricted Suppliers.

ATTACHMENT J TO THE ORDER DOCUMENT

Software Addendum

1 Relationship to General Terms and Conditions

This Addendum is subject to the Amended General Terms and Conditions and applicable Order Documents.

2 Additional Definitions

The following defined terms are in addition to those defined in the General Terms and Conditions:

Authorized Installations means installations of Itron Software only on one production environment, one disaster recovery environment and one test environment on Customer premises.

Authorized User means an employee or contractor of Customer who Customer permits to access and use the Itron Software and/or Documentation pursuant to Customer's license hereunder.

Endpoints, for the purposes of this Addendum, means an electric meter, battery-powered device, or any other device that Itron has agreed to monitor as part of a Service Offering which Endpoints are identified in the Order Document or Pricing Summary.

Itron Software means the machine readable (object code) version of computer programs listed in a pricing summary to be licensed to Customer under this Agreement that are developed by or on behalf of Itron.

License Term means the duration of the Itron Software license granted by Itron to Customer under this Addendum; unless expressly specified otherwise, the License Term for each Itron Software product is perpetual.

Software means Itron Software and Third-Party Software, including any updates provided to Customer pursuant to this Agreement.

Software Warranty Period means a period of ninety (90) days from the date of delivery, unless another Software Warranty Period is expressly stated in the applicable Order Document.

Third-Party Software means the machine readable (object code) version of computer programs listed on an Order Document to be licensed to Customer by a third-party and that are not developed by or on Itron's behalf.

3 Ordering Software

Customer shall order Software by executing the Contract and issuing Notice to Proceed to Itron in accordance with this Agreement.

4 Delivery and Invoicing

Itron will promptly deliver Software electronically, on tangible media, or by other means following Itron's acceptance of the applicable Purchase Order. Risk of loss of any tangible media on which the Software is delivered will pass to Customer on delivery to carrier. Itron will invoice Customer for Fees due for Software upon the date of delivery.

5 Itron Software License

Subject to and conditioned on Customer's payment of all applicable Fees and compliance with this Agreement, Itron hereby grants to Customer a non-exclusive, non-sublicensable, and non-transferable license during the License Term to use Authorized Installations of Itron Software and related

Documentation for Customer's internal business purposes solely: (i) within the Territory; (ii) in connection with the number of Endpoints or other devices specified on the applicable Order Document; and (iii) in accordance with any other restrictions specified on the applicable Order Document.

6 Third-Party Software

All Third-Party Software and related documentation is separately licensed to Customer by the applicable third-party, and Customer's rights and responsibilities with respect to such software or documentation shall be governed in accordance with the third-party licensor's applicable software license. If Customer chooses to order Third-Party Software, Customer shall enter into or accept one or more separate third-party agreements as part of the ordering, fulfillment, installation and/or download processes for such Third-Party Software. Customer has the right to accept or reject license terms for Third-Party Software.

7 Documentation

Itron will make its Documentation, including but not limited to release notes, user manuals, existing defects, available via download and provide Customer with download instructions.

8 Itron Software License Restrictions.

Customer shall not use the Itron Software or Documentation for any purpose beyond the scope of the licensed granted in this Addendum. Without limiting the foregoing, Customer will not at any time, directly or indirectly: (i) modify or create any derivative works from Itron Software, (ii) distribute the Itron Software, (iii) include or combine Itron Software with any software, equipment, or hardware other than as expressly authorized in writing by Itron, (iv) use Itron Software to provide services to third-parties, (v) reverse assemble, decompile, reverse engineer Itron Software or otherwise attempt to derive its source code except to the extent that such restriction is prohibited by applicable law, (vi) export Itron Software out of the Territory, (vii) use any Itron Software to create products or services that compete with any of Itron's products or services, or (viii) copy Itron Software except to make one machine readable copy for disaster recovery or archival purposes. Customer's breach of these restrictions or use of Itron Software or Documentation other than as licensed hereunder shall constitute a material breach of this Agreement and shall result in revocation and immediate termination of all rights and licenses granted under this Agreement. Revocation does not preclude Itron from pursuing any legal and equitable remedies for Customer's breach of these restrictions. Customer is responsible and liable for all uses of Itron Software and Documentation resulting from access provided by Customer, directly or indirectly, whether such access or use is permitted or in violation of this Agreement. Without limiting the generality of the foregoing, Customer is responsible for all acts and omissions of Authorized Users, and any act or omission by an Authorized User that would constitute a breach of this Agreement if taken by Customer will be deemed a breach of this Agreement by Customer. Customer shall take reasonable efforts to make all Authorized Users aware of this Agreement's provisions as applicable to such Authorized User's use of the Itron Software, and shall cause Authorized Users to comply with such provisions.

If an Itron Software license is acquired under a United States government contract, Customer acknowledges that such Itron Software (including updates thereto) and associated Documentation are "Commercial Computer Software" as defined in 48 C.F.R. 12.212 of the Federal Acquisition Regulations (FAR) and in 48 C.F.R. 227.7014(a)(i) of the Department of Defense Federal Acquisition Regulations Supplement (DFARS), and are provided with only the commercial rights and subject to the restrictions described in this Agreement.

Customer shall not use the Itron Software or Documentation for any purpose beyond the scope of the licensed granted in this Addendum. Without limiting the foregoing, Customer will not at any time, directly or indirectly: (i) modify or create any derivative works from Itron Software, (ii) distribute the Itron Software, (iii) include or combine Itron Software with any software, equipment, or hardware other than as expressly authorized in writing by Itron, (iv) use Itron Software to provide services to third-parties, (v)

reverse assemble, decompile, reverse engineer Itron Software or otherwise attempt to derive its source code except to the extent that such restriction is prohibited by applicable law, (vi) export Itron Software out of the Territory, (vii) use any Itron Software to create products or services that compete with any of Itron's products or services, or (viii) copy Itron Software except to make one machine readable copy for disaster recovery or archival purposes. Customer's breach of these restrictions or use of Itron Software or Documentation other than as licensed hereunder shall constitute a material breach of this Agreement and shall result in revocation and immediate termination of all rights and licenses granted under this Agreement. Revocation does not preclude Itron from pursuing any legal and equitable remedies for Customer's breach of these restrictions. Customer is responsible and liable for all uses of Itron Software and Documentation resulting from access provided by Customer, directly or indirectly, whether such access or use is permitted or in violation of this Agreement. Without limiting the generality of the foregoing, Customer is responsible for all acts and omissions of Authorized Users, and any act or omission by an Authorized User that would constitute a breach of this Agreement if taken by Customer will be deemed a breach of this Agreement by Customer. Customer shall take reasonable efforts to make all Authorized Users aware of this Agreement's provisions as applicable to such Authorized User's use of the Itron Software, and shall cause Authorized Users to comply with such provisions.

To the extent directive 2009/24/EC on the legal protection of computer programs or similar legislation or regulations (collectively, the "directives") may provide Customer the right to decompile Itron Software in order to obtain information necessary to achieve the interoperability of an independently created computer program, prior to exercising any such possible rights under the directives, Customer agrees to: (a) first notify Itron of Customer's good faith belief that information necessary to achieve the interoperability of an independently created computer program is not otherwise available and that decompilation is indispensable within the meaning of the directives; and (b) provide Itron with a reasonable amount of time to respond to Customer regarding the foregoing assertions.

Customer shall not use the Itron Software or Documentation for any purpose beyond the scope of the licensed granted in this Addendum. Without limiting the foregoing, Customer will not at any time, directly or indirectly: (i) modify or create any derivative works from Itron Software, (ii) distribute the Itron Software, (iii) include or combine Itron Software with any software, equipment, or hardware other than as expressly authorized in writing by Itron, (iv) use Itron Software to provide services to third-parties, (v) reverse assemble, decompile, reverse engineer Itron Software or otherwise attempt to derive its source code except to the extent that such restriction is prohibited by applicable law, (vi) export Itron Software out of the Territory, (vii) use any Itron Software to create products or services that compete with any of Itron's products or services, or (viii) copy Itron Software except to make one machine readable copy for disaster recovery or archival purposes. Customer's breach of these restrictions or use of Itron Software or Documentation other than as licensed hereunder shall constitute a material breach of this Agreement and shall result in revocation and immediate termination of all rights and licenses granted under this Agreement. Revocation does not preclude Itron from pursuing any legal and equitable remedies for Customer's breach of these restrictions. Customer is responsible and liable for all uses of Itron Software and Documentation resulting from access provided by Customer, directly or indirectly, whether such access or use is permitted or in violation of this Agreement. Without limiting the generality of the foregoing, Customer is responsible for all acts and omissions of Authorized Users, and any act or omission by an Authorized User that would constitute a breach of this Agreement if taken by Customer will be deemed a breach of this Agreement by Customer. Customer shall take reasonable efforts to make all Authorized Users aware of this Agreement's provisions as applicable to such Authorized User's use of the Itron Software and shall cause Authorized Users to comply with such provisions.

9 Limited Itron Software Warranty

For the Software Warranty Period, Itron warrants solely to Customer that the Itron Software will substantially conform in all material respects to the applicable Itron published specifications. As Customer's

sole and exclusive remedy for any breach of this warranty, Itron will, at its option, during the applicable Software Warranty Period, repair or replace non-conforming Itron Software to substantially conform to the foregoing warranty, provided that Itron will have no obligation to repair or replace any non-conforming Itron Software if this Agreement or applicable Order Document has terminated or expired. The foregoing warranty does not apply to non-conformities in Itron Software due to: (i) modifications not made or approved by Itron in writing; (ii) Customer's or any third party's negligence or intentional acts; (iii) misuse or abuse, including the failure to use or install Itron Software in accordance with the Documentation; (iv) incorrect data, or data entry or output, as applicable, by Customer or a third party; (v) use with third party software, hardware or firmware not provided or authorized by Itron in writing; (vi) a Force Majeure event; or (vii) viruses or security vulnerabilities introduced into the Itron Software or Customer's systems through no fault of Itron. After the applicable Software Warranty Period, any Itron Software errors and any maintenance updates will be addressed under the Maintenance and Support Services Addendum.

10 Effect of Expiration or Termination for Cause

Upon termination of an Itron Software license for cause or expiration of a License Term, whichever occurs first, Customer shall immediately discontinue use of the applicable Itron Software and related Documentation, and Customer will destroy or return to Itron any and all copies. Upon Itron's request, Customer will confirm in writing that Customer has destroyed or has returned Itron Software and related Documentation in compliance with this section. This requirement applies to copies in all forms, partial and complete, in all types of media and computer memory, and whether or not modified or merged into other files or materials. Termination of an Itron Software license for cause will not restrict Itron from pursuing any other remedies available to it, including injunctive relief, nor will it relieve Customer of its obligation to pay all fees that accrued prior to such termination.

11 Third-Party Software Warranty

Itron is not the owner of Third-Party Software and makes no representations or warranties whatsoever, directly or indirectly, express or implied, as to the durability, and fitness for use, merchantability, condition, quality, performance or non-infringement of any Third-Party Software. Third-Party Software shall be subject to any warranties provided by the Third-Party Software provider. Itron will pass through to Customer, or make commercially reasonable efforts to enforce on Customer's behalf, any warranties and remedies received from the Third Party Software provider.

12 License Use Verification & Audit

12.1 License Use Verification

Customer represents and warrants the Itron Software will be used by Customer in compliance with the licenses granted in this Addendum. Promptly upon Itron's written request, and no more than once annually, Customer must furnish Itron with a letter signed by an officer of Customer, verifying such compliance, and confirming the number, identification, type and location of Endpoints and other devices being managed by Customer using Itron Software.

12.2 Audit

Itron has the right to audit Customer records to verify the number of Endpoints and other devices being managed by Customer using Itron Software and otherwise confirm Customer's compliance with license restrictions and Fee obligations of this Agreement. Itron must provide Customer with at least thirty (30) days prior written notice of the audit. The audit must be conducted during Customer's normal business hours at a mutually agreeable location. Itron's right to conduct an audit under this Section is limited to one (1) time per year, unless Itron has reason to believe that Customer is out of compliance with the license restrictions and Fee obligations of this Agreement. Itron has the right to use an independent auditor to conduct the audit. The audit shall be at Itron's sole cost and expense, unless the audit identifies a deficiency in Fees or other amounts owed or reimbursable by Customer during the audited period that is greater than

five percent (5%) of the total amounts payable by Customer – in which case Customer must reimburse Itron for all reasonable costs of the audit. All amounts found to be owed by Customer pursuant to an audit will be payable within thirty (30) days after receipt of invoice from Itron.

13 Survival

The following sections of this Addendum shall survive termination or expiration of this Agreement or any Order Document or Statement of Work: 1 (Relationship to General Terms and Conditions), 2 (Additional Definitions), 4 (Delivery and Invoicing), 5 (Itron Software License) except to the extent applicable license rights expire or are terminated in accordance with this Agreement, 6 (Third-Party Software), 8 (Itron Software License Restrictions), 9 (Limited Itron Software Warranty), 10 (Effect of Termination for Cause), 11 (Third-Party Software Warranty), 12 (License Use Verification & Audit) and 13 (Survival).