

MASTER SERVICES AND SOFTWARE AS A SERVICE AGREEMENT

This Master Services and Software as a Service Agreement (“**Agreement**”), dated as of April 10, 2020 (the “**Effective Date**”) sets forth the terms under which Convergent Solutions, Inc. (“**Exiger**”) will provide Citizens Property Insurance Corporation (“**Customer**”) with access to and use of certain software-as-a-service offering(s) and other services identified in applicable Statements of Work.

- A. Exiger focuses on technology-enabled solutions which we call “DDIQ” (our machine-learning due diligence product) and Insight 3PM (our third party management and risk rating platform) (collectively, “**Hosted Services**”), and Exiger’s affiliates provide a wide range of other services, including manual due diligence reports, investigations, best-in-class consulting on financial crimes compliance and related issues, independent monitorships and other integrity monitoring services (collectively, together with Hosted Services, the “**Services**”).
- B. Under this Agreement, Exiger is available to provide Hosted Services, and Exiger’s affiliates are available to provide other Services under one or more Statements of Work; alternatively, and solely in Customer’s discretion, Exiger is available to provide all Services offered by Exiger and its affiliates through its inter-company services arrangements, in order to facilitate Customer’s onboarding process.

1. DEFINITIONS

1.1 “**Affiliates**” means any entity that directly or indirectly, through one or more intermediaries, controls, or is controlled by, or is under common control with a party to this Agreement, by way of majority voting equity ownership.

1.2 “**Agreement**” means these terms and conditions, together with any and all Statements of Work referencing these terms and conditions, the Schedules attached hereto and any other exhibits, addendum or appendices thereto, whether attached or incorporated by reference. Attached hereto are Schedule A (Citizen’s Standard Terms and Conditions); Schedule B (Data Processing Exhibit); and Schedule C (the Scope of Work).

1.3 “**Customer Data**” means all electronic data or information submitted by Customer or its Affiliates to and stored by the Hosted Service or elsewhere by Exiger.

1.4 “**EU Data Protection Laws**” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom, applicable to the processing of Personal Data under the Agreement, including (where applicable) the GDPR.

1.5 “**Exiger Materials**” means the Service software, specifications, documentation and Exiger information technology systems and any and all other information, data, databases, documents, materials, works and other content, devices, methods, processes, hardware, software and other technologies and inventions, including any deliverables, technical or functional descriptions, requirements, plans or reports, that are provided or used by Exiger or any subcontractor in connection with the Services or otherwise comprise or relate to the Services or Exiger information technology systems, and any modifications, improvements or enhancements.

1.6 “**GDPR**” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of the natural persons with regard to the processing of personal data and on the free movement of such data (known as the General Data Protection Regulation).

1.7 “Law” means any statute, law, ordinance, regulation, rule, code, order, constitution, treaty, common law, judgment, decree or other requirement of any federal, state, local or foreign government or political subdivision thereof, or any arbitrator, court or tribunal of competent jurisdiction.

1.8 “Losses” means any and all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees and the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers.

1.9 “Person” means an individual, corporation, partnership, joint venture, limited liability entity, governmental authority, unincorporated organization, trust, association or other entity.

1.10 “Personal Data” means all data which is defined as ‘Personal Data’ in the EU Data Protection Laws and to which EU Data Protection Laws apply and which is provided by Customer to Exiger. The rights and responsibilities between the Parties with respect to the processing of such data is defined in Schedule B.

1.11 “Process” means to take any action or perform any operation or set of operations that the Hosted Services are capable of taking or performing on any data, information or other content, including to collect, receive, input, upload, download, record, reproduce, store, organize, compile, combine, log, catalog, cross-reference, manage, maintain, copy, adapt, alter, translate or make other derivative works or improvements, process, retrieve, output, consult, use, perform, display, disseminate, transmit, submit, post, transfer, disclose or otherwise provide or make available, or block, erase or destroy. **“Processing”** and **“Processed”** have correlative meanings.

1.12 “Intellectual Property Rights” means any and all registered and unregistered rights granted, applied for or otherwise now or hereafter in existence under or related to any patent, copyright, trademark, trade secret, database protection or other intellectual property rights laws, and all similar or equivalent rights or forms of protection, in any part of the world.

1.13 “Resultant Data” means generic statistical information pertaining to Customer’s use of the Services that is used for the routine operation of the Services (e.g. when and for how long a User logs into the Service).

1.14 “Service Software” means the Exiger software application or applications and any third-party or other software, and all new versions, updates, revisions, improvements and modifications of the foregoing, that Exiger provides access to and use of as part of the Services.

1.15 “Statement of Work” or **“SOW”** means the statement of work attached hereto as Schedule C (**“Statement of Work No. 1”**) or any statement of work that may be mutually executed by the parties from time to time. Each SOW will be subject to the terms and conditions of this Agreement.

1.16 “Users” means individuals who are authorized by Customer to use the Hosted Service pursuant to the terms and conditions of this Agreement and the applicable SOW.

2. GENERAL TERMS OF ACCESS TO THE HOSTED SERVICE

2.1 Services and License.

2.1.1 Services. During the Term, Exiger shall provide to Customer and its Users the Services described in an applicable SOW and this Agreement, including to host, manage, operate and maintain the

Hosted Services in substantial conformity with the Service Level Agreement and any other Services requested by Customer. At Customer's election, it may enter into SOW with any Affiliates of Exiger which will be governed by this Agreement.

2.1.2 License. Subject to the terms of this Agreement and payment of the applicable fees, Exiger grants to Customer during the Term a limited, non-transferable, revocable, and non-exclusive license to permit Users to use the Hosted Service in accordance with the use parameters, pricing, and payment terms described in this Agreement and the applicable SOW and in accordance with the terms and conditions of this Agreement.

2.1.3 Changes. Exiger reserves the right, in its sole discretion, to make any changes to the Services and Exiger Materials that it deems necessary or useful to: (a) maintain or enhance (i) the quality or delivery of Exiger's services to its customers, (ii) the competitive strength of or market for Exiger's services or (iii) the Services' cost efficiency or performance; or (b) to comply with applicable Law. Exiger will not make changes that materially degrade the performance of any of the Services without Customer's written consent. Customer agrees to cooperate with Exiger in effectuating the timely implementation of such changes, including acceptance of new versions of Hosted Services.

2.1.4 Systems Management. Exiger has and will retain sole control over the operation, provision, maintenance and management of the Services and Exiger Materials, including the: (i) Exiger systems; (ii) location(s) where any of the Services are performed; (iii) selection, deployment, modification and replacement of the Service Software; and (iv) performance of support services and Service maintenance, upgrades, corrections and repairs.

2.1.5 Subcontractors. Exiger may from time to time in its discretion engage third parties to perform Services (each, a "**Subcontractor**").

2.2 Use of the Hosted Service.

2.2.1 Limitations on Use. Customer is responsible for all activities conducted by its Users and for its Users' compliance with this Agreement. Each party will comply with all applicable Laws in connection with its use of or provision of the Hosted Service, as applicable, including without limitation those related to privacy, electronic communications and anti-spam legislation. Customer will not: (a) sell, lease, license or sublicense the Hosted Service; (b) introduce into or transmit through the Hosted Service any virus, worm, trap door, back door, and other harmful or malicious code, files, scripts, agents, or programs; (c) copy, modify or create derivative works or improvements of the Services or Exiger Materials; (d) reverse engineer, disassemble, decompile, decode, adapt or otherwise attempt to derive or gain access to the source code of the Services or Exiger Materials, in whole or in part; (e) bypass or breach any security device or protection used by the Services or Exiger Materials or access or use the Services or Exiger Materials other than by a User through the use of his or her own then valid access credentials; (f) damage, destroy, disrupt, disable, impair, interfere with or otherwise impede or harm in any manner the Services, Exiger systems or Exiger's provision of services to any third party, in whole or in part; (g) access or use the Services or Exiger Materials in any manner or for any purpose that infringes, misappropriates or otherwise violates any Intellectual Property Right or other right of any third party, or that violates any applicable Law; (h) access or use the Services, Exiger Materials for the purpose of (or as a factor in) (x) establishing an individual's eligibility for personal credit or insurance or assessing risks associate with existing consumer credit obligations, (y) evaluating an individual for employment, promotion, reassignment or retention, or (z) any other personal business transaction with another individual; (i) execute a search on an individual without all necessary consents from such individual to perform the searches performed. Customer shall be responsible for its Users' use of the Hosted Service, including Customer's contractors and agents, and Customer's Affiliates, and compliance with this Agreement; or (j) otherwise access or use the Services or

Exiger Materials beyond the scope of the authorization expressly granted under this Agreement and the applicable Statements of Work.

2.2.2 Suspension or Termination of Services. Exiger may, directly or indirectly, and by use of any lawful means, suspend, terminate or otherwise deny Customer's, any User's or any other Person's access to or use of all or any part of the Services or Exiger Materials, without incurring any resulting obligation or liability, if: (a) Exiger receives a judicial or other governmental demand or order, subpoena or law enforcement request that expressly or by reasonable implication requires Exiger to do so; or (b) Exiger believes, in its good faith and reasonable discretion, that: (i) Customer or any User has failed to comply with, any term of this Agreement, or accessed or used the Services beyond the scope of the rights granted or for a purpose not authorized under this Agreement or in any manner that does not comply with applicable Law or with any instruction or requirement of the specifications for the Services in applicable Statements of Work; (ii) Customer or any User is, has been, or is likely to be involved in any fraudulent, misleading or unlawful activities relating to or in connection with any of the Services; or (iii) this Agreement expires or is terminated. Customer also agrees that Exiger may with reasonably contemporaneous telephonic or electronic notice to Customer suspend access to the Hosted Service if Exiger reasonably concludes that Customer's use of the Hosted Service: (i) is being used to engage in denial of service attacks, spamming, or illegal activity; or (ii) is causing immediate, material and ongoing harm to Exiger or others. This section does not limit any of Exiger's other rights or remedies, whether at law, in equity or under this Agreement.

2.3 Service Levels and Support. Subject to the terms and conditions of this Agreement, Exiger will use commercially reasonable efforts to make the Hosted Services available at the service levels set forth in the applicable SOW (the "**Service Level Agreement**"). The Services include Exiger's standard customer support services at the support levels Customer purchases in accordance with the applicable SOW.

2.4 Non-Solicitation. During the Term and for one year after, Customer shall not, and shall not assist any other Person to, directly or indirectly recruit or solicit (other than by general advertisement not directed specifically to any Person or Persons) for employment or engagement as an independent contractor any Person then or within the prior twelve months employed or engaged by Exiger or any Subcontractor and involved in any respect with the Services or the performance of this Agreement.

2.5 Data Privacy and Security.

2.5.1 Exiger Systems and Security Obligations. Exiger will employ security measures in accordance with the SOW and Exiger's data privacy and security policies. If the Services involve the transfer of Personal Data of a data subject based in the European Economic Area, the Data Processing Exhibit attached hereto as Schedule B will apply to Exiger's Processing of that Personal Data, and the parties will execute the Standard Contractual Clauses attached to the Data Processing Exhibit.

2.5.2 Data Backup. The Services do not replace the need for Customer to maintain regular data backups or redundant data archives. Exiger systems are programmed to perform routine backups from time to time. In the event of any loss, destruction, damage, or corruption of Customer Data caused by Exiger systems or Services, Exiger will, as its sole obligation and liability and as Customer's sole remedy, use commercially reasonable efforts to restore the Customer Data from Exiger's then most current backup of such Customer Data.

3. CONFIDENTIALITY

3.1 Confidential Information. The rights and responsibilities of the Parties with respect to the treatment of Confidential Information disclosed during the course of this Agreement are defined in Schedule A.

4. INTELLECTUAL PROPERTY RIGHTS

All right, title and interest in and to the Services and Exiger Materials, including all Intellectual Property Rights therein, are and will remain with Exiger. Customer has no right, license or authorization with respect to any of the Services or Exiger Materials except as expressly set forth here. All other rights in and to the Services and Exiger Materials are expressly reserved by Exiger and any respective third-party licensors. In furtherance of the foregoing, Customer hereby unconditionally and irrevocably grants to Exiger an assignment of all right, title and interest in and to the Resultant Data, including all Intellectual Property Rights relating thereto.

5. PAYMENT TERMS

5.1 Fees. Customer shall pay Exiger the fees set forth in the applicable SOW (“Fees”) in accordance with this section.

5.2 Fee Increases. Exiger will increase Fees at the beginning of each Renewal Term as set forth in the applicable SOW, effective upon thirty (30) days’ written notice to Customer, and the applicable SOW will be deemed amended accordingly.

5.3 Taxes. All Fees and other amounts payable by Customer under this Agreement are exclusive of taxes and similar assessments. Customer is responsible for all sales, use, value-added and excise taxes, and any other similar taxes, duties and charges of any kind imposed by any federal, national, state, provincial or local governmental or regulatory authority on any amounts payable by Customer hereunder, other than any taxes imposed on Exiger's income.

5.4 Payment. Customer shall pay all Fees within 30 days of the date of the invoice thereof, or, if set forth in the applicable SOW, on or prior to the due dates set forth in the applicable SOW. Customer shall make all payments hereunder in the currency set forth in the applicable SOW. Customer shall make payments to the address or account specified in the SOW or such other address or account as Exiger may specify in writing from time to time. Additional payment terms may be set forth in the applicable SOW.

5.5 Late Payment. If Customer fails to make any payment when due then, in addition to all other remedies that may be available:

5.5.1 Exiger may charge interest on the past due amount at the rate of 1.5% per month calculated daily and compounded monthly or, if lower, the highest rate permitted under applicable Law; and

5.5.2 if such failure continues for fourteen days following written notice thereof, Exiger may suspend performance of the Services until all past due amounts and interest thereon have been paid, without incurring any obligation or liability to Customer or any other Person by reason of such suspension.

5.6 No Deductions or Setoffs. All amounts payable to Exiger under this Agreement shall be paid by Customer to Exiger in full without any setoff, recoupment, counterclaim, deduction, debit or withholding for any reason.

6. INDEMNIFICATION

6.1 Exiger Indemnification. Exiger shall indemnify, defend and hold harmless Customer and Customer's officers, directors, employees, agents, successors and assigns (each, a “Customer Indemnitee”) from and against any and all Losses incurred by Customer Indemnitee arising out of or

relating to any claim, suit, action or proceeding (each, an “**Action**”) by a third party (other than an Affiliate of Customer) that Customer's or an User's use of the Services (excluding Customer Data) in compliance with this Agreement (including the Specifications) infringes any Intellectual Property Rights. The foregoing obligation does not apply to any Action or Losses arising out of or relating to any:

6.1.1 access to or use of the Services or Exiger Materials in combination with any hardware, system, software, network or other materials or service not provided or authorized in writing by Exiger;

6.1.2 modification of the Services or Exiger Materials other than: (i) by or on behalf of Exiger; or (ii) with Exiger's written approval in accordance with Exiger's written specification;

6.1.3 failure to timely implement any modifications, upgrades, replacements or enhancements made available to Customer by or on behalf of Exiger;

6.1.4 Exiger's compliance with any specifications or directions provided by or on behalf of Customer or any User; or

6.1.5 act, omission or other matter described in **Section 6.2**. (Customer Indemnification), whether or not the same results in any Action against or Losses by any Exiger Indemnitee.

6.2 Customer Indemnification. Customer shall indemnify, defend and hold harmless Exiger and its Subcontractors and Affiliates, and each of its and their respective officers, directors, employees, agents, successors and assigns (each, an “**Exiger Indemnitee**”) from and against any and all Losses incurred by such Exiger Indemnitee in connection with any Action by a third party (other than an Affiliate of an Exiger Indemnitee) that arises out of or relates to Customer’s unlawful acts or omissions in the performance of its obligations under this Agreement.

6.3 SOLE REMEDY. THIS SECTION SETS FORTH CUSTOMER'S SOLE REMEDIES AND EXIGER'S SOLE LIABILITY AND OBLIGATION FOR ANY ACTUAL, THREATENED OR ALLEGED CLAIMS THAT THIS AGREEMENT OR ANY SUBJECT MATTER HEREOF (INCLUDING THE SERVICES AND EXIGER MATERIALS) INFRINGES, MISAPPROPRIATES OR OTHERWISE VIOLATES ANY THIRD PARTY INTELLECTUAL PROPERTY RIGHT.

7. TERM AND TERMINATION

7.1 Term. The term of this Agreement commences as of the Effective Date and will continue in effect for the term specified on the applicable SOW (the “**Initial Term**”).

7.2 Termination. In addition to any other express termination right set forth elsewhere in this Agreement:

7.2.1 Either party may terminate this Agreement, effective on written notice to the other party, if the other party materially breaches this Agreement, and such breach remains uncured sixty (60) business days after the non-breaching party provides the breaching party with written notice of such breach.

7.2.2 Either party may terminate this Agreement, effective immediately upon written notice to the other party, if the other party: (i) becomes insolvent or is generally unable to pay, or fails to pay, its debts as they become due; (ii) files or has filed against it, a petition for voluntary or involuntary bankruptcy or otherwise becomes subject, voluntarily or involuntarily, to any proceeding under any domestic or foreign bankruptcy or insolvency Law; (iii) makes or seeks to make a general assignment for the benefit of its creditors; or (iv) applies for or has appointed a receiver, trustee, custodian or similar agent appointed by

order of any court of competent jurisdiction to take charge of or sell any material portion of its property or business.

7.2.3 Exiger may terminate this Agreement, effective on written notice to Customer, if Customer: (i) fails to pay any amount when due hereunder, and such failure continues more than thirty (30) days after Exiger's delivery of written notice thereof; or (ii) breaches any of its obligations under **Section 2** (General Terms of Access to Hosted Services), or **Section 3** (Confidentiality).

7.2.4 By ninety (90) calendar days advance written notice, Customer may terminate this Agreement in whole or in part, at its sole discretion and without the need to specify a reason for termination. The actual date of termination of this Agreement will be the later of ninety (90) calendar days from the date of the written notice, or as otherwise specified in Customer's written notice (the "Termination Date"). Where Customer elects to terminate this Agreement in part, Exiger shall continue to provide Services on any portion of the Agreement not terminated. Exiger shall be entitled to payment for Services satisfactorily performed through the Termination Date but shall not be entitled to recover any cancellation charges or damages, including lost profits or reliance damages. Exiger shall not have a reciprocal right to terminate without cause; it being understood that Customer's payment for Services forms the consideration for Exiger not having this right. In the event of Customer's termination without cause, Customer, at Customer's sole election, may also require Exiger to provide reasonable transition assistance. For avoidance of doubt, in the event Customer invokes this provision, Customer understands and agrees that Exiger will not refund any annual licensing fees paid for services that were not yet rendered at the time of termination.

7.3 Effect of Expiration or Termination. Upon any expiration or termination of this Agreement, except as expressly otherwise provided in this Agreement:

7.3.1 all rights, licenses, consents and authorizations granted by either party to the other hereunder will immediately terminate, and, upon written request, each party shall (subject to **Section 7.3.3** below) return or destroy all Confidential Information of the other party;

7.3.2 notwithstanding anything to the contrary in this Agreement, with respect to information and materials then in its possession or control: (i) the Receiving Party may retain the Disclosing Party's Confidential Information; (ii) Exiger may retain Customer Data; and (iii) Customer may retain Exiger Materials, in the case of each of subclause (i) (ii) and (iii) in its then current state and solely to the extent and for so long as required by applicable Law; (iv) Exiger may also retain Customer Data in its backups, archives and disaster recovery systems until such Customer Data is deleted in the ordinary course; and (v) all information and materials described in this section will remain subject to all confidentiality, security and other applicable requirements of this Agreement; and

7.3.3 Exiger may disable all Customer and User access to the Hosted Services and Exiger Materials.

7.4 Surviving Terms. The provisions set forth in the following sections, and any other right or obligation of the parties in this Agreement that, by its nature, should survive termination or expiration of this Agreement, will survive any expiration or termination of this Agreement: **Sections 3** (Confidentiality), **6** (Indemnification), **7.2** (Termination), **8** (Representations and Warranties), **9** (Limitations of Liability), and **11.7** (Force Majeure).

8. REPRESENTATIONS AND WARRANTIES

8.1 Mutual Representations and Warranties. Each party represents and warrants to the other party that:

8.1.1 it is duly organized, validly existing and in good standing as a corporation or other entity under the Laws of the jurisdiction of its incorporation or other organization;

8.1.2 it has the full right, power and authority to enter into and perform its obligations and grant the rights, licenses, consents and authorizations it grants or is required to grant under this Agreement;

8.1.3 the execution of this Agreement by its representative whose signature is set forth at the end of this Agreement has been duly authorized by all necessary corporate or organizational action of such party; and

8.1.4 when executed and delivered by both parties, this Agreement will constitute the legal, valid and binding obligation of such party, enforceable against such party in accordance with its terms.

8.2 Additional Exiger Representations, Warranties and Covenants. Exiger represents, warrants and covenants to Customer that Exiger will perform the Services using personnel of required skill, experience and qualifications and will devote adequate resources to meet its obligations under this Agreement.

8.3 Additional Customer Representations and Warranties. Customer represents and warrants to Exiger that (a) Customer owns or otherwise has and will have the necessary rights and consents in and relating to the Customer Data or any other materials provided by or through Customer so that, as received by Exiger and/or Processed in accordance with this Agreement, they do not and will not infringe, misappropriate or otherwise violate any Intellectual Property Rights, or any privacy or other rights of any third party or violate any applicable Law and (b) Customer and Users shall strictly adhere to the terms of this Agreement in connection with the use of the Service Software and the Services.

8.4 Warranty Disclaimer. ALL SERVICES AND EXIGER MATERIALS ARE PROVIDED “AS IS” AND EXIGER HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHER, AND EXIGER SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, EXIGER MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES OR EXIGER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, OPERATE WITHOUT INTERRUPTION, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM OR OTHER SERVICES EXCEPT IF AND TO THE EXTENT EXPRESSLY SET FORTH IN THE SPECIFICATIONS, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE OR ERROR FREE. CUSTOMER ACCEPTS FULL RESPONSIBILITY AND RISK FOR ANY USE OF ANY EXIGER MATERIALS AND CUSTOMER DATA, AND ANY DECISIONS MADE BY CUSTOMER IN RELIANCE THEREON.

9. LIMITATIONS OF LIABILITY. NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, PUNITIVE, INCIDENTAL, RELIANCE, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF DATA, BUSINESS, REVENUES, PROFITS OR GOODWILL, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EXCEPT FOR ANY THIRD PARTY CLAIMS ARISING OUT OF EACH PARTY'S INDEMNITY OR CONFIDENTIALITY OBLIGATIONS, EACH PARTY'S AGGREGATE LIABILITY FOR DAMAGES SHALL NOT EXCEED THE AMOUNTS PAID BY CUSTOMER UNDER THE SOW THAT RELATES TO THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE TWELVE (12) MONTH PERIOD PRIOR TO THE DATE THE CAUSE OF

ACTION AROSE AND, FOR ALL MATTERS IN THE AGGREGATE, IN NO EVENT SHALL A PARTY'S TOTAL LIABILITY EXCEED THE AMOUNTS PAID BY CUSTOMER TO EXIGER UNDER THIS AGREEMENT DURING THE TWELVE (12) MONTH PERIOD PRIOR TO THE DATE THE FIRST SUCH MATTER AROSE. THESE LIMITATIONS ARE INDEPENDENT FROM ALL OTHER PROVISIONS OF THIS AGREEMENT, FORM A MATERIAL BASIS OF THIS AGREEMENT, AND SHALL APPLY NOTWITHSTANDING THE FAILURE OF ANY REMEDY PROVIDED HEREIN.

10. GENERAL PROVISIONS

10.1 Notices. Notices between the parties will be by personal delivery, overnight delivery, facsimile transmission, or certified or registered mail, return receipt requested, and will be deemed given upon receipt at the address of the recipient party or ten (10) days after deposit in the mail, or via email with confirmation of receipt. Addresses used will be the ones set forth above or such other address as a party hereto will notify the other in writing.

10.2 Severability. In the event of any invalidity of any provision of this Agreement, the parties agree that such invalidity will not affect the validity of the remaining portions of this Agreement, and further agree to substitute for the invalid provision a mutually agreeable valid provision that most closely approximates the intent of the invalid provision.

10.3 Headings. The headings in this Agreement are for convenience of reference only and have no legal effect.

10.4 No Third Party Beneficiaries. This Agreement is intended for the sole and exclusive benefit of the signatories and is not intended to benefit any third party. Only the parties to this Agreement may enforce it.

10.5 Assignment. Neither party may assign, transfer, or delegate any of its rights and obligations under this Agreement without the prior written consent of an authorized representative of the other. Any assignment in violation of this Agreement will be void and of no force and effect. Exiger may assign, sublicense, delegate or transfer all or any portion of its rights or responsibilities under this Agreement by operation of law or otherwise to any subsidiaries or Affiliates thereof, or to any other party in connection with a merger, acquisition, reorganization, or a sale of substantially all of its assets without notice to Customer. All the terms and provisions of this Agreement will be binding upon and inure to the benefit of the parties, their successors and permitted assigns.

10.6 Relationship. Each party hereto is an independent contractor, and neither party is, nor will claim to be, a legal representative, partner, franchisee, agent or employee of the other. This Agreement sets forth the Parties' entire liability and exclusive remedies relating to this Agreement and the Hosted Service provided to Customer under this Agreement.

10.7 Force Majeure. Neither party will be liable to the other for a failure or delay in its performance of any of its obligations under this Agreement (except for the payment of amounts due hereunder) to the extent that such failure or delay is caused by circumstances beyond its reasonable control such as fire, riot, flood, labor disputes, natural disaster, regulatory action, internet or telecommunications failures, terrorist acts, or other causes beyond such party's reasonable control, provided that the non-performing party gives notice of such condition and continues or resumes its performance of such affected obligation to the maximum extent and as soon as reasonably possible. Customer may terminate this Agreement and receive a pro-rata refund of Fees paid for services not provided if a force majeure event affecting Exiger endures for more than thirty (30) days.

10.8 Counterparts and Fax Signatures. This Agreement may be executed in counterparts, each of which will constitute an original, and all of which will constitute one agreement. A signature transmitted via facsimile or scanned original will be deemed an enforceable signature for the purpose of demonstrating the signing party's assent to the Agreement.

10.9 Entire Agreement. This Agreement (including the Schedules hereto) constitutes the entire understanding and agreement between the parties with respect to the subject matter addressed herein and supersedes any and all prior or contemporaneous oral or written communications with respect to the subject matter hereof, all of which are merged herein. In the event of a conflict between the foregoing terms and conditions and any Schedules to this Agreement, the foregoing terms and conditions will control. The parties agree that in the event Customer utilizes a purchase order, any term therein which purports to modify or supplement the terms of this Agreement will be void with no force or effect.

10.10 Governing Law; Submission to Jurisdiction. This Agreement shall be deemed to have been made in the State of Florida and shall be subject to, and governed by, the laws of the State of Florida, and no doctrine of choice of law shall be used to apply any law other than that of the State of Florida. Each Party hereby irrevocably consents and submits to the exclusive jurisdiction of the Circuit Court of Leon County, Florida, for all purposes under this Agreement, and waives any defense to the assertion of such jurisdiction based on inconvenient forum or lack of personal jurisdiction. The Parties also agree to waive any right to jury trial.

10.11 Public Records Addendum ("Addendum"). Vendor agrees that the Addendum attached hereto is hereby incorporated into this Agreement in order to address the public posting of this Agreement and its disclosure to third parties.

10.12 Customer's Additional Terms. Attached as Schedule A are additional terms that Customer requires and Exiger agrees to. In the event of conflict between these additional terms and any other provision of this Master Services and Software as a Service Agreement, the terms in Schedule A shall control.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the date first above written.

CONVERGENT SOLUTIONS, INC.

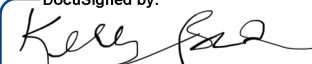
By _____

Name:

Title:

Date:

CITIZENS PROPERTY INSURANCE

DocuSigned by:
By  _____
7B9C7AA80097483...

Name: Kelly Booten

Title: Chief, Systems & Operations

Date: 4/9/2020

DocuSigned by:
By  _____
52091D0BF5B7478...

Name: Jay Adams

Title: Chief Claims Officer

Date: 4/9/2020

**ADDENDUM 1
PUBLIC RECORDS ADDENDUM (“ADDENDUM”)**

Company Name (“Vendor”): Convergent Solutions, Inc.
Agreement Name/Number (“Agreement”):
Primary Vendor Contact Name: [REDACTED]
Telephone: [REDACTED]
Email: [REDACTED]

Citizens is subject to Florida public records laws, including Chapter 119, Florida Statutes. As a part of providing public access to Citizens’ records, Citizens makes its contracts available on Citizens’ external website located at www.citizensfla.com/contracts. This Addendum is incorporated into the Agreement in order to address Citizens’ public posting of the Agreement and its disclosure to third parties.

If Vendor asserts that any portion of the Agreement is exempt from disclosure under Florida public records laws, (the “Redacted Information”), such as information that Vendor considers a protected “trade secret” per Section 815.045, Florida Statutes, then Vendor must select the corresponding declaration below and provide the following to Vendor.ManagementOffice@citizensfla.com:

- (1) **A copy of the Agreement in PDF format with the Redacted Information removed (the “Redacted Agreement”); and,**
- (2) **A dated statement on Vendor’s letterhead in PDF format clearly identifying the legal basis for Vendor’s redaction of the Redacted Information (the “Redaction Justification”).**

Vendor must select one of the two declarations below. If Vendor does not select one of the two declarations below, or if Vendor fails to provide the Redacted Agreement and Redaction Justification within thirty (30) days of Vendor’s receipt of the fully executed Agreement, then without further notice to Vendor, Citizens may post the non-redacted version of the Agreement on its public website and may release it to any member of the public.

<u>Vendor Declaration:</u>
<input type="checkbox"/> Vendor WILL NOT SUBMIT a Redacted Agreement. Citizens may post Vendor’s full, complete, and non-redacted Agreement on its public website, and may release the Agreement to any member of the public without notice to Vendor.
Or
<input checked="" type="checkbox"/> Vendor asserts that a portion of the Agreement is confidential and/or exempt under Florida Public Records law. Therefore, Vendor WILL SUBMIT a Redacted Agreement and a Redaction Justification within thirty (30) days of receipt of the fully executed Agreement. Citizens may post Vendor’s Redacted Agreement on its public website, or release it to any member of the public, without notice to Vendor. If Citizens receives a public records request for the Agreement, Citizens will provide only the Redacted Agreement and Redacted Justification to the requestor. Vendor acknowledges that, in the event of any legal challenge regarding these redactions, Vendor will be solely responsible for defending its position or seeking a judicial declaration.

**SCHEDULE A
CITIZENS' STANDARD TERMS AND CONDITIONS**

THIS SCHEDULE is entered into by Citizens Property Insurance Corporation (“Citizens” or “Customer”) and Convergent Solutions, Inc. (“Exiger” or “Vendor”), pursuant to, and will be governed by, the terms and conditions of that certain Master Services and Software as a Service Agreement between Customer and Exiger having as its effective date April 10, 2020 (the “Agreement”)

1. Definitions. As used in the Agreement, the following terms have the following meanings:

- 1.1. “Citizens Confidential Information” means all information, data, and documentation, whether marked as confidential or not, disclosed to Vendor in the course of this Agreement that is either: sub(a) Protected under any applicable state or federal law (including Chapter 119, Florida Statutes; Sections 501.171, and 627.351(6), Florida Statutes; Chapter 690-128, Florida Administrative Code; and, 15 U.S.C. § 6801 et seq.); (b) private information concerning Citizens employees or policyholders (including social security numbers, personal health information, personal credit information, banking information, drivers’ license numbers, personal email addresses, personal phone numbers, and home addresses); or, (c) related to any Citizens manuals, lists, operating and other systems or programs, business practices or procedures, insurance policies, claimants or claims, or any business, governmental, and regulatory matters affecting Citizens. “Citizens Confidential Information” does not include any information, data or documentation that: (a) is publicly available through no fault of Vendor or Vendor Staff; or, (b) Vendor developed independently without relying in any way on Citizens Confidential Information.
- 1.2. “Deliverables” means the quantifiable, measurable, and verifiable items required to be delivered to Citizens by Vendor under the Agreement.
- 1.3. “Services” means all services and Deliverables to be provided by Vendor to Citizens under the Agreement. If any service or Deliverable is not specifically described in the Agreement but is necessary for the proper performance and provisioning of the Services, that service or Deliverable shall be included within the definition of the Services to the same extent and in the same manner as if specifically described herein.
- 1.4. “Vendor Staff” means any of Vendor’s employees, agents, subcontractors or representatives who: (a) provide the Services; or, (b) have access to Citizens Confidential Information.

2. Deliverables.

- 2.1. Deliverables. Each Deliverable must be delivered by Vendor to Citizens in the time and manner specified in the Agreement and any associated exhibits or attachments. Failure to do so will entitle Citizens to: (a) withhold any payment associated with the Deliverable until such delivery is made; and/or, (b) terminate the Agreement for cause in accordance with the notice and cure provisions set forth in Section 10.2. below.
- 2.2. The provisions of this Section shall survive the termination of the Agreement.

3. Compensation.

- 3.1. Invoices. Vendor must timely submit all requests for compensation for Services or expenses, where permitted, in sufficient detail for a pre- or post-audit. The compensation request must include a unique invoice number, be in US dollars, legible, page-numbered, signed, and dated. Vendor shall also submit a copy, marked as duplicate, of the original, invoice to Citizens' Contract Manager or designee. All invoices and payment credits must be submitted to the attention of Citizens' Accounts Payable department at AccountsPayable@citizensfla.com or Post Office Box 10749, Tallahassee, Florida 32302-2749 in accordance with the Compensation Schedule and must include, at a minimum, the following: (a) Agreement/task order number/purchase order number, if applicable; (b) Vendor's name, address, phone number (and remittance address, if different); (c) Vendor's Federal Employment Identification Number; (d) Citizens' Contract Manager's name; (e) invoice date; (f) Services period; (g) taxes listed separately, if applicable (see Section 7.4.); and, (h) itemized Services for which compensation is being sought.
- 3.2. Payment Processing. Citizens may require any other information from Vendor that Citizens deems necessary to verify any compensation request placed under this Agreement and Vendor agrees that it will provide such information as reasonably requested by Citizens. Payment shall be due net thirty (30) calendar days of Citizens' actual receipt of a complete and undisputed invoice. Where a submitted invoice is incomplete, such as not containing the information described in this Section, Citizens will return the incomplete invoice to Vendor for correction within thirty (30) calendar days of Citizens' actual receipt of such invoice. Where Citizens reasonably disputes any part of a complete invoice, such as the amount of the compensation request, Citizens shall pay any undisputed portion of the invoiced amount within (30) calendar days of Citizens' actual receipt of the complete invoice and will describe the basis for the disputed portion of the invoiced amount. Where Vendor disagrees with Citizens dispute of any invoice, the Parties shall seek to resolve the dispute in accordance with the Dispute Resolution Process further described below. In no case shall Citizens be subject to late payment interest charges where Vendor has submitted an incomplete invoice or where Citizens has reasonably disputed an invoice. Where Vendor fails to submit an invoice within twelve (12) calendar months of the Services for which compensation is being requested, Vendor acknowledges and agrees that any payment due for such Services is forfeited by Vendor for its failure to timely submit an invoice.
- 3.3. Dispute Resolution Process. Each Party will make a good faith effort to resolve any disputes relating to this Agreement prior to commencing a legal action. These efforts may include an offer to arrange for executive-level discussions or an offer to submit the dispute to non-binding mediation. This Section shall not apply if (i) a Party considers the immediate commencement of a legal action for an injunction necessary to protect its interests (e.g., to protect against the improper use or disclosure of its confidential information); or, (ii) the dispute is subject to another provision in this Agreement that includes a different dispute resolution process. For the sake of clarity, Citizens is not subject to the dispute resolution processes set forth in The Florida Administrative Procedure Act, Chapter 120, Florida Statutes.
- 3.4. Travel-related Expenses. Vendor agrees to comply with Citizens' then-current Vendor Travel Reimbursement Guidelines. All travel-related expenses must be pre-approved in writing by Citizens' Contract Manager or designee. Citizens shall reimburse Vendor for pre-approved travel-related expenses incurred in the performance of Services following Citizens' receipt of Vendor's reimbursement request submitted in accordance with the then-current Vendor Travel Reimbursement Guidelines.

- 3.5. No Additional Charges. Except for the compensation described in the Compensation Schedule and travel-related expenses, if permitted, Citizens shall not be billed for or be obligated to pay to Vendor any charges, expenses, or other amounts for the Services or otherwise.
- 3.6. Offsets and Credits. Any amounts due from Vendor may be applied by Citizens against any amounts due to Vendor. Any such amounts that are not so applied shall be paid to Citizens by Vendor within thirty (30) calendar days following Citizens' request.
- 3.7. Taxes. Citizens is a State of Florida, legislatively created, governmental entity which does not pay federal excise or state sales taxes on direct purchases of tangible personal property. Vendor represents and warrants that it is an independent contractor for purposes of federal, state, and local employment taxes. Vendor agrees that Citizens is not responsible to collect or withhold any federal, state, or local employment taxes, including personal property tax, income tax withholding, and social security contributions, for Vendor or Vendor Staff. Any and all taxes, interest or penalties, including personal property tax or any federal, state, or local withholding or employment taxes, imposed, assessed, or levied as a result of the Agreement shall be paid or withheld by Vendor or, if assessed against and paid by Citizens, shall be immediately reimbursed by Vendor upon demand by Citizens.

4. Insurance.

- 4.1. Vendor Insurance Requirements. During the Agreement term, Vendor at its sole expense shall provide commercial insurance of such a type and with such terms and limits as may be reasonably associated with the Agreement. Providing and maintaining adequate insurance coverage is a material obligation of Vendor. Upon request, Vendor shall provide certificates of insurance. The limits of coverage under each policy maintained by Vendor shall not be interpreted as limiting the Contractor's liability and obligations under the Agreement. All insurance policies shall be through insurers authorized or eligible to write policies in Florida.

5. Records; Audits; Public Records Laws.

- 5.1. Record Retention. Vendor shall retain all records relating to this Agreement for the longer of: (a) five (5) years after the termination of this Agreement; or, (b) the period specified by Citizens as necessary to comply with Florida law.
- 5.2. Right to Audit and Inquire. Citizens shall have reasonable access to Vendor's facilities and has the right to review and audit any of Vendor's records relating solely to this Agreement, upon written notice to Vendor of at least three (3) business days. Vendor also agrees to reasonably cooperate with any independent inquiries made by Citizens' Office of Internal Audit and Office of the Inspector General. Vendor shall cooperate with the requestor and provide requested documentation in a timely manner (preferably within five (5) business days). Vendor must resolve any deficiencies discovered during an audit within ninety (90) calendar days from being reported. Citizens may extend the response time period in its sole discretion. Citizens has the right to conduct follow-up audits to assess Vendor's corrective action(s). Any entity performing auditing services on behalf of Citizens pursuant to this Section shall execute a non-disclosure agreement with regard to Vendor's proprietary information, unless precluded from doing so by law. Vendor shall not unreasonably delay or inhibit Citizens' right to audit as set forth in this Section.
- 5.3. Public Records Laws. Vendor acknowledges that Citizens is subject to Florida public records laws, including Chapter 119, Florida Statutes, (collectively, "Florida's Public

Records Laws”). Therefore, any information provided to Citizens or maintained by Vendor in connection with this Agreement may be subject to disclosure to third parties.

- 5.3.1. Protection of Vendor’s Confidential Information. Citizens represents to Vendor the following: (a) Section 627.351(6)(x)l.e., Florida Statutes, provides that proprietary information licensed to Citizens under a contract providing for the confidentiality of such information is confidential and exempt from the disclosure requirements of Florida’s Public Records Law; (b) Section 815.045, Florida Statutes, provides additional protections of Vendor’s trade secret information and an exemption from the disclosure requirements of Florida Public Records Law; and (c) other Florida Statutes allow for various protection of vendor’s trade secrets and financial information. In order to protect any information provided to Citizens that Vendor considers to be protected from disclosure under Florida law (“Vendors Confidential Information”), Vendor should clearly label and mark each page or section containing such information as “Confidential”, “Trade Secret” or other similar designation, provided any technical information that Vendor shares with Citizens regarding Vendor’s proprietary technology (such as any software or source code associated therein) should be afforded confidential treatment irrespective whether labeled or marked.
- 5.3.2. Responding to Request for Vendor Confidential Information. If Citizens receives a Public Records Request (“PRR”) or a request from any regulatory or legislative entity regarding Vendor’s Confidential Information, it shall promptly notify Vendor in writing. To the extent permitted by law, Citizens shall not produce Vendor’s Confidential Information unless authorized by Vendor, or by order of a court of competent jurisdiction. In the event a legal proceeding is brought to compel the production of Vendor’s Confidential Information, the Parties agree that Citizens is authorized to deliver Vendor’s Confidential Information to the court or other legal tribunal for disposition. If Vendor continues to assert in good faith that Vendor’s Confidential Information is confidential or exempt from disclosure or production pursuant to Florida’s Public Records Laws then Vendor shall be solely responsible for defending its position, or seeking a judicial declaration. Nothing in this Agreement shall create an obligation or duty for Citizens to defend or justify Vendor’s position. Vendor also agrees to reimburse Citizens for any attorneys’ fees, costs, and expenses incurred by Citizens or awarded against Citizens in any legal proceeding in which the issue is a third party’s challenge to Vendor’s assertion of an exemption under Florida’s Public Records Laws.
- 5.3.3. Vendor’s Duty to Forward Records Requests to Citizens. Vendor receives a PRR that is in any way related to this Agreement, Vendor agrees to immediately notify Citizens’ Records Custodian and forward the PRR to Citizens’ Records Custodian for logging and processing. Citizens’ Records Custodian’s email address is: Recordsrequest@citizensfla.com. Citizens shall be the Party responsible for coordinating the response and production to the PRR. Vendor shall communicate with Citizens to determine whether requested information is confidential and/or exempt from public records disclosure requirements. Vendor agrees to assist Citizens in responding to any PRR in a prompt and timely manner as required by Florida’s Public Records Laws.

IF VENDOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO VENDOR’S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS AGREEMENT, PLEASE CONTACT CITIZENS’ RECORDS CUSTODIAN AT (i) (850) 521-

8302; (ii) RECORDSREQUEST@CITIZENSFLA.COM; OR, (iii) RECORDS CUSTODIAN, CITIZENS PROPERTY INSURANCE CORPORATION, 2101 MARYLAND CIRCLE, TALLAHASSEE, FL 32303.

- 5.4. Vendor's Failure to Respond to Public Records Request. Vendor must comply with Citizens' request for records, including all documents, papers, letters, emails, or other materials in conjunction with this Agreement, within thirty (30) calendar days of Citizens' request. Vendor's failure to comply with Citizens request may be subject to penalties in accordance with Chapter 119.10, Florida Statutes. Vendor will hold Citizens harmless from any actions resulting from Vendor's non-compliance with Florida's Public Records Laws. Without limiting Citizens' other rights of termination as further described in this Agreement, Citizens may unilaterally terminate this Agreement for refusal by Vendor to comply with this Section unless the records are exempt from Section 24(a) of Article I of the State Constitution and Section 119.07(1), Florida Statutes.
- 5.5. The provisions of this Section shall survive the termination of the Agreement.

6. Security and Confidentiality.

- 6.1. General Requirements. Vendor shall implement and maintain appropriate safeguards to: (a) ensure the security and confidentiality of Citizens Confidential Information; (b) protect against any anticipated threats or hazards to the security or integrity of Citizens Confidential Information; and, (c) protect against unauthorized access to or use of Citizens Confidential Information that could cause harm or inconvenience to Citizens or any customer of Citizens.
- 6.2. Authority to Disclose Confidential Information to Others. Vendor acknowledges and agrees that any Citizens Confidential Information disclosed to or acquired by Vendor is disclosed and/or acquired solely for the purposes of facilitating the provision of the Services. Vendor shall restrict access to Citizens Confidential Information to Vendor Staff who will actually perform Services and Vendor shall provide such Vendor Staff with work environments that protect against inadvertent disclosure to others. Vendor shall be solely responsible for informing any individual or entity with access to Citizens Confidential Information of the provisions of this Agreement and shall be responsible for any acts of those individuals and entities that violate such provisions.
- 6.3. Unauthorized Disclosure of Confidential Information. Vendor will notify Citizens Contract Administrator as soon as possible of any potential or actual unauthorized disclosure, misuse, or misappropriation of Citizens Confidential Information of which it becomes aware and will cooperate in remedying such situation promptly. Pursuant to Section 501.171, Florida Statutes, if Vendor maintains computerized data that includes personal information, as defined in such statute, on behalf of Citizens, Vendor shall disclose to Citizens any breach of the security of the system as soon as practicable, but no later than ten (10) calendar days following the determination of the breach of security or reason to believe the breach occurred.
- 6.4. Notification of Anticipatory Breach. Vendor agrees that should it, for any reason, not be able to provide or maintain appropriate safeguards to fulfill its obligations under this Section, it will immediately notify Citizens Contract Administrator in writing of such inability and such inability on Vendor's part will serve as justification for Citizens' termination of this Agreement, at Citizens' sole election, at any time after the inability becomes known to Citizens.

- 6.5. Remedies. Vendor acknowledges that breach of Vendor's obligation of data security and confidentiality may give rise to irreparable injury to Citizens and Citizens' customers, which damage may be inadequately compensable in the form of monetary damages. Accordingly, Citizens may seek and obtain injunctive relief against the breach or threatened breach of the provisions of this Section, in addition to any other legal remedies which may be available, including, at the sole election of Citizens, the immediate termination, without penalty to Citizens, of this Agreement in whole or in part.
- 6.6. The provisions of this Section shall survive the termination of the Agreement.

7. Miscellaneous.

- 7.1. Vendor Conflicts of Interests. Vendor, and all principals in its business, must execute a Conflict of Interest Form as required by Citizens. Vendor shall not have a relationship with a Citizens officer or employee that creates a conflict of interest. If there is the appearance of a conflict of interest, Vendor will promptly contact Citizens' Contract Manager or designee to obtain a written decision as to whether action needs to be taken to ensure a conflict does not exist or that the appearance of a conflict is not significant.
- 7.2. No Gifts. Vendor shall not give a gift or make an expenditure to or for the personal benefit of a Citizens officer or employee.
- 7.3. Convicted Vendor List. Vendor shall immediately notify Citizens' Contract Manager or designee in writing if it or any of its affiliates are placed on the convicted vendor list maintained by the State of Florida pursuant to Section 287.133, Florida Statutes, or on any similar list maintained by any other state or the federal government.
- 7.4. Compliance with Laws. Vendor and Vendor Staff will comply with all applicable laws, ordinances, rules, and regulations governing Vendor's performance under this Agreement. This includes: (a) annual renewal of authority to transact business in the State of Florida (via www.sunbiz.org) or Vendor's annual written attestation that such authorization is not required; and, (b) maintaining all other necessary permits or licenses from federal, state, and local regulatory/licensing authorities.
- 7.5. Publicity; Use of Names and Logos. Vendor may use Citizens' name and logo in its marketing materials, website and social media to indicate that it is a participating or contracted vendor for Citizens. However, Vendor may not in any way state, imply or infer that it holds a "preferred," "approved," "awarded," "selected" or otherwise special status with Citizens in any such materials. This prohibition includes, but is not limited to, the use of endorsements or quotes from Citizens officials, Citizens vendor scores, or any other Citizens-related materials that may directly or indirectly imply that Vendor enjoys a special or preferred status with Citizens. Citizens reserves the right to determine that its name and/or logo have been misused and to request that Vendor cease using its name and/or logo in any way it deems inappropriate. Failure to comply will result in corrective action, up to and including contract termination. Vendor may only use the approved Citizens logo, which may be obtained by sending a request via email to: newsroom@citizensfla.com.
- 7.6. Waiver. The delay or failure by a Party to exercise or enforce any of its rights under this Agreement shall not constitute or be deemed a waiver of the Party's right thereafter to enforce those rights, nor shall any single or partial exercise of any such right preclude any other or further exercise thereof or the exercise of any other right.
- 7.7. Modification of Terms. Except as otherwise provided for herein, this Agreement may only be modified or amended upon a mutual written contract amendment signed by Citizens and Vendor or as otherwise permitted by this Agreement. Vendor may not unilaterally modify

the terms of this Agreement in any manner such as by affixing additional terms to any Deliverable (e.g., attachment or inclusion of standard preprinted forms, product literature, “shrink wrap” or “click through” terms, whether written or electronic) or by incorporating such terms onto Vendor’s order or fiscal forms or other documents forwarded by Vendor for payment and any such terms shall have no force or effect upon Citizens or this Agreement. Citizens' acceptance of any Service or processing of documentation on forms furnished by Vendor for approval or payment shall not constitute acceptance of any proposed modification to terms and conditions or any conflicting terms and conditions.

- 7.8. Assignment of Antitrust Claims. Vendor and Citizens recognize that in actual economic practice, overcharges resulting from antitrust violations are usually borne by the ultimate consumer. Therefore, Vendor hereby assigns to Citizens any and all claims under the antitrust laws of Florida or the United States for overcharges incurred in connection with this Agreement.

SCHEDULE B DATA PROCESSING EXHIBIT

This DATA PROCESSING EXHIBIT (the “DPE”) is entered into by Citizens Property Insurance Corporation (“Customer”) and Convergent Solutions, Inc. (“Exiger”), pursuant to, and will be governed by, the terms and conditions of that certain Master Services and Software as a Service Agreement between Customer and Exiger having as its effective date April 10, 2020 (the “Agreement”)

1. Definitions

1.1 The following expressions are used in this DPE:

(a) **"Adequate Country"** means a country or territory that the recognised under EU Data Protection Laws from time to time as providing adequate protection for personal data;

(b) **"Customer Group"** means Customer and any Affiliate established and/or doing business in the European Economic Area or Switzerland;

(c) **"Data Subject Request"** means a request from or on behalf of a data subject relating to access to, or rectification, erasure or data portability in respect of that person’s Personal Data or an objection from or on behalf of a data subject to the processing of its Personal Data consistent with that person’s rights under the EU Data Protection Laws;

(d) **"data controller", "data subject", "supervisory authority" and "data processor"** shall have the meanings ascribed to them in the EU Data Protection Laws;

(e) **"Exiger Group"** means Exiger and any Affiliate; and

(f) **“Process”, “Processes” or “Processing”** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, including the collection, recording, organization, storage, updating, modification, retrieval, consultation, use, transfer, dissemination by means of transmission, distribution or otherwise making available, merging, linking as well as blocking, erasure or destruction.

2. Status of the parties

2.1 The type of Personal Data Processed pursuant to this DPE and the subject matter, duration, nature and purpose of the Processing, and the categories of data subjects, are as described in Appendix 1.

2.2 Each of Customer and Exiger warrant in relation to Personal Data that it will comply (and will procure that any of its staff and/or sub-processors comply), with the EU Data Protection Laws. As between the parties, Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3 In respect of the parties’ rights and obligations under this DPE regarding the Personal Data, the parties hereby acknowledge and agree that, as between the parties, Customer or clients of Customer or other member of Customer Group is/are the Data Controller and Exiger is the Data Processor and

accordingly Exiger agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPE.

2.4 Each of Exiger and Customer shall notify to each other an individual within its organisation authorised to respond from time to time to enquiries regarding the Personal Data and each of Exiger and Customer shall deal with such enquiries promptly.

3. Exiger obligations

3.1 With respect to its Processing of Personal Data under this DPE, Exiger warrants that it shall:

(a) only process the Personal Data in order to provide the Services and shall act only in accordance with this Agreement and Customer's written instructions as represented by the Agreement and this DPE;

(b) in the unlikely event that applicable law requires Exiger to process Personal Data other than pursuant to Customer's instruction, notify Customer (unless prohibited from so doing by applicable law);

(c) without undue delay upon becoming aware, inform Customer if, in Exiger's opinion, any instructions provided by Customer under Clause 3.10 infringe the GDPR;

(d) implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks that are presented by the processing, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. Such measures include, without limitation, the security measures set out in Appendix 2;

(e) take reasonable steps to ensure that only authorised personnel have access to such Personal Data and that any persons whom it authorises to have access to the Personal Data are under obligations of confidentiality;

(f) without undue delay upon becoming aware, notify Customer of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data (a "**Security Breach**");

(g) promptly provide Customer with reasonable cooperation and assistance in respect of the Security Breach and all information in Exiger's possession concerning the Security Breach;

(h) not make any announcement about a Security Breach (a "**Breach Notice**") without:

(i) the prior written consent from Customer; and

(ii) prior written approval by Customer of the content, media and timing of the Breach Notice;

unless required to make a disclosure or announcement by applicable law;

(i) promptly notify Customer if it receives a Data Subject Request. Exiger shall not respond to Data Subject Requests without Customer's prior written consent except to confirm that such request relates to Customer. To the extent Customer does not have the ability to address a Data Subject Request (including via the Services), Exiger shall provide reasonable assistance to facilitate the Data

Subject Request, provided Customer shall pay Exiger's charges for providing such assistance, at Exiger's standard consultancy rates set out in the Agreement.

(j) without undue delay following, and in any event within sixty (60) days of, termination or expiry of the Agreement or completion of the Services, delete Customer (at Customer's direction) all Personal Data (including copies thereof) Processed pursuant to this DPE.

(k) provide such assistance as Customer reasonably requests (taking into account the nature of processing and the information available to Exiger) to assist Customer with its obligations under EU Data Protection Laws with respect to:

- (i) data protection impact assessments (as such term is defined in the GDPR);
- (ii) notifications to the supervisory authority under EU Data Protection Laws and/or communications to data subjects by Customer in response to any Security Breach; and
- (iii) Customer's compliance with its obligations under the GDPR with respect to the security of processing;

provided Customer shall pay Exiger's charges for providing the assistance in clause 3(1)(k), at Exiger's standard consultancy rates set out in the Agreement.

4. Sub-processing

4.1 Customer grants a general authorisation (a) to Exiger to appoint other members of the Exiger Group as sub-processors and (b) to Exiger and other members of the Exiger Group to appoint sub-processors to support the performance of the Services.

4.2 Exiger will maintain a list of sub-processors at URL to be provided to Customer and will add the names of new or replacement sub-processors to the list prior to any sub-processing of Personal Data by the new or replacement sub-processor. If Customer has a reasonable objection to any new or replacement sub-processor, it shall notify Exiger of such objections in writing within ten (10) days of the notification and the parties will seek to resolve the matter in good faith.

4.3 Exiger will ensure that any sub-processor it engages to provide the services on its behalf in connection with this Agreement does so only on the basis of a written contract which imposes on such sub-processor terms substantially no less protective of Personal Data than those imposed on Exiger in this DPE (the "**Relevant Terms**"). Exiger shall procure the performance by such sub-processor of the Relevant Terms and shall be liable to Customer for any breach by such sub-processor of any of the Relevant Terms.

5. Audit and records

5.1 Exiger shall, in accordance with EU Data Protection Laws, make available to Customer such information in Exiger's possession or control as Customer may reasonably request and which Exiger is lawfully entitled to disclose with a view to demonstrating Exiger's compliance with the obligations of data processors under EU Data Protection Law in relation to its processing of Personal Data.

5.2 Customer may exercise its right of audit under EU Data Protection Laws, through Exiger providing:

(a) an audit report not older than 18 months by a registered and independent external auditor demonstrating that Exiger's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard (such as ISO 27001 or SSAE 16 II SOC1 and SOC2); and

(b) additional information in Exiger's possession or control to an EU supervisory authority when it requests or requires additional information in relation to the data processing activities carried out by Exiger under this DPE.

6. Data transfers

6.1 To the extent any Processing of Personal Data by Exiger takes place in any country outside the EEA (except if in an Adequate Country), the parties agree that the standard contractual clauses approved by the EU authorities under EU Data Protection Laws and attached to this DPE (the "SCCs") will apply with respect to that Processing, and that Exiger will comply with the obligations of the 'data importer' and Customer will comply with the obligations of 'data exporter', as set forth in the SCCs.

6.2 Customer acknowledges that the provision of the Services under the Agreement may require the Processing of Personal Data by sub-processors, as permitted under this DPE, in countries outside the EEA from time to time.

6.3 If, in the performance of this DPE and/or the Agreement, Exiger transfers any Personal Data to a sub-processor (which shall include without limitation any affiliates of Exiger) and without prejudice to clause 4 where such sub-processor will process Personal Data outside the EEA, Exiger shall in advance of any such transfer ensure that a mechanism to achieve adequacy in respect of that processing is in place such as:

(a) execution of a written agreement between Exiger and the sub-processor providing at least an equivalent level of data protection as required of Exiger under this DPE, and/or a version of the SCCs approved by the EU authorities under EU Data Protection Laws providing at least an equivalent level of data protection as required of Exiger under this DPE; or

(b) the existence of any other specifically approved safeguard for data transfers (as recognised under the EU Data Protection Laws) and/or a European Commission finding of adequacy.

6.4 The following terms shall apply to the clauses set out in the SCCs:

(a) Customer may exercise its right of audit under clause 5.1(f) of the SCCs as set out in, and subject to the requirements of, clause 5.2 of this DPE; and

(b) Exiger may appoint sub-processors as set out, and subject to the requirements of, clauses 4 and 6.3 of this DPE.

7. General

7.1 If Customer determines that a Data Breach with respect to its Personal Data requires notification to any supervisory authority and/or data subjects and/or the public or portions of the public, Customer will notify Exiger before the communication is made and supply Exiger with copies of any written documentation to be filed with the supervisory authority and of any notification Customer proposes to make (whether to any supervisory authority, data subjects the public or portions of the public) which references Exiger, its security measures and/or role in the Security Breach, whether or

not by name. Subject to Customer's compliance with any mandatory notification deadlines under the GDPR, Customer will consult with Exiger in good faith and take account of any clarifications or corrections Exiger reasonably requests to such notifications and which are consistent with the GDPR.

7.2 This DPE is without prejudice to the rights and obligations of the parties under the Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPE and the terms of the Agreement, the terms of this DPE shall prevail so far as the subject matter concerns the processing of Personal Data.

7.3 Exiger's liability to Customer and to each member of Customer Group (taken together) under or in connection with this DPE (including under the standard contractual clauses set out in the SCCs) shall be subject to the same limitations and exclusions of liability as apply under the Agreement as if that liability arose under the Agreement.

7.4 This DPE sets out all of the terms that have been agreed between the parties in relation to the subjects covered by it. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPE.

7.5 A person who is not a party to this DPE shall not have any rights to enforce this DPE including (where applicable) under the Contracts (Rights of Third Parties) Act 1999 of the United Kingdom to enforce any term of this Addendum.

7.6 Should any provision of this DPE be invalid or unenforceable, then the remainder of this DPE shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

7.7 Without prejudice to clause 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the SCCs, this DPE shall be governed by and construed in accordance with the laws of the country of territory stipulated for this purpose in the Agreement and each of the parties agrees to submit to the Choice of jurisdiction as stipulated in the Agreement in respect of any claim or matter arising under this DPE.

7.8 Other than in respect of any accrued liabilities of either party and the provisions of clauses 1, 2 and this clause 7, this DPE shall terminate automatically on the expiry or termination for whatever reason of the Agreement.

Attachment 1 to the Data Processing Exhibit

Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: CITIZENS PROPERTY INSURANCE CORPORATION

Address: 2102 Maryland Circle, Tallahassee, FL 32303

Tel.: 904-407-0270; fax: N/A; e-mail: Jennifer.Peeri@citizensfla.com

Other information needed to identify the organization: N/A

And

Name of the data importing organisation: CONVERGENT SOLUTIONS, INC.

Address: c/o Exiger LLC, 1095 Avenue of the Americas, 5th Floor, New York, NY 10036, USA

Tel.: 212.455.9400; fax: N/A; e-mail: [REDACTED]

Other information needed to identify the organisation: This relationship is serviced by Exiger Canada, Inc.

EACH A “PARTY”, TOGETHER “THE PARTIES”, HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) *'the data exporter'* means the entity who transfers the personal data;
- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of EU Data Protection Laws 95/46/EC;
- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established; and
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of EU Data Protection Laws 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be

replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the country of establishment of the data exporter.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of

the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Citizen Property Insurance Corporation, which wishes to receive due diligence and related services

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Convergent Solutions, Inc., which provides due diligence and related services

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

The data subjects are the existing or prospective clients and/or vendors of the data exporter and its affiliates located in the EEA and Switzerland, and individuals who are employees, principals, agents, or representatives of, or otherwise affiliated or associated with, individual or institutional clients and/or vendors, or prospective clients and/or vendors, of the data exporter and its affiliates in the EEA and Switzerland.

Categories of data

The personal data transferred concern the following categories of data (please specify):

name, address, date of birth, Social Security Number, Tax ID number, passport number, or other government-issued identification number or code, and such other data that may be transferred from the data exporter to the data importer for the purposes of performing the services pursuant to the services agreement entered into by the parties.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

None

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

processing open web sources and selected data bases to extract due diligence information; the processing shall continue until the earliest of (i) expiry/termination of the Agreement or (ii) the date

upon which processing is no longer necessary for the purposes of either party performing its obligations under the Agreement (to the extent applicable);

Appendix 2
to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The data importer will undertake appropriate technical and organizational measures to protect against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. The measures to be taken should take into account available technology and the cost of implementing the specific measures, and must ensure a level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

Appropriate measures must include, without limitation, the following:

1. Adopting and implementing data importer's policies and standards related to security;
2. Assigning responsibility for information security management;
3. Devoting adequate personnel resources to information security;
4. Requiring employees, vendors and others with access to personal data to enter into signed confidentiality agreements;
5. Conducting training to make employees aware of information security risks and to enhance compliance with the data importer's policies and standards related to data protection;
6. Preventing unauthorized access to personal data through the use, as appropriate, of physical and logical (password) entry controls, secure areas for data processing, procedures for monitoring the use of data processing facilities, and built-in system audit trails;
7. Protecting data maintained in online systems through the use, as appropriate, of secure passwords, network intrusion detection technology, encryption and authentication technology, secure log-on procedures, and virus protection;
8. Monitoring compliance with the data importer's policies and standards related to data protection on an ongoing basis;
9. Complying with all of the provisions of the Agreement relating to security which provisions shall take precedence over this Appendix 2 in the event of any conflict or inconsistency; and
10. Taking such other steps as may be appropriate under the circumstances.

**SCHEDULE C
STATEMENT OF WORK NO. 1**

THIS STATEMENT OF WORK, including all exhibits, schedules, attachments and annexes hereto (“SOW”), is entered into by Citizens Property Insurance Corporation (“Customer”) and Convergent Solutions, Inc. (“Exiger”) pursuant to, and will be governed by, the terms and conditions of that certain Master Services and Software as a Service Agreement between Customer and Exiger having as its effective date April 10, 2020 (the “Agreement”).

This SOW sets forth the agreement of the parties regarding the Services that Exiger will supply, perform and deliver to and for Customer in accordance with this SOW and the Agreement.

SOW Effective Date:	The effective date of this SOW is April 10, 2020.
SOW Initial Term:	5 years

Additional Terms and Conditions

1. Customer's Service Fees.

Base Software license and Implementation Fee for 5-year term: [REDACTED]

Service	Subscription Start Date	Subscription Term	# of Authorized Users	Maximum # of Annual Profiles	Cost USD
Implementation	April 10, 2020	One-time	NA	NA	[REDACTED]
Access to Insight 3PM Platform	April 10, 2020	Annual	[REDACTED]	[REDACTED]	[REDACTED]
Total Cost for Year 1:					[REDACTED]
Total Cost for Year 2:					[REDACTED]
Total Cost for Year 3:					[REDACTED]
Total Cost for Year 4:					[REDACTED]
Total Cost for Year 5:					[REDACTED]

Implementation and annual fees for Year 1 will be invoiced and payable upon execution of this SOW. Annual Fees for subsequent years will be payable at the beginning of the new year (e.g., The Annual Fees for Year 2 will be invoiced on April 10, 2021).

2. Exiger's Services Description and Pricing:

Service	Description	Term	Price
Access to Insight 3PM Platform	<p>Customer will be given access to the Exiger Insight 3PM product via one license for all compliance and legal team members as well as required business users. Access will be granted via usernames and passwords for each user.</p> <p>Features:</p> <ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] 	[REDACTED]	[REDACTED]

<p>DDIQ</p>	<p>DDIQ (Due Diligence IQ) is Exiger’s proprietary due diligence engine. With technology built on machine learning (Artificial Intelligence) and Natural Language Processing (NLP), DDIQ rapidly executes hundreds of searches and analyzes thousands of data sources about companies and individuals and provides actionable intelligence in minutes. The DDIQ decision engine employs the same cognitive processes that a due diligence researcher would, without the constraints of human-based research and at a fraction of the cost.</p> <p>[REDACTED]</p> <ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] 	<p>[REDACTED]</p>
<p>Monitoring</p>	<p>[REDACTED]</p> <ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] 	<p>[REDACTED]</p>
<p>Support</p>	<p>Exiger will provide access to Insight 3PM application support M-F 8am – 8pm local hours support for Customer users as well as third party questionnaire recipients. Detailed SLA attached.</p> <p>[REDACTED]</p>	<p>[REDACTED]</p>
<p>Client Success Manager</p>	<p>Post go-live, Customer will be assigned a client success manager, who will speak with Customer on a regular basis to gather feedback on the product and ensure it is meeting their specific needs. The client success manager be the primary liaison on best use of the product and will act as a conduit for technical product suggestions by Customer.</p>	<p>[REDACTED]</p>
<p>Implementation</p>	<p>Exiger will provide a dedicated implementation team that will act as the project management function from implementation kickoff to go-live. The price listed here is based on the general scope of implementation defined with Customer. Exiger will agree and define the detailed scope and timing of implementation with Customer after kickoff. Exiger will agree on a go-live date with Customer during set-up and implementation. In the event Exiger personnel are required onsite for implementation, Exiger will</p>	<p>[REDACTED]</p>

	<p>charge reasonable travel expenses consistent with Customer’s internal guidelines and approved by Customer in writing. Exiger may charge Customer Professional Service Fees for additional configuration performed after the go-live date. Implementation includes:</p> <ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] 		
Training	Exiger will provide up to two training sessions annually for users via Webex or similar virtual platform. Additional training sessions will be subject to additional charge.		
Entity Upload Service Fee	If Customer requests that Exiger assist with the mass uploading of entities, Exiger will charge an entity upload fee.		
Document Upload Service Fee	If Customer requests that Exiger assist with the mass uploading of documents to be assigned to legacy third parties, Exiger will charge a document upload fee.		
Customization	If necessary, Exiger and Customer will agree on development modifications to the core Exiger Insight 3PM platform to fit Customer third-party management workflow, and the parties will agree on additional timetables and fees payable by Customer to Exiger for such modifications.		
Professional Services Fee	The modification of questionnaires, risk models, workflows and other configurable features in the system requires administrative support. Customer point of contact can request these changes through their Exiger support team. Depending upon Exiger resource availability, modifications to an existing questionnaire or risk model will be made within approximately 5 business days and new questionnaires will be added within approximately 10 business days. If Customer adds more than the number of questionnaires, users or risk models contemplated above, Exiger may administer the hourly professional services fee.		
Hosted Services	Exiger will use commercially reasonable efforts to make the Hosted Services available at the service levels set forth in <u>Attachment A</u> .		

Schedule/Plan	<p>Except as may otherwise be specified herein, the time table for the performance of the Services will be determined on an as needed basis. All onboarding requests will need to go through a formal submission, review and acceptance process. At the end of that process Exiger will provide Customer with a schedule based on current availability of resources and timing of releases.</p> <p>The Parties will participate in the kick-off within 30 days from Effective Date. The Go Live will be within 90 days from the kickoff.</p>	N/A	N/A
---------------	--	-----	-----

Attachment A
Service Level Agreement

1. Definitions

Capitalized terms used in this Attachment A will have the meanings set forth below or as otherwise set forth in the main body of the Agreement. If the definitions conflict, the definitions set forth below shall prevail.

“First Level Support” means to (a) answer, in the first instance, all questions and inquiries of any Authorized User concerning the use and operation of, and Problems concerning, the Service Software; and (b) in the first instance, attempt to resolve any Problems reported by Authorized Users.

“Maintenance Release” means any updates to the Hosted Services that are intended to correct Problems and may include minor enhancements to the Hosted Services as may be provided by Exiger from time to time during the term pursuant to this Agreement.

“Maintenance Window” means a period designated by Exiger during which maintenance will be performed.

“Problem” means any defect, error, bug or other failure of all or part of the Hosted Services not conforming to, or performing in accordance with, the specifications.

“Regular Support Hours” means 8 a.m. to 8 p.m. Eastern Standard Time during any business day.

“Resolution” means correction or elimination of a Problem.

“Resolution Time(s)” means the period of time within which Exiger will provide a Resolution.

“Response Time(s)” means the time period, commencing on Exiger Help Desk receipt of the technical support request indicating the occurrence of a Problem, within which Exiger shall deliver a response to Customer confirming that Exiger received such technical support request and has commenced working on the Problem.

“Second Level Support” means to: (a) analyze and resolve any Problems or other matters concerning the Service Software that are referred to the Exiger Help Desk by the Customer Help Desk that cannot be resolved by Customer; (b) follow up directly with the Customer Help Desk with respect to all matters concerning the Service Software that are referred to the Exiger Help Desk by the Customer Help Desk; and (c) keep Customer Help Desk reasonably apprised of the status of, or resolution of, any Problems or other matters concerning the Service Software that are referred to the Exiger Help Desk by the Customer Help Desk.

“Targeted Resolution Time” means the period of time within which Exiger will use commercially reasonable efforts to provide a Resolution.

“Workaround” means a temporary solution to a Problem which results in the return of the Hosted Services to functional or operational status. Notwithstanding the availability of a Workaround, Exiger will continue to fix the error. For certainty, Exiger may provide such a solution through the provision of instructions that results in (or if followed by Customer would have resulted in) such a temporary solution.

2. Maintenance and Support

(a) Maintenance Releases. Exiger shall provide Maintenance Releases to support Hosted Services to Customer on the following terms:

i. Exiger shall have sole discretion over the provision of Maintenance Releases;

- ii. Customer may not refuse the provision of any Maintenance Release unless such release degrades the performance of Hosted Services;
 - iii. the provision of Maintenance Releases shall be included at no extra charge;
 - iv. Exiger shall make available to Customer any Maintenance Release as soon as it is made generally available by Exiger to any of its other clients unless a delay is caused by the past provision of Customization Services; and
 - v. Customer will be notified of any planned downtime for upgrades and patches to the service, at least 7 days in advance, and Exiger will use commercially reasonable efforts to schedule such planned downtime during non-Regular Support Hours.
- (b) Availability Calculation. Availability is based on a weekly 7 day x 24 hour calculation excluding scheduled and emergency downtime. The calculation will be as follows: $((a - b) / a) \times 100$, where “a” is the total number of hours in a given calendar quarter, and “b” is the total number of hours that service is not available in a given quarter. Specifically excluded from “b” in the calculation of the availability measurement are (1) all planned downtime including the standard Maintenance Window and the other scheduled and emergency downtime; (2) a service interruption caused by a security threat until such time as the security threat has been eliminated; (3) reasons of a Force Majeure Event (as defined in the Agreement) or events which are outside Exiger’s immediate control; (4) use of unapproved or modified hardware by or on behalf of Customer or Authorized User; and/or (5) issues arising from misuse of the Hosted Services by Customer or its agents or Authorized Users.
- (c) Remedies. Exiger’s exceeding, meeting, or failing to meet the availability as measured over any quarter may be reflected in credits issued pursuant to the following schedule (“Service Credits”):
- i. Availability calculation between 99.0% to 100% provides no service credit.
 - ii. Availability calculation below 99.0% provides credit as discussed in (iii) below.
 - iii. Exiger will issue a service credit reducing Customers’s annual fee in an amount equal to 0.5% of the annual fee applied to the first annual invoice presented to the Customer each year for each 1% of loss of Services (below the 99.0% level). If the Agreement terminates and the Customer does not owe Exiger any fees against which to credit an outstanding service credit, Exiger will issue such service credit as a refund payment to Customer.

The Service Credits shall be cumulative. The annual Service Credits are capped at a maximum of five percent (5%) of the Customer’s annual fee for the Services.

- (d) Chronic Outage. In the event of a chronic Hosted Services outage (“Chronic Outage”) as defined below, Customer may request an escalation of repair “Chronic Outage” means a specific element of a particular Hosted Service (i) that experiences three (3) or more occurrences of repairs during a given month not resulting from an Authorized User-caused impairment or (ii) that is in violation of the same availability SLA objective more than three (3) times within a given year. Exiger will have ten (10) business days following receipt of Customer’s notification of a Chronic Outage to evaluate and prescribe a resolution, including a timeline to complete the prescribed repairs.
- (e) Optional Termination for Persistent Failure to meet the Availability service level. Customer will be entitled to terminate this SOW immediately by written notice to Exiger if the Availability Percentage is 80% or less on five (5) occasions in any rolling six (6) month period during the SOW Term. Upon termination for said Persistent Failure, Exiger will refund to Customer any prepaid fees in relation to any period post the termination date.

3. Problem Management

- (a) First Level Support. Customer shall use commercially reasonable efforts to provide First Level Support. Customer shall designate specific personnel to provide First Level Support (the “Customer Help Desk”) and provide Exiger with the telephone number and email addresses of all such personnel. Customer shall ensure that all personnel of the Customer Help Desk have sufficient qualifications, technical expertise and/or experience for Customer to perform its obligations hereunder and will complete any training provided by Exiger. Customer may substitute the personnel (with the required qualifications) acting as Customer Help Desk at any time by providing to Exiger prior written notice thereof.
- (b) Exiger Help Desk. Exiger shall establish, maintain and operate a help desk (the “Exiger Help Desk”) staffed by live personnel during Regular Support Hours. The Exiger Help Desk shall be accessible to the Customer help desk at:
 - i. via email at InsightSupport@exiger.com; and
 - ii. via telephone at 800-673-7073.

The Exiger Help Desk shall be staffed with the knowledge and expertise to: (a) reasonably answer and respond to commercially reasonable inquiries and questions of Customer Help Desk in respect of the use of the Hosted Services; (b) receive notice of Problems from Customer Help Desk; (c) reasonably answer questions or inquiries of the Authorized User concerning technical or operational matters relating to the Hosted Services; (d) use commercially reasonable efforts to respond to, diagnose and correct Problems; and (e) liaise with Customer Help Desk in respect of any resolution of Problems.

- (c) Second Level Support. In the event that Customer is unable to receive or otherwise find an answer in the first instance to any Authorized User inquiry or Problem, Customer shall direct Customer Help Desk to directly contact the Exiger Help Desk to provide Second Level Support. Customer Help Desk shall continue to be the direct interface to such Authorized User in respect of such inquiry or Problem. Customer shall promptly provide Exiger with all available information and reasonable assistance concerning any reported Problems or other client matters referred to Exiger for resolution. Exiger shall be responsible for all Second Level Support. To provide “Second Level Support” means that Exiger shall use commercially reasonable efforts to provide technical support and maintenance services and implement and maintain a Problem Reporting and resolution process (as described below).
- (d) Response and Resolution Times. Resolution of a problem may be achieved through the provision of a Workaround, provided that Exiger shall make commercially reasonable efforts to provide a permanent solution to the Problem in a subsequent Maintenance Release. The time to provide a Resolution or Workaround shall be measured commencing on the submission of the technical support request to the Exiger Help Desk and shall conclude when the Problem is Resolved. Response Times and Resolution Times for all Problems apply and shall be determined on a Regular Support Hours basis (i.e. upon receipt of a Problem Exiger will work continuously during Regular Support Hours until Resolved).

Exiger will make commercially reasonable efforts to acknowledge technical support requests and take steps to resolve Problems as follows:

<u>Severity</u>	<u>Description</u>	<u>Target Acknowledgement Time</u>	<u>Notification Method</u>	<u>Exiger will aim to provide updates until resolved approximately every:</u>	<u>Target Resolution Time</u>
HIGH	The Problem renders part or all of the core functionality of the service inoperable or causes a significant degradation. Alternatively, the value of the service is severely diminished or the integrity of the related business is at risk	30 minutes	Email	30 minutes	4 hours
MEDIUM	A Problem which has an impact on the service for which a work around exists - meaning a method used to circumvent the issue without eliminating the issues until the issue is actually resolved.	60 minutes	Email	Business day	Within 3 business days
LOW	A Problem which has minimal impact on the day-to-day running of the service	24 hours	Email	Weekly, depending on the scope of the work with respect to the LOW priority Problem	Due to the varied nature of these Problems, the resolution will vary, but Exiger should make every commercially reasonable effort to promptly resolve the issue.

All times above apply during Regular Support hours.

The remedies set forth in this Service Level Agreement are the sole and exclusive remedy for any issues within the scope of or otherwise relating to this Attachment A or any problems arising in connection with the Hosted Services.