Contract Abstract

A Matter #:A-36259

Contract Information

Contract & Solicitation Title: Short Term Rental Property Identification and Compliance Monitoring

Contract Summary: Short Term Rental Property Identification and Compliance Monitoring

Contract Number: 394916 Solicitation Number: Sole Source Requisition Number:

Type of Contract/PO: IDIQ Contract

Contract Start Date: 1/15/2017 Contract Expiration Date: 1/14/2022

Estimated Contract Life Value: $1,000,950 Fund: PIP BU: 01101690

Selection Method: Sole Source

Procurement Staff: Rick Brown BAO Staff: Select from the Following:

Department(s) Served: **Finance**

Contractor Information

Contracting Firm: Host Compliance LLC

Address 1: 735 Market St, Floor 4

Address 2:

City: San Francisco State: CA Zip: 94103

Company Contact: Ulrik Binzer Email Address: binzer@hostcompliance.com

Phone #: 857-928-0955 E1#: 271744

Contract Signatory: Mr. Ulrik Binzer **Email Address: binzer@hostcompliance.com**

Subcontractor Information

Small Business Program: No SBE/SDV participation Amount:

Procurement Nondiscrimination Program: No MWBE Participation Amount:

Disadvantaged Business Enterprise: Was Not applicable for this contract Amount:

Summary of Offers	Score (RFQ Only)	Cost	Result
Host Compliance LLC		$1,000,950	Awarded
			No Other Offers
			No Other Offers
			No Other Offers
			No Other Offers
			No Other Offers
			No Other Offers

Metro Procurement Nashville

Host Compliance Services Agreement Contract 394916

THIS SERVICES AGREEMENT (the "**Agreement**") is entered into as of the January 20, 2017 (the "**Effective Date**"), between Host Compliance LLC, ("**Host Compliance**") and Metropolitan Government of Nashville and Davidson County, with an address at 700 2nd Avenue South, Suite 205, Nashville, TN 37210 (the "**Customer**"). This Agreement sets forth the terms and conditions under which Host Compliance agrees to license to Customer certain hosted software and provide all other services necessary for Customer's productive use of such software (the "Services") as further described in the attached Schedule 1.

1.0 Services.

1.1 Subscriptions. Unless otherwise provided in the attached Schedule 1, (a) Services are purchased as subscriptions, (b) additional service subscriptions may be added during a subscription term, with the pricing for such additional services, prorated for the portion of that subscription term remaining at the time the subscriptions are added, and (c) any added subscriptions will terminate on the same date as the underlying subscription.

1.2 Provision of Services. Customer and any individuals who is authorized by Customer to use the Service (including employees, consultants, contractors and agents, and third parties with which Customer transacts business) ("End Users") may access and use the Services and any other Services that may be ordered by the Customer from time to time pursuant to a valid subscription in accordance with the terms of this Agreement.

1.3 Facilities and Data Processing. Host Compliance will use, at a minimum, industry standard technical and organizational security measures to store data provided by Customer, or obtained by Customer through the use of the Services ("Customer Data"). These measures are designed to protect the integrity of Customer Data and guard against unauthorized or unlawful access. Host Compliance will continue to use Amazon Web Services (AWS) GovCloud (US) to host this solution. This stipulation does not extend to storage of backups. Host Compliance asserts no rights or privileges to Customer Data outside use of data to provide the agreed upon contracted services.

1.4 Modifications to the Services. Host Compliance may update the Services from time to time. If Host Compliance updates the Services in a manner that materially improves functionality, Host Compliance will inform the Customer.

2.0 Customer Obligations.

2.1 Customer Administration of the Services. Customer is responsible for appointing a main contact person for Host Compliance to communicate with (the "Administrator") and such person shall be responsible for: (i) maintaining the confidentiality of passwords and accounts; (ii) managing access to Administrator and End User accounts; and (iii) ensuring that Administrators' and End User's use of the Services complies with this Agreement.

2.2 Compliance. Customer is responsible for use of the Services and will comply with laws and regulations applicable to Customer's use of the Services, if any.

2.3 Unauthorized Use & Access. Customer will limit the access and usage of the Services to authorized End Users and terminate any unauthorized use of or access to the Services. Customer will promptly notify Host Compliance of any unauthorized use of or access to the Services.

2.4 Restricted Uses. Customer will not and will ensure that its End Users do not: (i) sell, resell, or lease the Services; or (ii) reverse engineer or attempt to reverse engineer the Services, nor assist anyone else to do so.

2.5 Third Party Requests.

2.5.1 "Third Party Request" means a request from a third party for records relating to Customer's or an End User's use of the Services including information regarding an End User. Third Party Requests may include valid search warrants, court orders, or subpoenas, or any other request for which there is written consent from End Users permitting a disclosure.

2.5.2 Customer is responsible for responding to Third Party Requests via its own access to information policies. Customer will seek to obtain information required to respond to Third Party Requests and will contact Host Compliance only if it cannot obtain such information despite diligent efforts.

2.5.3 If Host Compliance receives a Third Party Request, Host Compliance will make reasonable efforts, to the extent allowed by law and by the terms of the Third Party Request, to: (A) promptly notify Customer of Host Compliance's receipt of a Third Party Request; (B) comply with Customer's reasonable requests regarding efforts to oppose a Third Party Request; and (C) provide Customer with information or tools required for Customer to respond to the Third Party Request (if Customer is otherwise unable to obtain the information). If Customer fails to promptly respond to any Third Party Request, then Host Compliance may, but will not be obligated to do so.

2.5.4 If Customer receives a Third Party Request for access to the Services, or descriptions, drawings, images or videos of the Services' user interface, Customer will make reasonable efforts, to the extent allowed by law and by the terms of the Third Party Request, to: (A) promptly notify Host Compliance of Customer's receipt of such Third Party Request; (B) comply with Host Compliance's reasonable requests regarding efforts to oppose a Third Party Request; and (C) provide Host Compliance with information required for Host Compliance to respond to the Third Party Request. If Host Compliance fails to promptly respond to any Third Party Request, then Customer may, but will not be obligated to do so.

3.0 Intellectual Property Rights; Confidentiality

3.1 Reservation of Rights. Except as expressly set forth herein, this Agreement does not grant (i) Host Compliance any intellectual Property Rights in the Customer Data or (ii) Customer any Intellectual Property Rights in the Services, any other products or offerings of Host Compliance, Host Compliance trademarks and brand features, or any improvements, modifications or derivative works of any of the foregoing. "Intellectual Property Rights" means current and future worldwide rights under patents, copyright, trade secret, trademark, moral rights and other similar rights. Host Compliance hereby waives any and all statutory and common law liens it may now or hereafter have with respect to

Customer Data or information. Nothing in this agreement or any other agreement between Customer and Host Compliance shall operate as an obstacle to Customer's right to retrieve any and all Customer information from Host Compliance or its agents or to retrieve such information. Upon request, Host Compliance shall provide Customer with an inventory of Customer information that Host Compliance stores and/or backs up.

3.2 Suggestions. Host Compliance may, at its discretion and for any purpose, use, modify, and incorporate into its products and services, and license and sub-license, any feedback, comments, or suggestions Customer or End Users send Host Compliance or post in Host Compliance' online forums without any obligation to Customer.

3.3 Confidential Information. Customer understands and agrees that it will not reveal, publish or otherwise disclose to any person, firm or corporation, without written authorization of Host Compliance, or except as required by law, any Confidential Information of Host Compliance, including without limitation any trade secrets, confidential knowledge, data or other proprietary information relating to the Services. "Confidential Information" means all information, written or oral, relating to the business, operations, services, facilities, processes, methodology, technologies, intellectual property, research and development, customers, strategy or other confidential or proprietary materials of Host Compliance.

3.4 Tennessee Open Records Act.

3.4.1 Host Compliance acknowledges that Customer is subject to the Title 10, chapter 4, Part 5, of the Tennessee Code Annotated and related statutes ("Open Records Act"), and as such is obligated to comply with said state law. If a request is made pursuant to the Open Records Act to view records related to their contractual relationship, Customer agrees to notify Host Compliance of such request and the date such records will be released.

3.4.2 Further, Tennessee Code Annotated Section 10-7-504(i) specifies that information which would allow a person to obtain unauthorized access to confidential information or to government property shall be maintained as confidential. "Government property" includes electronic information processing systems, telecommunication systems, or other communications systems of a governmental entity subject to the statutory provision. Any information which Customer marks or otherwise designates anything other than "Public Information" will be deemed and treated as sensitive information, which is defined as any information not specifically labeled as "Public Information." Information which qualifies as "sensitive information" may be presented in oral, written, graphic, and/or machine-readable formats. Regardless of presentation format, such information will be deemed and treated as sensitive information. Host Compliance may have access to sensitive information. Host Compliance is required to maintain such information in a manner appropriate to its level of sensitivity. All sensitive information must be secured at all times including, but not limited to, the secured destruction of any written or electronic information no longer needed. The unauthorized access, modification, deletion, or

disclosure of any Customer information may compromise the integrity and security of Customer, violate individual rights of privacy, and/or constitute a criminal act.

3.5 Information Security Breach Notification. Host Compliance shall notify Customer of any data breach within 24 hours of Host Compliance's knowledge or reasonable belief (whichever is earlier) that such breach has occurred. The Breach Notice should describe the nature of the breach, the scope of the information compromised, the date the breach occurred. Host Compliance shall cooperate with Customer in connection with Customer's efforts to mitigate the damage or harm of such breach.

4.0 Fees & Payment.

4.1 Fees.

4.1.1 Customer will pay Host Compliance Two Hundred Thousand One Hundred Ninety Dollars ($200,190.00) upfront annually.

4.1.2 Customer will make reasonable efforts to pay any amounts related to the Services within 30 days of receipt of the applicable invoice but in any event shall make payment within 60 days. Unless otherwise indicated, all dollar amounts referred to in the Agreement are in U.S. funds.

4.1.3 Host Compliance agrees to accept all payment in U.S. funds payable via electronic payments.

4.1.4 Customer acknowledges that while it may choose to delay the implementation of the Services, this is not a valid reason for withholding payment on any invoices.

4.2 Taxes. Customer is a governmental entity generally exempt from taxation and will not be responsible for any taxes imposed on Host Compliance. Host Compliance understands that it cannot claim an exemption from taxes by virtue of any exemption that is provided to Customer.

4.3 Purchase Orders. If Customer requires the use of a purchase order or purchase order number, Customer (i) must provide the purchase number at the time of purchase and (ii) agrees that any terms and conditions on a Customer purchase order will not apply to this Agreement or the Services provided hereunder and are null and void.

5.0 Term & Termination.

5.1 Term. The term of this Agreement shall be five years commencing on the date this contract is signed by all required parties and filed in the office of the Metropolitan Clerk ("Effective Date").

5.2 Termination for Convenience. Customer may terminate this Agreement at any time upon thirty (30) days written notice to Host Compliance.

5.3 Effects of Termination for Convenience. If this Agreement is terminated by Customer in accordance with Section 5.2 (Termination for Convenience): (i) the rights granted by Host Compliance to Customer will cease immediately and Host Compliance will return any Customer data to Customer; and (ii) after a reasonable period of time, Host Compliance may delete any Customer Data relating to Customer's account. The following sections will survive expiration or termination of this Agreement: 2.5 (Third Party Requests), 3.0 (Intellectual Property Rights; Confidentiality), , 5.2 (Termination for Convenience),

5.3 (Effects of Termination for Convenience), 6.0 (Indemnification), 7.0 (Exclusion of Warranties; Limitation of Liability), and 8.0 (Miscellaneous).

5.4 Termination for Breach: A party may terminate this Agreement for cause upon 45 days written notice to the other party of a material breach if such breach remains uncured at the expiration of such period.

5.5 Refund or Payment upon Termination for Breach. If this Agreement is terminated by Customer in accordance with Section 5.4 (Termination for Breach), Host Compliance will refund Customer any prepaid fees covering the remainder of the term of all Subscriptions after the effective date of termination.

5.6 Effects of Termination for Breach. If this Agreement is terminated in accordance with Section 5.4 (Termination for Breach): (i) the rights granted by Host Compliance to Customer will cease immediately (except as set forth in this section); (ii) Host Compliance may provide Customer access to its account at then-current fees so the Customer may export its Customer Data; and (iii) after a reasonable period of time, Host Compliance may delete any Customer Data relating to Customer's account. The following sections will survive expiration or termination of this Agreement: 2.5 (Third Party Requests), 3.0 (Intellectual Property Rights; Confidentiality), , 5.5 (Refund or Payment upon Termination for Breach), 5.6 (Effects of Termination for Breach), 6.0 (Indemnification), 7.0 (Exclusion of Warranties; Limitation of Liability), and 8.0 (Miscellaneous).

5.7 Lack of Funding. Should funding for the Agreement be discontinued, Customer shall have the right to terminate the Agreement immediately upon written notice to Host Compliance.

5.8 Change in Law. Should a change in federal, state, or local law prevent Customer from utilizing the Services as the parties intend, Customer shall have the right to terminate the Agreement immediately upon written notice to Host Compliance.

6.0 Indemnification.

6.1 By Host Compliance. Host Compliance will indemnify, defend and hold harmless Customer from and against all liabilities, damages, and costs (including settlement costs and reasonable attorney's fees) arising out of any claim by a third party against Customer to the extent based on an allegations that Host Compliance' technology used to provide the Services to the Customer infringes or misappropriates any copyright, trade secret, patent or trademark right of the third party. In no event will Host Compliance have any obligations or liability under this section arising from: (i) use of any Services in a modified form or in combination with materials not furnished by Host Compliance and (ii) any content, information, or data provided by Customers, End Users, or other third parties.

6.2 By Customer. Only to the extent permitted by law, Customer will indemnify, defend, and hold harmless Host Compliance from and against all liabilities, damages, and costs (including settlement costs) arising out of any claim by a third party against Host Compliance regarding: (i) Customer Data; (ii) Customer's use of the Services in violation of this Agreement; or (iii) End Users' use of the Services in violation of this Agreement.

6.3 Possible Infringement. If Host Compliance believes the Services infringe or may be alleged to infringe a third party's Intellectual Property Rights, then Host Compliance may (i) obtain the right for Customer, at Host Compliance's expense, to continue using the Services; (ii) provide a non-infringing functionally

equivalent replacement for the Services; or (iii) modify the Services so that they no longer infringe. If Host Compliance does not believe the options described in this section are reasonable then Host Compliance may suspend or terminate this Agreement and/or Customer's use of the affected Services with no further liability or obligation to the Customer other than the obligation to provide the Customer with a pro-rata refund of pre-paid fees for the affected portion of the Services.

6.4 General. The party seeking indemnification will promptly notify the other party of the claim and cooperate with the other party in defending the claim. The indemnifying party will have full control and authority over the defense, except that: (i) any settlement requiring the party seeking indemnification to admit liability requires prior written consent, not to be unreasonably withheld or delayed and (ii) the other party may join in the defense with its own counsel at its own expense.

7.0 Exclusion of Warranties; Limitation of Liability; Insurance.

7.1 Exclusion of Warranties. Except as explicitly set forth in this Agreement, Host Compliance makes no other representation, warranty or condition, express or implied, and expressly excludes all implied or statutory warranties or conditions of merchantability, merchantable quality, durability or fitness for a particular purpose, and those arising by statute or otherwise in law or from a course of dealing or usage of trade with respect to the Services. Host Compliance does not make any representations or warranties of any kind to Customer with respect to any third party software forming part of the Services

7.2 Limitation on Indirect Liability. To the fullest extent permitted by law, except for Host Compliance and Customer's indemnification obligations hereunder, neither Customer nor Host Compliance and its affiliates, suppliers, and distributors will be liable under this Agreement for (i) indirect, special, incidental, consequential, exemplary, or punitive damages, or (ii) loss of use, data, business, revenue, or profits (in each case whether direct or indirect), even if the party knew or should have known that such damages were possible and even if a remedy fails of its essential purpose.

7.3 Limitation on Amount of Liability. To the fullest extent permitted by law, Host Compliance' aggregate liability under this Agreement will not exceed the amount paid by Customer to Host Compliance hereunder prior to the event giving rise to liability.

7.4 Insurance. During the term of this Agreement, Host Compliance, at its expense, agrees to obtain and maintain in full force and effect for the duration of the Agreement and any extension hereof General Liability Insurance in the amount of one million dollars, Professional Liability Insurance in the amount of one million dollars. Such insurance shall contain or be endorsed to contain a provision that includes Customer, its officials, officers, employees, and volunteers as additional insureds. Prior to commencement of services, Host Compliance shall furnish Customer with original certificates and amendatory endorsements effecting coverage required by this section and provide that such insurance shall not be cancelled, allowed to expire, or be materially reduced in coverage except on 30 days' prior written notice to:

Department of Law
Insurance and Risk Management
Metropolitan Courthouse, Suite 108 POBox 196300

Nashville, TN 37219

8.0 Miscellaneous.

8.1 Special Terms and Conditions. Host Compliance agrees to the specific terms and conditions contained in Schedule 2, attached hereto, related to the following topics:

- **8.1.1** Information Backup, Contingency Planning and Risk Management
- **8.1.2** Incident Response
- **8.1.3** Physical and Environmental Security
- **8.1.4** Contractor Managed System Requirements

8.2 Terms Modification. This Agreement may be modified from time to time only by written amendment executed by the parties and their signatories hereto.

8.3 Entire Agreement. The Agreement including any invoice provided by Host Compliance, constitutes the entire agreement between Customer and Host Compliance with respect to the subject matter of this Agreement and supersedes and replaces any prior or contemporaneous understandings and agreements, whether written or oral, with respect to the subject matter of this Agreement. If there is a conflict between the documents that make up this Agreement, the documents will control in the following order: this Agreement, then the invoice.

8.4 Governing Law and Venue. The validity, construction and effect of this Agreement and any and all extensions and/or modifications thereof shall be governed in accordance with the laws of the State of Tennessee. Any action between the parties arising from this Agreement shall be maintained in the courts of Davidson County, Tennessee.

8.5 Severability. Should any provision of this Agreement be declared to be invalid by any court of competent jurisdiction, such provision shall be severed and the remaining provisions of the Agreement will remain in full effect.

8.6 Waiver or Delay. Any express waiver or failure to exercise promptly any right under the Agreement will not create a continuing waiver or any expectation of non-enforcement.

8.7 Assignment. Customer may not assign or transfer this Agreement or any rights or obligations under this Agreement without the written consent of Host Compliance. Host Compliance may not assign this Agreement without providing notice to Customer, except Host Compliance my assign this Agreement or any rights or obligations under this Agreement to an affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets without providing notice. Any other attempt to transfer or assign is void.

8.8 Force Majeure. Except for payment obligations, neither Host Compliance nor Customer will be liable for inadequate performance to the extent caused by a condition that was beyond the party's reasonable control (for example, natural disaster, act of war or terrorism, riot, labor condition, governmental action and Internet disturbance).

8.9 Procurement Piggybacking. Host Compliance agrees to reasonably participate in any "piggybacking" programs pertinent to local government.

Schedule 1

Scope of Services:

Address Identification

Monthly email-delivered report and live web-delivered dashboard with complete address information and screenshots of all identifiable STRs within the jurisdiction of the Metropolitan Government of Nashville and Davidson County ("Metropolitan Government"):

- Up-to-date list of jurisdiction's active STR listings
- High resolution screenshots of all active listings (captured weekly)
- Full address and contact information for all identifiable STRs in jurisdiction
- All available listing and contact information for non-identifiable STRs in jurisdiction

Compliance Monitoring

Ongoing monitoring of the short-term rentals operating in Metropolitan Government's jurisdiction for zoning and permit compliance coupled with systematic outreach to non-compliant short-term rental property owners (using Metropolitan Government of Nashville-Davidson's form letters)

- Ongoing monitoring of STRs for zoning and permit compliance
- Pro-active and systematic outreach to unpermitted and/or illegal short-term rental operators (using jurisdiction's form letters)
- Monthly staff report on jurisdiction's zoning and permit compliance:
- Up-to-date list of STRs operating illegally or without the proper permits
- Full case history for non-compliant listings

Rental Activity Monitoring and Tax Collection Support

Ongoing monitoring of jurisdiction's short-term rental properties for signs of rental activity and/or tax compliance:

- Automatic monitoring of review activity across 15+ STR websites
- Weekly screenshots of reviews and calendars for each active listing
- Quarterly pro-active, systematic and data-informed outreach to short-term rental operators regarding their tax remittance obligations (using jurisdiction's form letters)
- Quarterly staff report on jurisdiction's STR tax compliance:
- Up-to-date list of short-term rental landlords suspected of under-reporting taxes
- Documentation of information that serves as the foundation for the suspicion of tax under-reporting
- Custom reports and analysis to support tax audits and other STR related investigations

Note: Detailed rental activity monitoring requires 6 months of data accumulation to be most effective.

24/7 Short-term Rental Hotline

24/7 staffed telephone and email hotline for neighbors to report non-emergency problems related to STR properties:

- Incidents can be reported by phone or email
- Full documentation of all reported incidents
- Digital recordings and written transcripts of all calls
- Ability for neighbors to include photos, video footage and sound recordings to document complaints
- Real-time outreach to owners of problem properties (whenever owner's contact info is known)
- Weekly staff reports containing:
  - The # and types of reported incidents
  - List of properties for which incidents have been reported
- Custom reports and analysis of hotline related activities

SECTION BU

Information Backup, Contingency Planning and Risk Management

1 **General.**

1.1 Contractor agrees to backup Metro Government Information which Contractor maintains or Stores. Backup and restoration procedures and related infrastructure, including frequency of backup, offsite storage, media lifespan and media reliability, must be commensurate with the criticality and availability requirement of the Metro Government Information being backed up.

1.2 Upon Metro Government's request, Contractor shall supply Metro Government with an inventory of Metro Government Information that Contractor Stores and/or backed up.

1.3 Contractor shall periodically, no less often than annually, test backup tapes or media by restoring Metro Government Information to a system similar to the original system where the Metro Government Information are stored.

1.4 Upon Metro Government's request, Contractor shall supply copies of Metro Government Information in a format requested by Metro Government.

1.5 Contractor shall backup business critical information at a frequency determined by Metro Government business owner.

2 **Storage of Backup Media.** Contractor shall store archival and backup media in a secured offsite location. Upon request, Contractor will promptly notify Metro Government of the physical address of the offsite location. The backups of the information should be stored in a manner commiserate with the security around the information. The backup tapes should be encrypted if the sensitivity of the information requires that level of security.

3 **Disaster Recovery Plan.** Contractor will maintain a Disaster Recovery Plan for all applications or information stores which contain business critical information. This plan will outline the procedures necessary to restore business critical information on the application or systems in a timely fashion in the case of an emergency or disaster.

4 **Emergency Mode Operation Plan.** Contractor shall maintain an emergency mode operating plan which ensures that systems or applications using or accessing business critical information are operational during an emergency or natural disaster, or are made operational after a disaster in a prompt manner, commensurate with the criticality of the information on the system.

5 **Testing and Revision Procedure.** Contractor agrees to test, at least annually, Contractor Disaster Recovery Plan and emergency mode operations plan and maintain a documented procedure for such testing. Contractor shall document the results and findings from such testing and revise the plan accordingly.

6 **Risk Management Requirements.** Contractor shall implement internal risk management practices to ensure the confidentiality, integrity and availability of Metro Government Information. These practices will be no less secure than the ones used by Contractor to protect Contractor's own Sensitive Information or information of comparable sensitivity.

SECTION IR

Incident Response

1 **Incident Reporting.** Contractor shall report any Information Security Incident of which it becomes aware, or failure of any technical or procedural controls, which has or had a potential to affect Metro Government Network, Metro Government Infrastructure or Metro Government Information to Metro Government and according to the following timeline and procedure:

1.1 Contractor shall promptly report to Metro Government any successful Information Security Incident (with or without actual harm to system or information) within 24 hours of becoming aware of the incident. At a minimum, such report shall contain: (a) date and time when the Information Security Incident occurred; (b) the date and time when such incident was discovered by Contractor; (b) identification of the systems, programs, networks and/or Metro Government Information affected by such incident; (c) preliminary impact analysis; (d) description and the scope of the incident; and (e) any mitigation steps taken by Contractor However, if Contractor is experiencing or has experienced a Information Breach or a successful Information Security Incident to systems that host or Store Sensitive Information or an Information Security Incident that is causing or has caused material disruption to the functionality or operation of Contractor systems or damage to Contractor hardware, software or information, including a successful attack by Malicious Software, Contractor shall report such security breach or incident to Metro Government both to the ITS Help Desk at (615) 862-HELP and to the Metro Government department within 24 hours from Contractor's reasonable awareness of such security breach or incident.

1.2 Contractor shall document any attempted but unsuccessful Information Security Incident of which it becomes aware and report to Metro Government upon its request. The frequency, content, and format of such report will be mutually agreed upon by the parties.

2 **Incident Response.**

2.1 Contractor shall have a documented procedure for promptly responding to an Information Security Incidents and Information Breach that complies with applicable law and shall follow such procedure in case of an incident. Contractor shall have clear roles defined and communicated within its organization for effective internal incidence response.

2.2 Contractor shall designate a contact person for Metro Government to contact in the event of an Information Security Incident. This contact person should possess the requisite authority and knowledge to: (i) act as a liaison to communicate between Contractor and Metro Government regarding the incident (including providing information requested by Metro Government); (ii) perform the reporting obligations of Contractor under this exhibit; and (iii) develop a mitigation strategy to remedy or mitigate any damage to Metro Government Network, Metro Government Infrastructure, Metro Government Information or the Product or Service provided to Metro Government that may result from the Information Security Incident.

SECTION PES

Physical and Environmental Security

Contractor shall implement security measures at any Contractor facilities where Sensitive Information is stored. Such security measures must include, at a minimum:

1 **Contingency Operations.** A documented Disaster Recovery Plan for accessing the facility and the Sensitive Information, and restoring Sensitive Information if needed, in the case of an emergency or crisis.

2 **Environmental Safeguards.** Reasonable environmental safeguards to protect systems storing Sensitive Information from smoke, heat, water, fire, humidity, or power surge damage.

3 **Access Control.** Appropriate controls which ensure that only authorized personnel are allowed physical access to the facility. Examples of appropriate controls include, but are not limited to: signage; personnel badges and controlled badge access; visitor sign in, escort, and sign out; security guards; and video surveillance for information centers which store Sensitive Information.

4 **Maintenance Records.** Contractor shall conduct regular maintenance on systems which contain Sensitive Information and to facility's physical and environmental controls (e.g., temperature, physical access). Contractor shall maintain documentation of any repairs or maintenance performed on the systems or facility and shall provide Metro Government a copy of such records upon its reasonable request.

5 **Physical Safeguards.** Contractor shall use best efforts to prevent theft or damage to Contractor systems or storage media containing Sensitive Information. Such efforts shall include, but are not limited to:

5.1 Protecting systems or devices that contain un-encrypted Sensitive Information with physical barriers such as locked cabinet, floor to ceiling room, or secured cage.

5.2 Not storing Un-encrypted Sensitive Information in "multi-party" shared physical environments with other entities.

5.3 Not transporting or shipping un-encrypted media which stores Sensitive Information unless the information is sanitized through full media overwrite (at least one complete pass), or media destruction through shredding, pulverizing, or drive-punching (e.g., breaking the hard drive platters).

5.4 In the event Products generate, store, transmit or process Sensitive Information and the Product does not support encryption, Contractor shall be solely responsible for the provision of physical security measures for the applicable Products (e.g., cable locks on laptops).

SECTION VMGT

Contractor Managed System Requirements

1 Vulnerability and Patch Management.

1.1 For all Contractor Managed Systems that store Metro Government Information, Contractor will promptly address Vulnerabilities though Security Patches. Unless otherwise requested by Metro Government, Security Patches shall be applied within fourteen (14) days from its release for Critical Security Patches, thirty (30) days for Important Security Patches, and twelve (12) months for all other applicable Security Patches. Contractor may provide an effective technical mitigation in place of a Security Patch (if no Security Patch is available or if the Security Patch is incompatible) which doesn't materially impact Metro Government's use of the system nor require additional third party products.

1.2 If the application of Security Patches or other technical mitigations could impact the operation of Contractor Managed System, Contractor agrees to install patches only during Metro Government approved scheduled maintenance hours, or another time period agreed by Metro Government.

1.3 Contractor Managed Systems on the Metro Government Network or Metro Government Infrastructure, the Metro Government retains the right to delay patching for whatever reason it deems necessary.

1.4 Metro Government will monitor compliance and check for Vulnerabilities on all Products on the Metro Government Network or Metro Government Infrastructure. Contractor shall provide Metro Government administrative credentials upon request for the purpose of monitoring compliance of a given Product. Metro Government will not knowingly change configurations of the Contractor Managed Systems without prior approval from Contractor.

1.5 Government may monitor compliance of Contractor Managed Systems. Contractor agrees to allow Metro Government to check for Vulnerabilities during agreed upon times using mutually agreed upon audit methods.

1.6 Contractor shall use all reasonable methods to mitigate or remedy a known Vulnerability in the Contractor Managed System according to the level of criticality and shall cooperate fully with Metro Government in its effort to mitigate or remedy the same. Upon Metro Government's request, Contractor shall implement any reasonable measure recommended by Metro Government in connection with Contractor's mitigation effort.

2 System Hardening.

2.1 Contractor Managed Systems, Contractor shall ensure that either: (i) file shares are configured with access rights which prevent unauthorized access or (ii) Contractor shall remove or disable file shares that cannot be configured with access controls set forth in (i) hereof. Access rights to file shares that remain under (i) must use the Principle of Least Privilege for granting access.

2.2 In the event that Contractor is providing Products or systems that are to be directly accessible from the Internet, Contractor shall disable or allow disabling by Metro Government of all active or executed software components of the Product or system that are not required for proper functionality of the Product or system.

2.3 Contractor shall ensure that Contractor Managed Systems are synchronized with reliable time sources and have the proper time zone set or no time offset (e.g., GMT or UTC). In the case of systems residing on the Metro Government Network, Contractor shall ensure that all such systems are synchronized with an Metro Government corporate timeserver in their respective Regional Information Centers (RDC).

2.4 For Contractor Managed Systems, Contractor shall remove or disable any default or guest user accounts. Default accounts that cannot be removed or disabled must have their default password changed to a Strong Password that is unique to the respective site and Metro Government.

2.5 For Contractor Managed Systems, Contractor shall ensure that the system is configured to disable user accounts after a certain number of failed login attempts have occurred in a period of time less than thirty (30) minutes of the last login

attempt or that system monitoring and notification is configured to alert system administrators to successive failed login attempts for the same user account.

3 **Authentication**.

3.1 Contractor shall assign a unique user ID to any Agent or end user who accesses Sensitive Information on Contractor Managed Systems. This unique ID shall be configured so that it enables tracking of each user's activity within the system.

3.2 Contractor agrees to require authentication for access to Sensitive Information on Contractor Managed System.

3.3 Contractor agrees to configure the system to support Strong Authentication for accessing Sensitive Information from any Open Network (e.g., Internet, open wireless). For avoidance of doubt, Metro Government Network is considered a trusted network.

3.4 Contractor shall configure the system to expire passwords at least every one-hundred and eighty (180) days and require a password change on the next successful login. For system that cannot support Strong Passwords, Contractor shall configure the system to expire passwords every ninety (90) days.

3.5 Unless otherwise agreed by Metro Government, Contractor shall ensure that Contractor Managed Systems will require Strong Password for user authentication.

4 **Automatic Log off.** Contractor shall configure systems which store Sensitive Information to automatically logoff user sessions at the most after 20 minutes of inactivity.

5 **User Accountability.** Contractor shall report to Metro Government, on request, all user accounts and their respective access rights within the system within five (5) business days or less of the request.

6 **Information Segregation, Information Protection and Authorization.** Contractor shall implement processes and/or controls to prevent the accidental disclosure of Metro Government Sensitive Information to other Contractor Metro Governments, including an Affiliates of Metro Government.

7 **Account Termination**. Contractor shall disable user accounts of Agents or Metro Government end users for the system within five (5) business days of becoming aware of the termination of such individual. In the cases of cause for termination, Contractor will disable such user accounts as soon as administratively possible.

8 **System / Information Access.**

8.1 Contractor and its Agents shall only access system, application or information which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent Contractor or its Agent from accessing those information or functions outside of Metro Government's authorization. Contractor shall impose reasonable sanctions against any Agent who attempts to bypass Metro Government security controls.

8.2 Contractor agrees to use the Principle of Least Privilege when granting access to Contractor Managed Systems or Metro Government Information.

9 **System Maintenance.**

9.1 Contractor shall maintain system(s) that generate, store, transmit or process Metro Government Sensitive Information according to manufacturer recommendations. Contractor shall ensure that only those personnel certified to repair such systems are allowed to provide maintenance services.

9.2 Contractor shall keep records of all preventative and corrective maintenance on systems that generate, store, transmit or process Metro Government Sensitive Information. Such records shall include the specific maintenance performed, date of maintenance, systems that the maintenance was performed on including identifiers (e.g., DNS name, IP address) and results of the maintenance. Upon request by Metro Government, Contractor shall supply such record within thirty (30) days.

Contract Number _____

Notices and Designation of Agent for Service of Process

All notices to METRO shall be mailed or hand delivered to:

PURCHASING AGENT
PROCUREMENT DIVISION
DEPARTMENT OF FINANCE
PO BOX 196300
NASHVILLE, TN 37219-6300

Notices to CONTRACTOR shall be mailed or hand delivered to:

CONTRACTOR:	Host Compliance LLC
Attention:	Ulrik Binzer
Address:	735 Market Street, Suite 400
Telephone:	857-928-0955
Fax:	NA
E-mail:	binzer@hostcompliance.com

CONTRACTOR designates the following as the CONTRACTOR's agent for service of process and will waive any objection to service of process if process is served upon this agent:

Designated Agent: NA

Attention: NA

Address: NA

[SPACE INTENTIONALLY LEFT BLANK]

Contract Number _____

Effective Date

This contract shall not be binding upon the parties until it has been fully electronically approved by the supplier, the authorized representatives of the Metropolitan Government, and filed in the office of the Metropolitan Clerk.

THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

APPROVED AS TO PROJECT SCOPE:

DocuSigned by: Tom Eddlemon
65A9B587275F451...
Dept. / Agency / Comm. Head or Board Chair.

DS NG
Dept. Fin.

APPROVED AS TO COMPLIANCE WITH PROCUREMENT CODE:

DocuSigned by: Jeff L. Gossage
7D9F3E023C9F4E2...
Purchasing Agent

Purchasing

APPROVED AS TO AVAILABILITY OF FUNDS:

DocuSigned by: Talia Lomax O'dneal
EC3EA21F849C47C...
Director of Finance

DS AN
OMB

DS kG
BA

APPROVED AS TO FORM AND LEGALITY:

DocuSigned by: Margaret O. Darby
50B50B7AB9D9435...
Metropolitan Attorney

DS BC
Insurance

FILED BY THE METROPOLITAN CLERK:

Metropolitan Clerk

Date

CONTRACTOR

Host Compliance LLC
Company Name

DocuSigned by: Mr. Ulrik Binzer
C671F4BECABF043C...
Signature of Company's Contracting Officer

Mr. Ulrik Binzer
Officer's Name

Ulrik Binzer
Officer's Title

HOST COMPLIANCE

HOST COMPLIANCE, LLC
Short-term Rental Compliance Monitoring and Associated Services
HCSA - 5-5-2016 - P
Contract 394916

Schedule 1

Scope of Services:

Address Identification

Monthly email-delivered report and live web-delivered dashboard with complete address information and screenshots of all identifiable STRs within the jurisdiction of the Metropolitan Government of Nashville and Davidson County ("Metropolitan Government"):

- Up-to-date list of jurisdiction's active STR listings
- High resolution screenshots of all active listings (captured weekly)
- Full address and contact information for all identifiable STRs in jurisdiction
- All available listing and contact information for non-identifiable STRs in jurisdiction

Compliance Monitoring

Ongoing monitoring of the short-term rentals operating in Metropolitan Government's jurisdiction for zoning and permit compliance coupled with systematic outreach to non-compliant short-term rental property owners (using Metropolitan Government of Nashville-Davidson's form letters)

- Ongoing monitoring of STRs for zoning and permit compliance
- Pro-active and systematic outreach to unpermitted and/or illegal short-term rental operators (using jurisdiction's form letters)
- Monthly staff report on jurisdiction's zoning and permit compliance:
- Up-to-date list of STRs operating illegally or without the proper permits
- Full case history for non-compliant listings

Rental Activity Monitoring and Tax Collection Support

Ongoing monitoring of jurisdiction's short-term rental properties for signs of rental activity and/or tax compliance:

- Automatic monitoring of review activity across 15+ STR websites
- Weekly screenshots of reviews and calendars for each active listing
- Quarterly pro-active, systematic and data-informed outreach to short-term rental operators regarding their tax remittance obligations (using jurisdiction's form letters)
- Quarterly staff report on jurisdiction's STR tax compliance:
- Up-to-date list of short-term rental landlords suspected of under-reporting taxes
- Documentation of information that serves as the foundation for the suspicion of tax under-reporting
- Custom reports and analysis to support tax audits and other STR related investigations

Note: Detailed rental activity monitoring requires 6 months of data accumulation to be most effective.

24/7 Short-term Rental Hotline

24/7 staffed telephone and email hotline for neighbors to report non-emergency problems related to STR properties:

- Incidents can be reported by phone or email
- Full documentation of all reported incidents
- Digital recordings and written transcripts of all calls
- Ability for neighbors to include photos, video footage and sound recordings to document complaints
- Real-time outreach to owners of problem properties (whenever owner's contact info is known)
- Weekly staff reports containing:
  - The # and types of reported incidents
  - List of properties for which incidents have been reported
- Custom reports and analysis of hotline related activities

SECTION BU

Information Backup, Contingency Planning and Risk Management

1 **General.**

1.1 Contractor agrees to backup Metro Government Information which Contractor maintains or Stores. Backup and restoration procedures and related infrastructure, including frequency of backup, offsite storage, media lifespan and media reliability, must be commensurate with the criticality and availability requirement of the Metro Government Information being backed up.

1.2 Upon Metro Government's request, Contractor shall supply Metro Government with an inventory of Metro Government Information that Contractor Stores and/or backed up.

1.3 Contractor shall periodically, no less often than annually, test backup tapes or media by restoring Metro Government Information to a system similar to the original system where the Metro Government Information are stored.

1.4 Upon Metro Government's request, Contractor shall supply copies of Metro Government Information in a format requested by Metro Government.

1.5 Contractor shall backup business critical information at a frequency determined by Metro Government business owner.

2 **Storage of Backup Media.** Contractor shall store archival and backup media in a secured offsite location. Upon request, Contractor will promptly notify Metro Government of the physical address of the offsite location. The backups of the information should be stored in a manner commiserate with the security around the information. The backup tapes should be encrypted if the sensitivity of the information requires that level of security.

3 **Disaster Recovery Plan.** Contractor will maintain a Disaster Recovery Plan for all applications or information stores which contain business critical information. This plan will outline the procedures necessary to restore business critical information on the application or systems in a timely fashion in the case of an emergency or disaster.

4 **Emergency Mode Operation Plan.** Contractor shall maintain an emergency mode operating plan which ensures that systems or applications using or accessing business critical information are operational during an emergency or natural disaster, or are made operational after a disaster in a prompt manner, commensurate with the criticality of the information on the system.

5 **Testing and Revision Procedure.** Contractor agrees to test, at least annually, Contractor Disaster Recovery Plan and emergency mode operations plan and maintain a documented procedure for such testing. Contractor shall document the results and findings from such testing and revise the plan accordingly.

6 **Risk Management Requirements.** Contractor shall implement internal risk management practices to ensure the confidentiality, integrity and availability of Metro Government Information. These practices will be no less secure than the ones used by Contractor to protect Contractor's own Sensitive Information or information of comparable sensitivity.

SECTION IR

Incident Response

1 **Incident Reporting.** Contractor shall report any Information Security Incident of which it becomes aware, or failure of any technical or procedural controls, which has or had a potential to affect Metro Government Network, Metro Government Infrastructure or Metro Government Information to Metro Government and according to the following timeline and procedure:

1.1 Contractor shall promptly report to Metro Government any successful Information Security Incident (with or without actual harm to system or information) within 24 hours of becoming aware of the incident. At a minimum, such report shall contain: (a) date and time when the Information Security Incident occurred; (b) the date and time when such incident was discovered by Contractor; (b) identification of the systems, programs, networks and/or Metro Government Information affected by such incident; (c) preliminary impact analysis; (d) description and the scope of the incident; and (e) any mitigation steps taken by Contractor However, if Contractor is experiencing or has experienced a Information Breach or a successful Information Security Incident to systems that host or Store Sensitive Information or an Information Security Incident that is causing or has caused material disruption to the functionality or operation of Contractor systems or damage to Contractor hardware, software or information, including a successful attack by Malicious Software, Contractor shall report such security breach or incident to Metro Government both to the ITS Help Desk at (615) 862-HELP and to the Metro Government department within 24 hours from Contractor's reasonable awareness of such security breach or incident.

1.2 Contractor shall document any attempted but unsuccessful Information Security Incident of which it becomes aware and report to Metro Government upon its request. The frequency, content, and format of such report will be mutually agreed upon by the parties.

2 **Incident Response.**

2.1 Contractor shall have a documented procedure for promptly responding to an Information Security Incidents and Information Breach that complies with applicable law and shall follow such procedure in case of an incident. Contractor shall have clear roles defined and communicated within its organization for effective internal incidence response.

2.2 Contractor shall designate a contact person for Metro Government to contact in the event of an Information Security Incident. This contact person should possess the requisite authority and knowledge to: (i) act as a liaison to communicate between Contractor and Metro Government regarding the incident (including providing information requested by Metro Government); (ii) perform the reporting obligations of Contractor under this exhibit; and (iii) develop a mitigation strategy to remedy or mitigate any damage to Metro Government Network, Metro Government Infrastructure, Metro Government Information or the Product or Service provided to Metro Government that may result from the Information Security Incident.

SECTION PES

Physical and Environmental Security

Contractor shall implement security measures at any Contractor facilities where Sensitive Information is stored. Such security measures must include, at a minimum:

1 **Contingency Operations.** A documented Disaster Recovery Plan for accessing the facility and the Sensitive Information, and restoring Sensitive Information if needed, in the case of an emergency or crisis.

2 **Environmental Safeguards.** Reasonable environmental safeguards to protect systems storing Sensitive Information from smoke, heat, water, fire, humidity, or power surge damage.

3 **Access Control.** Appropriate controls which ensure that only authorized personnel are allowed physical access to the facility. Examples of appropriate controls include, but are not limited to: signage; personnel badges and controlled badge access; visitor sign in, escort, and sign out; security guards; and video surveillance for information centers which store Sensitive Information.

4 **Maintenance Records.** Contractor shall conduct regular maintenance on systems which contain Sensitive Information and to facility's physical and environmental controls (e.g., temperature, physical access). Contractor shall maintain documentation of any repairs or maintenance performed on the systems or facility and shall provide Metro Government a copy of such records upon its reasonable request.

5 **Physical Safeguards.** Contractor shall use best efforts to prevent theft or damage to Contractor systems or storage media containing Sensitive Information. Such efforts shall include, but are not limited to:

5.1 Protecting systems or devices that contain un-encrypted Sensitive Information with physical barriers such as locked cabinet, floor to ceiling room, or secured cage.

5.2 Not storing Un-encrypted Sensitive Information in "multi-party" shared physical environments with other entities.

5.3 Not transporting or shipping un-encrypted media which stores Sensitive Information unless the information is sanitized through full media overwrite (at least one complete pass), or media destruction through shredding, pulverizing, or drive-punching (e.g., breaking the hard drive platters).

5.4 In the event Products generate, store, transmit or process Sensitive Information and the Product does not support encryption, Contractor shall be solely responsible for the provision of physical security measures for the applicable Products (e.g., cable locks on laptops).

SECTION VMGT

Contractor Managed System Requirements

1 Vulnerability and Patch Management.

1.1 For all Contractor Managed Systems that store Metro Government Information, Contractor will promptly address Vulnerabilities though Security Patches. Unless otherwise requested by Metro Government, Security Patches shall be applied within fourteen (14) days from its release for Critical Security Patches, thirty (30) days for Important Security Patches, and twelve (12) months for all other applicable Security Patches. Contractor may provide an effective technical mitigation in place of a Security Patch (if no Security Patch is available or if the Security Patch is incompatible) which doesn't materially impact Metro Government's use of the system nor require additional third party products.

1.2 If the application of Security Patches or other technical mitigations could impact the operation of Contractor Managed System, Contractor agrees to install patches only during Metro Government approved scheduled maintenance hours, or another time period agreed by Metro Government.

1.3 Contractor Managed Systems on the Metro Government Network or Metro Government Infrastructure, the Metro Government retains the right to delay patching for whatever reason it deems necessary.

1.4 Metro Government will monitor compliance and check for Vulnerabilities on all Products on the Metro Government Network or Metro Government Infrastructure. Contractor shall provide Metro Government administrative credentials upon request for the purpose of monitoring compliance of a given Product. Metro Government will not knowingly change configurations of the Contractor Managed Systems without prior approval from Contractor.

1.5 Government may monitor compliance of Contractor Managed Systems. Contractor agrees to allow Metro Government to check for Vulnerabilities during agreed upon times using mutually agreed upon audit methods.

1.6 Contractor shall use all reasonable methods to mitigate or remedy a known Vulnerability in the Contractor Managed System according to the level of criticality and shall cooperate fully with Metro Government in its effort to mitigate or remedy the same. Upon Metro Government's request, Contractor shall implement any reasonable measure recommended by Metro Government in connection with Contractor's mitigation effort.

2 System Hardening.

2.1 Contractor Managed Systems, Contractor shall ensure that either: (i) file shares are configured with access rights which prevent unauthorized access or (ii) Contractor shall remove or disable file shares that cannot be configured with access controls set forth in (i) hereof. Access rights to file shares that remain under (i) must use the Principle of Least Privilege for granting access.

2.2 In the event that Contractor is providing Products or systems that are to be directly accessible from the Internet, Contractor shall disable or allow disabling by Metro Government of all active or executed software components of the Product or system that are not required for proper functionality of the Product or system.

2.3 Contractor shall ensure that Contractor Managed Systems are synchronized with reliable time sources and have the proper time zone set or no time offset (e.g., GMT or UTC). In the case of systems residing on the Metro Government Network, Contractor shall ensure that all such systems are synchronized with an Metro Government corporate timeserver in their respective Regional Information Centers (RDC).

2.4 For Contractor Managed Systems, Contractor shall remove or disable any default or guest user accounts. Default accounts that cannot be removed or disabled must have their default password changed to a Strong Password that is unique to the respective site and Metro Government.

2.5 For Contractor Managed Systems, Contractor shall ensure that the system is configured to disable user accounts after a certain number of failed login attempts have occurred in a period of time less than thirty (30) minutes of the last login

attempt or that system monitoring and notification is configured to alert system administrators to successive failed login attempts for the same user account.

3 **Authentication**.

3.1 Contractor shall assign a unique user ID to any Agent or end user who accesses Sensitive Information on Contractor Managed Systems. This unique ID shall be configured so that it enables tracking of each user's activity within the system.

3.2 Contractor agrees to require authentication for access to Sensitive Information on Contractor Managed System.

3.3 Contractor agrees to configure the system to support Strong Authentication for accessing Sensitive Information from any Open Network (e.g., Internet, open wireless). For avoidance of doubt, Metro Government Network is considered a trusted network.

3.4 Contractor shall configure the system to expire passwords at least every one-hundred and eighty (180) days and require a password change on the next successful login. For system that cannot support Strong Passwords, Contractor shall configure the system to expire passwords every ninety (90) days.

3.5 Unless otherwise agreed by Metro Government, Contractor shall ensure that Contractor Managed Systems will require Strong Password for user authentication.

4 **Automatic Log off.** Contractor shall configure systems which store Sensitive Information to automatically logoff user sessions at the most after 20 minutes of inactivity.

5 **User Accountability.** Contractor shall report to Metro Government, on request, all user accounts and their respective access rights within the system within five (5) business days or less of the request.

6 **Information Segregation, Information Protection and Authorization.** Contractor shall implement processes and/or controls to prevent the accidental disclosure of Metro Government Sensitive Information to other Contractor Metro Governments, including an Affiliates of Metro Government.

7 **Account Termination**. Contractor shall disable user accounts of Agents or Metro Government end users for the system within five (5) business days of becoming aware of the termination of such individual. In the cases of cause for termination, Contractor will disable such user accounts as soon as administratively possible.

8 **System / Information Access.**

8.1 Contractor and its Agents shall only access system, application or information which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent Contractor or its Agent from accessing those information or functions outside of Metro Government's authorization. Contractor shall impose reasonable sanctions against any Agent who attempts to bypass Metro Government security controls.

8.2 Contractor agrees to use the Principle of Least Privilege when granting access to Contractor Managed Systems or Metro Government Information.

9 **System Maintenance.**

9.1 Contractor shall maintain system(s) that generate, store, transmit or process Metro Government Sensitive Information according to manufacturer recommendations. Contractor shall ensure that only those personnel certified to repair such systems are allowed to provide maintenance services.

9.2 Contractor shall keep records of all preventative and corrective maintenance on systems that generate, store, transmit or process Metro Government Sensitive Information. Such records shall include the specific maintenance performed, date of maintenance, systems that the maintenance was performed on including identifiers (e.g., DNS name, IP address) and results of the maintenance. Upon request by Metro Government, Contractor shall supply such record within thirty (30) days.

ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 10/19/2016

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	CONTACT NAME:	
TechInsurance 1101 Central Expy. South, Suite 250 Allen, TX 75013	PHONE (A/C, No, Ext): 800-668-7020	FAX (A/C, No): (877) 826-9067
	E-MAIL ADDRESS:	

INSURER(S) AFFORDING COVERAGE		NAIC #
INSURER A :	Sentinel Insurance Company, Limited	11000
INSURER B :	Trumbull Insurance Company	27120
INSURER C :	ACE	22667
INSURER D :		
INSURER E :		
INSURER F :		

INSURED

Host Compliance Llc
735 Market St
San Francisco, CA 94103

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	✓ COMMERCIAL GENERAL LIABILITY ☐ CLAIMS-MADE ✓ OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: ✓ POLICY ☐ PRO-JECT ☐ LOC ☐ OTHER:	Yes		46SBAUQ5747	5/25/2016	5/25/2017	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG $	$ 1,000,000 $ 1,000,000 $ 10,000 $ 1,000,000 $ 2,000,000 $ 2,000,000 $
A	AUTOMOBILE LIABILITY ☐ ANY AUTO ☐ ALL OWNED AUTOS ☐ SCHEDULED AUTOS ✓ HIRED AUTOS ✓ NON-OWNED AUTOS	Yes		46SBAUQ5747	5/25/2016	5/25/2017	COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident) $	$ 1,000,000 $ $ $ $
	☐ UMBRELLA LIAB ☐ OCCUR ☐ EXCESS LIAB ☐ CLAIMS-MADE ☐ DED ☐ RETENTION $						EACH OCCURRENCE AGGREGATE $	$ $ $
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? Y/N: N (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N/A		46WECAR1436	5/25/2016	5/25/2017	✓ PER STATUTE ☐ OTH-ER E.L. EACH ACCIDENT E.L. DISEASE - EA EMPLOYEE E.L. DISEASE - POLICY LIMIT	 $ 1,000,000 $ 1,000,000 $ 1,000,000
C	Professional Liability (Errors and Omissions)			G26775292001	5/25/2016	5/25/2017	$1,000,000 / $1,000,000	

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Metropolitan Government of Nashville and Davidson County, its officials, officers, employees, and volunteers are named as Additional Insured (per GL form SS 00 08 04 05) as their interests may appear in regards to general liability and automobile liability. Workers Compensation is provided in the state of TN.

CERTIFICATE HOLDER

Metropolitan Government of Nashville and Davidson County
Metro Courthouse
Nashville, TN 37201

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE