RF-Works
Service Attachment 2
Wireless as a Service (WaaS)

This Service Attachment (the "Service Attachment"), is between RF Works ("Service Provider") having an office at 2172 Citygate Dr. Columbus, Ohio 43219, and the State of Ohio, through the Department of Administrative Services ("the State"), having its principal place of business at 30 East Broad Street, 40th Floor, Columbus, Ohio 43215 (jointly referred hereto as the "Parties"), and it is effective as of the date signed by the State. It amends that certain Master Cloud Services Agreement ("MCSA") between the Parties dated August 28, 2013.

As of the effective date of this Service Attachment 2, RF-Works Service Attachment 1, dated October 31, 2013 is hereby canceled and will no longer be in effect.

1. **Definitions.**

   The defined Terms in the MCSA will have the same meanings in this Service Attachment as they do in the MCSA. There may be additional definitions contained herein.

2. **Services.**

   Overview.

   The RF-Works Wireless service offering is the Service Provider's Wireless as a Service (WaaS) offering that provides robust Wi-Fi. The service is an overlay to the existing Local Area Network (LAN) and provides tiers of service to enable guest Wi-Fi, internal business use, voice and Location Based services.

   Standard Service Features.

   Service Provider will provide Enterprise class managed 802.11 Wireless LAN (WLAN) service and equipment. The Enterprise class wireless equipment used by Service Provider is defined by the Gartner Magic Quadrant for WLAN. The service covers all design and implementation tasks including an active site survey, installation, low voltage cabling to Access Points, all WLAN hardware, and connection to a wireless LAN controller and management platform. Guest Access Services provides guest Wi-Fi access with a custom portal for acceptable use policy (AUP) and logical traffic isolation between connections used for internal business use. The wireless service is an overlay onto the existing Subscribing Entity provided LAN and WAN infrastructure and utilizes the Subscribing Entity's own Internet Provider. The wireless service requires low voltage Ethernet cabling which can be installed by the Service Provider or the Subscribing Entity can install the cable per the Service Provider Design Specification. In the event that the Subscribing Entity chooses to install their own cable, a monthly discount will be applied

   Listed below you will find descriptions to assist in determining the right level of Service is for an agency.

Determining Access Point needs.

When deploying Wireless as a Service (WaaS), Service Provider will assist Subscribing Entity with determining what the tier of Service which will dictate the number of access points needed

for both coverage and capacity. The following descriptions are meant to educate the Subscribing Entities on how those decisions should be made.

How many Access Points will you need in your deployment?

In general most wireless deployments fall into one of three tiers of Service, which are broad coverage, general data use, and voice grade wireless. The business use of the wireless will determine which category is chosen and thus will determine the number of wireless Access Points required for deployment. Wireless Guest Access will be available in all tiers of Service.

When the goal is maximum coverage, the enterprise can keep costs low by deploying as few access points as possible and turning up the radio signal power as high as possible. But real-world experience shows that this high-powered approach is not the solution for high capacity deployments. In fact, cranking up the power creates many problems for sites that require high throughput.

Optional Service Features.

In some scenarios business and state policies could dictate that Wi-Fi access be physically separated from the internal LAN. There may also be instances in which the existing LAN is not able to support the WLAN for technical reason. In the event that the purchaser desires the WLAN components to be completely isolated from the existing LAN then Service Provider can provide for enterprise class isolated LAN switching components solely for the use of the wireless service. These LAN components will continue to require WAN connectivity for access back into the cloud and to provide Internet connectivity as previously described.

Outdoor wireless access and bridging services can be provided as an alternative to expensive fiber optic cabling. Due to the unique nature of these services some optional services may be quoted on an individual case basis as custom offerings that include one-time implementation costs and ongoing management costs

Cabling is an optional service, which will meet all prevailing local codes and governing body codes as well as IEEE, TIA / EIA and ISO / IEC Standards for Cabling and Wiring with the exception of asbestos abatement. Asbestos abatement will be the responsibility of the Subscribing Entity. The cabling installation cost will be a one-time charge. The charge will be billed per access point. The cost will range from $240 - $600 depending on the complexity of the run.

Provision of Services. The Service Provider will make the Services available to the Subscribing Entities pursuant to the Agreement, this Service Attachment, and the applicable Order during each Order Term. The State agrees that purchases hereunder are neither contingent on the delivery of any future functionality or features nor dependent on any oral or written public comments made by the Service Provider regarding future functionality or features.

RF-Works
Service Attachment 2
Wireless as a Service (WaaS)

The Service Provider Responsibilities.

The Service Provider must:

(i) provide the Service Provider's basic support for the Services to the Subscribing Entities at no additional charge, and/or upgraded support if available and if purchased,

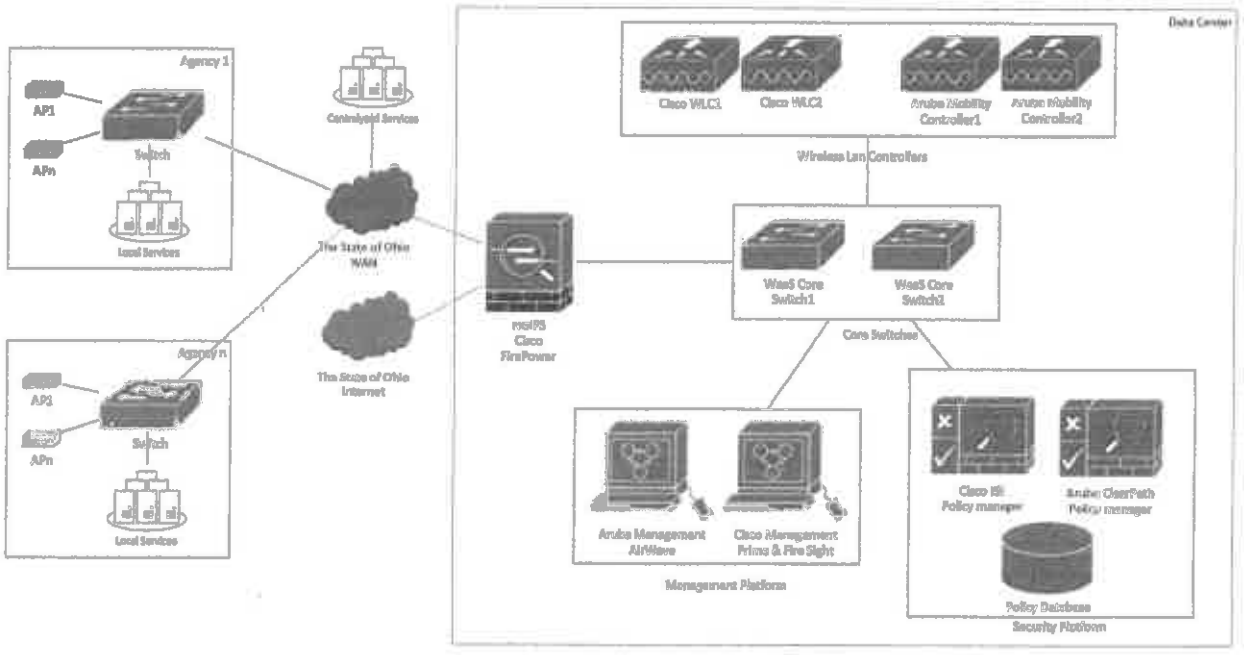
(ii) use commercially reasonable efforts to make the Services available 24 hours a day, 7 days a week, except for:

(a) Planned downtime (of which the Service Provider must give at least 10 calendar days' notice via the Customer Support Center (CSC) and which the Service Provider must schedule 10 p.m. and 6 a.m. Eastern Time and on Saturdays, or

(b) Any unavailability covered by the Agreement's Excusable Delay clause or by the Service Level section later herein, and

(iii) Provide the Services in full accordance with applicable laws and government regulations.

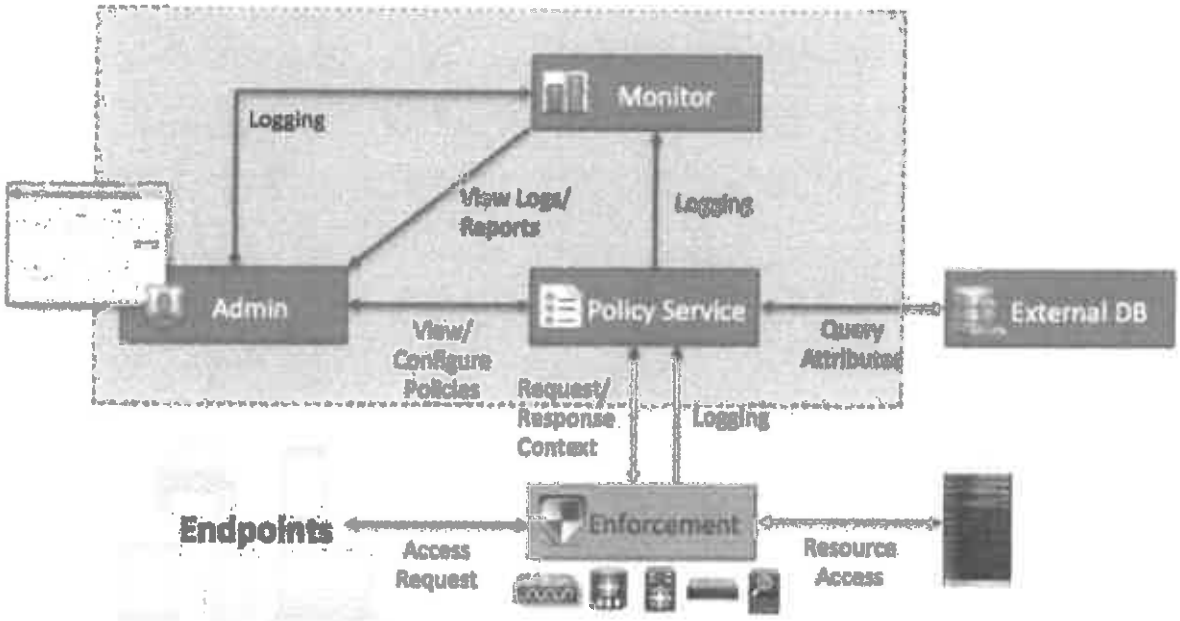
Service Provider will provide a hybrid solution based on Aruba and Cisco devices. Service Provider will manage all legacy equipment with a migration path to either a Cisco or Aruba Enterprise Architecture based on the State's hardware preference. The logical diagram of the solution is presented below:



AirWave will assure management of all state legacy devices as-is until end of life: Aruba, Cisco/Meraki, HP. Management of the WaaS will be assured by Aruba AirWave/Cisco Prime.

Security solution consists by Cisco FirePower/FireSight NGIPS and Aruba Clear Path/Cisco ISE policy managers. Cisco FirePower NGIPS will monitor agency wireless traffic. Aruba Clear Path/Cisco ISE will assure seamless wireless connectivity between locations.

RF-Works
Service Attachment 2
Wireless as a Service (WaaS)



Security solution together with Aruba Mobility Controller/Cisco Wireless LAN Controller will Addresses WLAN and wired network security concurrently.

Service Provider WaaS solution is fully compliant with PCI 3.0:

Goal	PCI Requirement	Product Enforcement	How It's Met
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration	FirePower, ISE/ClearPath	Cisco FirePOWER NGIPS will assure both firewall and IPS/IDS functionalities.
	2. Do not use vendor-supplied defaults for system passwords and other security parameters	FirePower, ISE/ClearPath	RF Works do not use default passwords. A politic of password complexity and periodic change is in place.
Protect Data	3. Protect data	Wireless Lan Controllers	Wireless: PEAP/EAP
	4. Encrypt transmission of data across open, public networks	Wireless Lan Controllers	Wired: encrypted communication between AP and Controller
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs	ISE/ClearPath	Security System Aruba ClearPath/Cisco ISE do not permit endpoints with outdated AntivirusPrograms to access network. For those endpoints only a quarantine network is offered in order to update AntivirusPrograms.
	6. Develop and maintain secure systems and applications	FirePower	All WaaS subsystems are periodically upgraded to keep track of all Security Alerts.
Implement Strong Access Control Measures	7. Restrict access to data by business need to know	ISE/ClearPath	Security System Aruba ClearPath/Cisco ISE policy managers will restrict devices to data by business need to know, based on OISP specifications
	8. Assign a unique ID to each person with computer access	ISE/ClearPath, FirePower	OISP will assign a unique ID to each person with computer access.
	9. Restrict physical access to data	Not Applicable	Policies in place in The State of Ohio restrict physical access to data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and data	ISE/ClearPath, FirePower	All WaaS subsystems logs are provided to The State of Ohio SIEM.
	11. Regularly test security systems and processes	FirePower	RF Works together with OISP will regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel	Not Applicable	OISP will maintain a policy that addresses information security for all personnel.

Service Provider WaaS design adheres to The State of Ohio security controls.

Security Solution based on Aruba Clear Path/Cisco ISE will assure that:

- All devices on wireless networks meet the set security policy
- Deny access to non-conforming devices or allow access to a quarantine network to remedy non-conformities. Both actions can be configured on OISP request
- Includes standard security configurations for client devices and Aps

Cisco Wireless LAN Controllers/Aruba Mobility controller will:

- Configure\control signal strength and direction
- Identify unauthorized WAPs, peer-to-peer networks, or ad hoc networks
- Identify/detect rouge wireless devices within 5 minutes
- All wireless traffic will be monitored by WIDS as it passes into the wireless network (with the help of Cisco FirePower/FireSight
- Use network vulnerability scanning tools to detect WAPs and discover vulnerabilities on wireless devices
- All clients:
  - Have a single connection to Enterprise (no dual connections of wired/wireless simultaneously)
  - Have wireless to wired network, not bridge to Local networks and will not allow dual homed devices at client level

Traffic between wireless and wired networks is separated by firewall. Separate secure paths for authenticated and unauthenticated users (guest vs employee) are assured. All of the WaaS solution is protected by firewalls. Cisco FirePower will protect WaaS solution by DDOS.

Service Provider, through management system, will implement scheduled patch and maintenance Cycles. Hardened configurations are managed by a configuration management system (Cisco Prime/Aruba Clear Path) and hardened configurations are applied to wireless devices.

Service Provider will implement and report on timeout features, session management, audit logs of all logins and paired activity, automatic disconnects over extended periods of connection.

Service Provider WaaS implement secured authentication using EAP/TLS and/or PEAP. Wireless clients will use strong, multifactor authentication. All Wireless traffic will use WPA2 with AES encryption.

Service Provider WaaS will report all logging and alerting to The State of Ohio SIEM. State of Ohio analyst will have access to monitor, view logging and alerting. The State of Ohio will be allowed monitor through SNMP (Simple Network Management Protocol) all deployed devices.

RF-Works
Service Attachment 2
Wireless as a Service (WaaS)

Site Survey

Service Provider will perform an active comprehensive, site evaluation and survey for an IEEE 802.11a/b/g/n/ac wireless local area network (WLAN), at our own expense, prior to quotation for each State of Ohio site. The purpose of the evaluation is to ascertain the number and strategic placement of the access points (APs) required for seamless IEEE 802.11a/b/g/n/ac wireless radiofrequency (RF) propagation within the prescribed areas of the facility. The proposed WLAN Site Survey will deliver optimal bandwidth, wireless coverage, effective throughput, network capacity, roaming capability, and Quality of Service. The Service Provider engineering team will utilized RF testing equipment to test based on the service tier chosen by the IT Management to provide a design that provides a minimum of 20% overlap of adjacent cell coverage, where coverage is provided. A minimum signal floor of -65 dBm, with a minimum signal-to-noise ratio (SNR) of 25 dB for 2.4 GHz and 5 GHz spectra will observed within the extents of each cell.

Service Tier Options

Service Provider wireless deployments fall into one of three tiers of Service, which are broad coverage, general data use, and voice grade wireless. The business use of the wireless will determine which category is chosen and thus will determine the number of wireless Access Points required for deployment. Wireless Guest Access will be available in all tiers of Service.

Tier I – Broad Coverage - Low Cost Maximum Coverage deployments generally support a small number of users with generally low throughput demands. This is a common approach used in public hot spots, warehouses, factories, and very small office installations where cost-effective coverage is more important than bandwidth performance.

Tier II - General Data Use – Most environments fall in to this category where general computing is the primary use and the wired and wireless networks feel like a common experience for users. This type of service will provide for robust data performance and enable collaboration from a mobility perspective.

Tier III – High Capacity Use – High capacity deployments on the other hand support a larger number of high bandwidth users and mission critical wireless services such as voice over wireless, video, location and tracking services.

Implementation

Service Provider WaaS offering covers all design and implementation tasks including an active site survey, installation, low voltage cabling to Access Points, all WLAN hardware, and connection to a wireless LAN controller, associated security, and management platform. Service Provider will install, configure, and test all hardware and software for each installation site. Service Provider has included all cost related to delivery, installation, configuration, testing, maintenance and support of all hardware and software and any other necessary aspects of the

solution. Service Provider will also be responsible for unboxing and disposing of all packaging materials.

Installation

The wireless service requires low voltage Ethernet cabling, which can be installed by Service Provider, or the Subscribing Entity can install the cable per the RF-Works Design Specification. In the event that the Subscribing Entity chooses to install their own cable, a monthly discount will be applied. The standard service feature includes only basic cabling service that requires no alteration to sensitive building structures, conduit, or asbestos abatement. Alteration to sensitive buildings, conduit, and asbestos abatement, will require additional charges.

If the Subscribing Entity chooses to have Service Provider execute the cabling all cables, wires, mounts, and connectors will be included. Infrastructure cabling will be run from the switch to the Access Point. The Point of Entry (POE) for the installation must address POE available within cabling limitation. In the scenario that an installation requires power to be run to the address cabling limitations optional service features will be required.

All cabling, wiring, connectors will be installed in a manner that meets the industry safety and security requirements and guidelines. No hazards will be created; any identified hazard will be identified in writing by the Subscribing Entity. Installations must be performed in a manner that does not harm or diminish local site designs or terminate building cable warranties, other buildings warranties, and structural integrity or, to the extent feasible, cosmetics. Installations will meet all prevailing local codes and governing body codes as well as IEEE, TIA/EIA and ISO/IEC Standards for Cabling and Wiring.

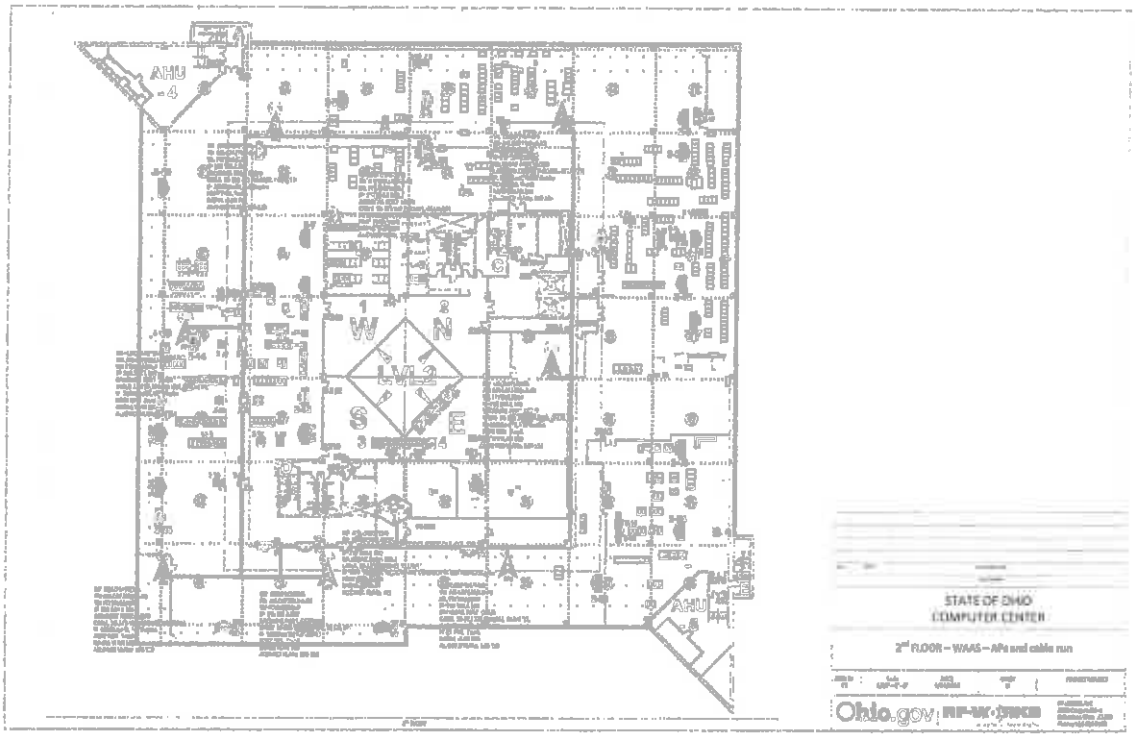
Documentation

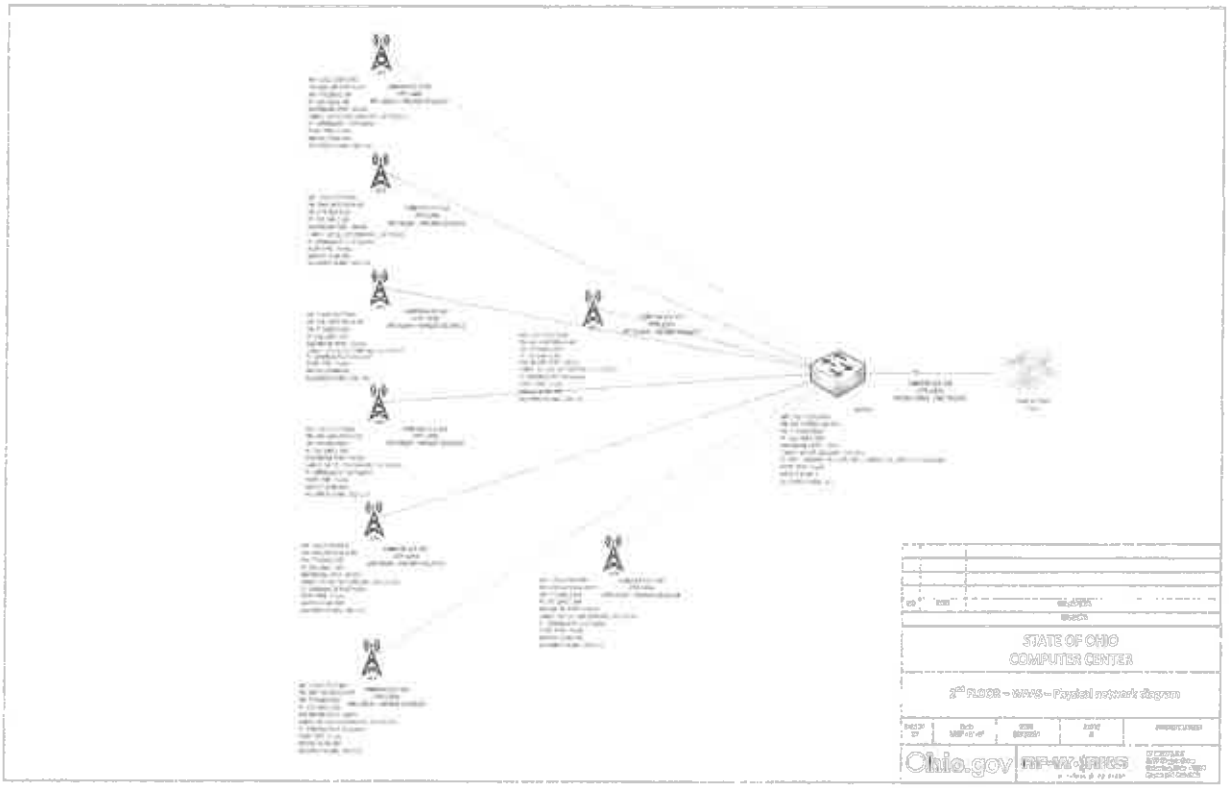
Service Provider will provide a physical network design using Visio Software to the Subscribing Entity. The Diagram will show the location of all network equipment and details of all connections between equipment. Details will include:

A) Equipment make and model
B) Serial Numbers
C) IP Addresses
D) Backbone port, media, speed, and duplex settings
E) VLAN assignments

Any other special settings requested

RF-Works
Service Attachment 2
Wireless as a Service (WaaS)





3. Fees and Payment

See Addendum A for pricing table.

Fees. The Subscribing Entities will pay all fees specified in an Order hereunder, subject to the Terms of the Agreement. Except as otherwise specified herein or in an Order, fees are based on Services purchased and not actual usage, and the number of Object subscriptions (e.g., the number of APs) can be increased or decreased during the relevant Order Term, as provided in the Agreement. Subscribing Entities will pay the first and last equivalent of their starting monthly fee and then monthly fees going forward will be calculated on the Objects in use. Object subscription fees are based on monthly periods that begin on the subscription start date and; therefore, fees for Object subscriptions added in the middle of a month will have a prorated fee and then be added in full for the next monthly period and the remaining periods unless Object Subscription decreases. Subscribing Entities will have the option to extend Terms each time that make an addition to their Object Subscription which will also drive down their cost per object. No Order may specify a Subscription Term not identified and priced in this Service Attachment. Nor may it cover any billable Services not listed in this Service Attachment as a Service.

After 90 days, the Service Provider may suspend the delinquent Subscribing Entity's access to the unpaid Services until all delinquent amounts are paid, notwithstanding the prohibition against self-help provided for elsewhere in the MCSA, but the Service Provider may not do so if the Subscribing Entity is disputing the applicable charges reasonably and in good faith and is cooperating diligently to resolve the dispute.

Invoicing and Payment. Fees will be invoiced monthly in advance and otherwise in accordance with the Order and the Agreement. Fees are due in accordance with the Terms of the Agreement, which no Order may alter except as provided in the MCSA section 1.6 Service Attachment(s) Renewal. The Subscribing Entity is responsible for providing complete and accurate billing and contact information to the Service Provider and notifying the Service Provider of any changes to such information.

4. Service Provider Trade-In Program Terms and Conditions

Service Provider Trade-In Program ("Program") is an 802.11 Access Point (AP) & Controller equipment collection program that is available via email tradein@Service Provider.com or (614) 800-2880. By participating in the Program, the Subscribing Entity agrees to be bound by the Service Provider Trade-In Terms and Conditions listed below. Before any such participation, Subscribing Entity must comply with State & Federal Surplus property procedures. (specifically, GSD-SFP-15) If there are any conflicts between the Service Provider Trade-In Program and the MCSA and SA, the MCSA and SA will prevail.

1. **Eligibility.** To receive a Trade-In Credit (Defined below), the Subscribing Entity must be a new or existing Service Provider customer with an active account with a recurring service charge in good standing. New or existing customers may participate in the program via notification utilizing the State's Ordering System.
    a. **Types of Credits.** The Program offers a credit amount applied to the monthly reoccurring charge (MRC). The amount is divided out across the MRC for the length of the contract. Service Provider' issuance of the Trade-In value is

dependent upon Subscribing Entity's trade-in of an eligible device. Service Provider does not offer refunds or cash reimbursement through this program.

b. **Credit Eligible Devices.** Enterprise Class 802.11 AP's & Controllers are eligible for a Trade-In Credit. Credits will only be issued for eligible devices that are in working order. In order to trade in devices, an Order will need to be placed through the State's Ordering System.
c. **Device Value.** When a Subscribing Entity submits device information to Service Provider, Service Provider will give the Subscribing Entity a valuation quote. The Subscribing Entity must accurately state the make, model, condition, and quantity of the devices. If information is not accurate, then Service Provider may adjust the valuation quote and notify the Subscribing Entity. All valuations quotes are within Service Provider sole discretion, and valuation quotes may change at any time and Subscribing Entity will be notified. The trade-in value of the device is non-negotiable. Service Provider device value is valid for 30 days from the date Subscribing Entity receives a quote.

2. **Device Title.** By participating in this Program, the Subscribing Entity represents that the Subscribing Entity has title, ownership, and interest in the devices submitted, and the Subscribing Entity can transfer the title, ownership, and interest in the devices to Service Provider. The Subscribing Entity agrees that Service Provider will not have any liability in excess of the accepted trade-in value for the devices that is submitted to this program.

5. Proprietary Rights

Reservation of Rights in Services. Subject to the limited rights expressly granted hereunder, the Service Provider reserves all rights, title, and interest in and to the Services, including all related intellectual property rights. No rights are granted to the State or Subscribing Entities hereunder other than as expressly set forth herein or elsewhere in the Agreement.

Restrictions. Subscribing Entities will not intentionally permit any third party to access the Services, except as permitted herein or in an Order, create derivative works based on the Services except as permitted herein or elsewhere in the Master Cloud Services Agreement (MCSA), reverse engineer the Services, or access the Services to build a competitive product or service or to copy any features, functions, or graphics of the Services. Nothing herein prohibits a Subscribing Entity from rights defined in this Service Attachment to support its own business purposes during and after any Term of an Order.

State Applications and Code. If a Subscribing Entity, a third party acting on a Subscribing Entity's behalf, or a user creates applications or program code using the Services, such will be part of the Subscribing Entity's Data. The Subscribing Entity authorizes the Service Provider to host, copy, transmit, display, and adapt such applications and program code, solely as necessary for the Service Provider to provide the Services in accordance with this

Service Attachment. Subject to the above, the Service Provider acquires no right, title or interest from the Subscribing Entity or its licensors under this Service Attachment in or to such applications or program code, including any intellectual property rights therein, and the Subscribing Entity is entitled to port, use, and host such anywhere.

Subscribing Entity's Data. Subject to the limited rights granted by a Subscribing Entity hereunder, the Service Provider acquires no right, title, or interest from a Subscribing Entity or its licensors under this Service Attachment in or to the Subscribing Entity's Data, including any intellectual property rights therein.

6. **Service Levels**

SLAs for the Services.

This Service Attachment includes SLAs that will be used to monitor and manage the Service Provider's performance of Services. The SLAs are listed below. Modifications to the SLAs provided below may only be made by the written Agreement of the State and the Service Provider and presented as an Amendment to this Service Attachment.

Availability.

"Availability" or "Available" means the Subscribing Entity's Users are able to access a Service and use all material features and functions of the Service effectively and efficiently and the Service meets all the SLAs contained in this Service Attachment. "Unavailability" or "Unavailable" means the Subscribing Entity's Users are unable to access the Service or use all the Service's features and functions effectively and efficiently or they do not otherwise meet all SLAs in this Service Attachment, subject to the following:

A Service may be inaccessible to a Subscribing Entity's Users during scheduled downtime. Scheduled downtime will occur 12:00 AM – 6:00 AM Eastern Time, Sunday.

In addition to scheduled downtime, the following will not be considered times when a Service is Unavailable:

(i) Outages resulting from a Subscribing Entity's equipment or its Internet service provider;
(ii) A Subscribing Entity's negligence or breach of its material obligations under this Service Attachment; and
(iii) Excusable Delays, as provided for and handled in accordance with the Service Attachment.
(iv) Power outages at the Subscribing Entity's facility.

RF-Works
Service Attachment 2
Wireless as a Service (WaaS)

SLA Credits.

The "Target Availability Level" is the Service's Availability Level that the Service Provider plans to meet or exceed during each calendar month. The "Service Availability Level" is the number of hours during a particular period that each individual Access Point was Available to the Subscribing Entity, excluding scheduled downtime permitted above, and divided by the total number of hours during such period. The Target Availability Level is provided in the next section.

The Service Provider must actively monitor and report to the Subscribing Entity any and all Unavailability of each individual Access Point monthly, along with reasonable details regarding such Unavailability. The Service Provider must also provide each Subscribing Entity that uses the Service a credit by Access Point within 30 days of any calendar month in which the Service Availability Level is below the Target Availability Level of each individual Access Point, calculated as set forth herein.

The applicable credit will be calculated as follows:

If the Service Provider fails to meet the Target Availability Level by up to four hours, each affected Subscribing Entity will be entitled to the equivalent of one day's fee for the Service. That is, if the fee is an annual fee, the credit would be 1/365th of that annual fee, or if it is a monthly fee, the Subscribing Entity would be entitled to 1/30th of its monthly fee as a credit. Further, the credit will double if the Target Availability Level is missed by more than four but less than eight hours for any calendar month. And if the failure to meet the Target Availability Level is greater than eight hours, the Subscribing Entity will be entitled to the entire fee applicable to that month. Pricing and service is provided based upon each individual Access Point, therefore availability and credits are calculated based on each individual Access Point as well.

Any such credits must be paid to the Subscribing Entity within 30 days after the month in which the Service Provider fails to meet the Target Availability Level.

If the Service Provider fails to meet the Target Availability Level for three consecutive calendar months, any affected Subscribing Entity may terminate any or all Orders for that Service for cause without termination fees.

Specific SLAs.

The Target Availability Level is 99.9% in any calendar month (e.g. 30 day month would have 43.2 minutes).

Support and Service Level Agreement details

An 802.11 Wireless LAN (WLAN) is a complex technology with many factors that can affect the user experience. Environmental factors such as building materials and even furniture can interfere with the wireless signal and cause a poor experience for the user. Also, there are two radios involved in a wireless connection, one being the Access Point and the other being the client. Both the Access Point and the client must perform at optimal levels for the user

experience to be satisfactory. The dynamic nature of the environment and the myriad of client types require constant monitoring and quick resolution to issues that will arise in a Wireless LAN.

Service Provider assigns priority to client support needs based upon the business impact of the incident. Although Service Provider will resolve all issues as quickly as possible, the following schedule outlines the maximum response times for different categories of incidents. There is a trade-off between response time and cost, and in order to keep Service Provider services affordable, we regrettably cannot guarantee the same response time for all levels of severity.

Please note that maximum response time represents time required for Service Provider to respond to the reporting party and begin troubleshooting the issue. Actual time for resolution depends on the specific nature of each incident.

Description of Incident	Users Affected	Priority Rating	Maximum Response Time	Communication Method / Follow-up
Network Device Failure	Multiple users, No work around	1	1 Hour 24/7	Direct verbal communication. Follow-up with designated contact very hour
C-level User	C-level User	1	1 Hour 24/7	Direct verbal communication. Follow-up with designated contact very hour
Critical Application	One or multiple	1	1 Hour 24/7	Direct verbal communication. Follow-up with designated contact very hour
Wireless Network Slowness	One or multiple	2	2 Business Hours	Direct verbal communication. Follow-up with designated contact very two hours
Client Device Issue	Single User	3	4 Business Hours	Direct verbal communication. Follow-up with designated contact very Four hours
Change Request	One or multiple	4	Scheduled / 3 days	Email Communication

Regularly Scheduled Wireless Tuning

In addition to standard remote and onsite support, the Subscribing Entity will receive prescheduled Bi-Annual Wireless Tuning with a dedicated engineer. The Subscribing Entity's primary care engineer will perform a Radio Frequency (RF) verification to ensure that the wireless connectivity is performing optimally as originally designed. There are some aspects of

wireless that cannot be monitored remotely so it is important that the Primary Care Engineer completes this proactive walk through as regular maintenance.

Subscribing Entity will receive an email update following each visit. The update includes a complete list of all items the engineer handled during his or her visit and includes details on anything that was found but not resolved.

Client Communications

Subscribing Entity will receive an email from Service Provider regarding the following topics:

1. Emergencies or widespread outages that the Subscribing Entity needs to know about
2. Network utilization statistics
3. Industry news and updates and how it affects the Subscribing Entity
4. Service Provider news and updates
5. Maintenance and update schedules

Scheduling and Service Tickets

Service Provider creates service tickets for all reported issues and sends automated emails to update the Subscribing Entity on the status of the ticket:

(i) Once an issue has been entered into our system, the person who reported it will receive an automated email letting him or her know that it has been received.
(ii) When the issue has been scheduled and assigned to an engineer, a second automated email will be sent identifying the name of the engineer assigned to the issue and the time that the engineer will work on it.
(iii) After the engineer has worked with the Subscribing Entity to resolve the issue, the engineer will close the ticket. The Subscribing Entity will receive an automated email saying the ticket is resolved. This email may contain a short survey asking about the experience on this particular issue, and we would appreciate a response so that we can continually gauge customer satisfaction.

Service Resolution Process

Service Provider' Support Desk is configured based on ITIL standards. ITIL is a set of concepts and best practices for IT Service firms detailing the process for key areas of service delivery like incident and escalations management, change management and application management.

All issues are reported to our Support Desk by email or phone and a service ticket is created with a unique ticket number. Our Support Desk engineers are certified in Tier 1 support. They will work the Subscribing Entities regarding issues and if they do not have the ability to resolve it, they will escalate it to our Systems Engineering Team.

Our Systems Engineering Team consists of highly skilled engineers ranging from Tier 2 to Tier 3 levels. Depending on the issue, an engineer will be assigned to work on the issue remotely or will be dispatched to the Subscribing Entity's site.

RF-Works
Service Attachment 2
Wireless as a Service (WaaS)

Support

In order to achieve the best response time and to ensure issues are properly tracked, we require that all issues be channeled through our Support Desk Team. Every service request received is given a Service Ticket Number and then triaged, scheduled, managed and resolved accordingly. Service requests can be submitted in two convenient ways:

PHONE: Dedicated Support Number Assigned at Setup

EMAIL: helpdesk@rf-works.com

For After-Hours Support and Emergencies, please call the assigned number

Service Escalations

Should the Subscribing Entity be dissatisfied with the timeliness of the resolution of the service request, send an email to management@rf-works.com. This email is sent to the Service Provider Operations Management Team, Account Management Team, and the Partners. Refer to Section 1.14 of the MCSA for any additional processes for conflict resolutions.

Support Desk Hours

Our Support Desk is fully staffed from 7am to 7pm EST Monday through Friday. During weeknights, week- end and holidays, Help Desk calls are handled by our Network Operation Teams. At all times, additional engineers from the Managed Services and Professional Services teams are on call to provide additional support to our NOC staff, if the need arises.

Change Control and Maintenance

For the purposes of this section, a Change is defined as the addition, modification, or removal of a configuration entry, service, or service component, and/or its associated elements.
Unless otherwise agreed upon between parties, all routine network maintenance and changes will be performed during the standard maintenance windows outlined below:

12:00 AM – 6:00 AM Eastern Time, Sunday

When routine maintenance is required, any Subscribing Entity impacted will be notified via email sating the time and reason for the maintenance. Following the maintenance an email will be sent to the Subscribing Entity that the maintenance has ended along with any pertinent information that may affect users as a result of any changes.

Emergency Maintenance

Any maintenance performed outside of the window of time above will be used to respond to emergency situations only. The Subscribing Entities Point of Contact will be notified by phone or email with as much advance notice as possible.

Periodic Wireless Service Review

Per Service Provider Service Attachment and during the terms of this Agreement every six months, Service Provider will provide an onsite active review of the deployment in the areas of Density and Security. Any tuning or repairs will be remediated at no additional cost to the Subscribing Entity. Service Provider will be responsible for initiating and scheduling this bi-annual event with the Subscribing Entity. After the review has been completed, Service Provider will provide a report identifying any issues identified and corrective action taken.

Optional Service Features

Outdoor Capabilities

Service Provider has the capability to design and implement an outdoor wireless or meshed network. Outdoor coverage will be priced on an individual case basis consisting of a one time implementation cost and then the ongoing monthly managed fee. (See table 2 without hardware in section 3. Service Provider Pricing & Terms)

Bridging

Service Provider offers short range MAN/Fiber alternatives and provide standard throughput scenarios. This option will be priced on an individual case basis comprised of a one-time implementation cost including hardware and the ongoing monthly-managed fee. (See table 2 in section 3. Service Provider Pricing & Terms)

Architectural Requirements

- Service Provider agrees that all state legacy devices can be managed as-is until end of life at that point Service Provider will follow the upgrade path to the Enterprise Standard, chosen by the State of Ohio, to either a Aruba or Cisco architecture.
- Service Provider agrees that Aruba, Cisco(Meraki), & HP can be managed by the Airwave solution proposed.
- The Service Provider Solution will managed multiple devices to monitor agency wireless traffic, with minimal disruption prior to transitioning to the recommended enterprise solution.
- Service Provider will manage state and agency equipment until end of life, then upgrade.
- Employee and Guest will have wireless connectivity that is seamless between locations using BYOD Security that can handle multiple manufacturers and devices.
- Service Provider has proposed a new extendible enterprise environment.

- Service Provider will utilize OIT Customer Service Center Management (ServiceNow for incidents and ordering)
- Service Provider has addressed WLAN and wired networks concurrently.
- Service Provider Solution includes PCI controls.

Solution Requirements

- Service Provider Design will adhere to the State of Ohio security controls.
- Service Provider will all devices on the wireless networks meet the set of security policy, denying access to non-conforming devices.
- Service Provider Solution includes standard set of security configurations for client devices and APs.
- Service Provider has the ability to configure/control signal strength and direction.
- Service Provider will have a single connection to the enterprise. No duel connections of wired/wireless simultaneously.
- Service Provider will have a wireless to wired network design, not bridge to local networks.
- Service Provider will not allow dual homed devices at the client level.
- Service Provider will implement wireless intrusion detection system to identify rouge devices on the network.
- Rouge Devices will be detected within 5 minutes.
- All Wireless traffic will be monitored by WIDS as it passes into the wireless network.
- Service Provider will conduct regular wireless scans to identify unauthorized WAPs and discover vulnerabilities on wireless devices.
- Service Provider will provide Firewall separation between wireless and wired networks.
- Separate secure paths for authentication WAPs, peer-to-peer networks, or ad hoc networks.
- Service Provider will use network vulnerability scanning tools to detect WAPs and discover vulnerabilities on wireless devices.
- Firewall separation between wireless and wired networks will be included in the design.
- Separate secure paths for authenticated and unauthenticated users (guest vs. employee) will be provided
- Firewall Protection for wireless components and controllers will be provided.
- Service Provider will provide DDOS protection for wireless infrastructure.
- Service Provider will provide a secure patch and maintenance cycles.
- Hardened configurations will be managed by a configuration management system.
- Service Provider will implement and report on timeout features, session management, audit logs of all logins and paired activity, automated disconnects over extended periods for connections.
- Service Provider managed Wireless networks will use authentication protocols such as EAP/TLS or PEAP.
- The Wireless clients will use strong, multifactor authentication.
- All Traffic in Service Provider Solution will use WPA2 with AES encryption.
- State of Ohio analyst will have access to monitor, view logging with alerting.
- Service Provider has the ability to monitor SNMP.

- Bluetooth will be disabled if not needed.
- There will be no infrastructure devices house wireless interface/abilities.

7. Terms and Termination

Subscription Term. Subscriptions commence on the start date specified in the applicable Order and continue for the Subscription Term specified therein, subject to relevant provisions in the MCSA, such as termination and the non-appropriation provisions. Should a Subscribing Entity elect to renew a subscription, provided this Service Attachment remains in effect or is renewed, the renewal will be at the Subscribing Entity's option and price will be according to the price listed in the Service Attachment or any associated Amendments.

8. Miscellaneous

Early Termination Charge.

As used in the MCSA, the 'Early Termination Charge' with respect to a Subscribing Entity's decision to terminate early will create a charge owed equal to three (3) months at their current monthly reoccurring charge. Any Subscribing Entity who terminates for reasons other than the biennial clause or Service provider performance, which is described as 'for convenience' in the MCSA, Agrees to pay an additional three (3) months of the monthly reoccurring charge as an 'Early Termination Charge' and forfeits any previously paid upfront fees.

Cabling Infrastructure Ownership.

In the event that cabling infrastructure was provided by Service Provider, the Subscribing Entity will own the cable infrastructure.

RF-Works
Service Attachment 2
Wireless as a Service (WaaS)

Equipment Buy-Out

At end of a Term the Subscribing Entity can purchase the 802.11 Access Points (AP) and AP accessories at fair market value or return the AP equipment & accessory assets. The assets appraisal value is determined by the length of Term selected. The Subscribing Entity's buyout option is for their Access Points and associated accessories in their facility. There is no buyout option for the shared equipment such as the wireless controller and management platform. The Subscribing Entity may require additional equipment in order for their facility's access points to be functional.

WaaS Equipment Buy-Out Structure				
	24 Month	36 Month	48 Month	60 Month
Percentage	45%	40%	30%	20%

In Witness Whereof, the Parties have executed this Service Attachment, which is effective on the date the State's duly authorized representative signs it on behalf of the State, ("Effective Date").

RF-WORKS	STATE OF OHIO, DEPARTMENT OF ADMINISTRATIVE SERVICES
Signature	Signature
James D. Portano	Robert Blair/srd
Printed Name	Printed Name
President	DAS Director Assistant Director/State CIO
Title	Title
2/23/16	2-25-2016
Date	Effective Date
20-0943384	
Federal Tax ID	

JOHN R. KASICH
GOVERNOR
STATE OF OHIO

Executive Order 2011-12K

Governing the Expenditure
of Public Funds for Offshore Services

WHEREAS, State of Ohio officials and employees must remain passionately focused on initiatives that will create and retain jobs in the United States in general and in Ohio in particular, and must do so especially during Ohio's continuing efforts to recover from the recent recession.

WHEREAS, allowing public funds to pay for services provided offshore has the potential to undermine economic development objectives in Ohio.

WHEREAS, the expenditure of public funds for services provided offshore may deprive Ohioans and other Americans of critical employment opportunities and may also undermine efforts to attract businesses to Ohio and retain them in Ohio, initiatives in which this State has invested heavily.

NOW THEREFORE, I, John R. Kasich, Governor of the State of Ohio, by virtue of the authority vested in me by the Constitution and the laws of this State, do hereby order and direct that:

1. No State Cabinet Agency, Board or Commission ("Executive Agency") shall enter into any contract which uses any public funds within its control to purchase services which will be provided outside the United States. This Executive Order applies to all purchases of services made directly by an Executive Agency and services provided by subcontractors of those providing services purchased by an Executive Agency.

2. This Executive Order will be personally provided, by the Director, Chair or other chief executive official of each Executive Agency, to the Chief Procurement Officer or other individual at that entity responsible for contracts for services.

3. The Department of Administrative Services, through Ohio's Chief Procurement Officer, shall have in place, by July 1, 2011, procedures to ensure all of the following:

    a. All agency procurements officers (APOs), or the person with equivalent duties at each Executive Agency, have standard language in all Executive Agency contracts which:

        i. Reflect this Order's prohibition on the purchase of offshore services.

ii. Require service providers or prospective service providers to:

1. Affirm that they understand and will abide by the requirements of this Order.
2. Disclose the location(s) where all services will be performed by any contractor or subcontractor.
3. Disclose the locations(s) where any state data associated with any of the services they are providing, or seek to provide, will be accessed, tested, maintained, backed-up or stored.
4. Disclose any shift in the location of any services being provided by the contractor or any subcontractor.
5. Disclose the principal location of business for the contactor and all subcontractors who are supplying services to the state under the proposed contracts.

b. All APOs confirm that all quotations, statements of work, and other such proposals for services affirm this Order's prohibition on the purchase of offshore services and include all of this Order's disclosure requirements.

i. Any such proposal for services lacking the affirmation and disclosure requirements of this Order will not be considered.
ii. Any such proposal where the performance of services is proposed to be provided at a location outside the United States by the contractor or any subcontractor will not be considered.

c. All procurement manuals, directive, policies, and procedures reflect the requirements of this Order.

d. All APOs have adequate training which addresses the terms of this Order.

4. Nothing in this Order is intended to contradict any state or federal law. In addition, this Order does not apply to:

a. Services necessary to support the efforts of the Department of Development to attract jobs and business to the state of Ohio;
b. Academic, instructional, educational, research or other services necessary to support the international missions of Ohio's public colleges and universities; or
c. Situations in which the Director of the Department of Administrative Services, or the Director's designee, shall determine that it is an emergency or that it is necessary for the State to waive some or all of the requirements of this Order. The Director shall establish standards by which Executive Agencies may request a waiver of some or all of the requirements of this Order and by which such requests will be evaluated and may be granted.

5. Executive Order 2010-09S is hereby rescinded.

I signed this Executive Order on June 21, 2011 in Columbus, Ohio and it will expire on my last day as Governor of Ohio unless rescinded before then.

John R. Kasich, Governor

ATTEST:

Jon Husted, Secretary of State

STANDARD AFFIRMATION AND DISCLOSURE FORM

EXECUTIVE ORDER 2011-12K

Governing the Expenditure of Public Funds on Offshore Services

All of the following provisions must be included in all invitations to bid, requests for proposals, State term schedules, multiple award contracts, and requests for quotations, informal quotations, and statements of work. This information is to be submitted as part of the response to any of the procurement methods listed.

By the signature affixed hereto, the Service Provider affirms, understands and will abide by the requirements of Executive Order 2011-12K. If awarded a contract, both the Service Provider and any of its subcontractors will perform no Services requested under this Agreement outside of the United States.

The Service Provider will provide all the name(s) and location(s) where Services under this Agreement will be performed in the spaces provided below or by attachment. Failure to provide this information may subject the Service Provider to sanctions. If the Service Provider will not be using subcontractors, indicate "Not Applicable" in the appropriate spaces.

1. **Principal location of business of Service Provider:**

   2172 Citygate Drive (Address) — **Columbus, Ohio 43214** (City, State, Zip)

   Name/Principal location of business of subcontractor(s):

   _____ (Name) — _____ (Address, City, State, Zip)

   _____ (Name) — _____ (Address, City, State, Zip)

2. **Location where Services will be performed by Service Provider:**

   _____ (Address) — _____ (City, State, Zip)

   Name/Location where Services will be performed by subcontractor(s):

   _____ (Name) — _____ (Address, City, State, Zip)

   _____ (Name) — _____ (Address, City, State, Zip)

3. Location where State data will be stored, accessed, tested, maintained or backed-up, by Service Provider:

(Address)	(Address, City, State, Zip)

Name/Location(s) where State data will be stored, accessed, tested, maintained or backed-up by subcontractor(s):

(Name)	(Address, City, State, Zip)
(Name)	(Address, City, State, Zip)
(Name)	(Address, City, State, Zip)
(Name)	(Address, City, State, Zip)
(Name)	(Address, City, State, Zip)

Service Provider also affirms, understands and agrees that Service Provider and its subservice Providers are under a duty to disclose to the State any change or shift in location of Services performed by Service Provider or its subcontractors before, during and after execution of any Agreement with the State. Service Provider agrees it will so notify the State immediately of any such change or shift in location of its Services. The State has the right to immediately terminate the contract, unless a duly signed waiver from the State has been attained by the Service Provider to perform the Services outside the United States.

On behalf of the Service Provider, I acknowledge that I am duly authorized to execute this Affirmation and Disclosure form and have read and understand that this form is a part of any Agreement that Service Provider may enter into with the State and is incorporated therein.

By: _____
Service Provider

Print Name: James D. Portaro

Title: President

Date: 2/23/16