

AMENDMENT #2 TO AGREEMENT FOR PROFESSIONAL SERVICES
BETWEEN
THE TRANSPORTATION AGENCY FOR MONTEREY COUNTY
AND
ALVAREZ TECHNOLOGY GROUP

THIS AMENDMENT No. 2 to the agreement dated December 4, 2019, between the Transportation Agency for Monterey County, hereinafter referred to as "TAMC," and Alvarez Technology Group, a California corporation, hereinafter referred to as "Consultant," is hereby entered into between TAMC and the Consultant.

RECITALS:

- A. **WHEREAS**, TAMC and Consultant entered into an agreement for professional services on December 4, 2019, hereinafter referred to as "Agreement," to provide managed information technology services;
- B. **WHEREAS**, TAMC and Consultant entered into Amendment #1 to the Agreement on August 26, 2020 to increase the not-to-exceed amount by Three Thousand Seven Hundred Thirty-five Dollars (\$3,735), for a total contract not-to-exceed amount One Hundred Fifty Thousand Six Hundred Dollars (\$150,600), to cover additional costs related to the Agency's Microsoft Azure cloud server;
- C. **WHEREAS**, TAMC is seeking, and Consultant is able to provide, additional cybersecurity protections consistent with the National Institute of Standards and Technology cybersecurity framework to fortify the Agency's network against potential attacks and provide additional staff training;
- D. **WHEREAS**, TAMC and Consultant desire to amend the Agreement to include these services in the scope of work and cover the additional costs.

NOW, THEREFORE, the parties agree to amend the Agreement as follows:

1. **SCOPE OF WORK**

The Scope of Work attached to the Agreement as Attachment A is hereby replaced with the Scope of Work designated Exhibit A-1 and dated May 26, 2021 and shall be effective upon execution. Exhibit A-1 is attached hereto as Exhibit A-1.

2. **TOTAL COMPENSATION**

The total compensation to be paid pursuant to this Agreement as amended shall be increased by Twenty-Five Thousand Six Hundred Dollars (\$25,600), and the total contract shall not exceed One Hundred Seventy-Six Thousand Two Hundred Dollars (\$176,200). All references to the amount \$150,600 shall be replaced with the amount \$176,200. The Budget attached to the Agreement as Exhibit B is hereby replaced with

the Budget designated Exhibit B-2 dated May 26, 2021 and shall be effective upon execution. Exhibit B-2 is attached hereto as Exhibit B-2. The total compensation to be paid pursuant to this Agreement as amended shall not exceed

3. REMAINDER OF TERMS UNCHANGED

All other terms of the Agreement remain in full effect.

An executed copy of this Amendment No. 2 shall be attached to the Agreement and shall be incorporated as if fully set forth therein.

IN WITNESS WHEREOF, the parties hereto have executed this Amendment No. 2 to the Agreement with Consultant.

TAMC

Alvarez Technology Group

By: _____
Debra L. Hale
Executive Director

By: _____
Name:
Title:

Dated: _____

Dated: _____

By: _____
Name:
Title:

Dated: _____

INSTRUCTIONS: If Consultant is a corporation (including limited liability and nonprofit corporations), the full legal name of the corporation shall be set forth together with the signatures of two specified officers. If Consultant is a partnership, the name of the partnership shall be set forth together with the signature of a partner with authority to execute this Agreement on behalf of the partnership. If Consultant is contracting in an individual capacity, the individual shall set forth the name of his or her business, if any, and shall personally sign the Agreement.

Approved as to form:

TAMC Counsel

EXHIBIT A-1: Scope of Work

May 26, 2021

Background: The Transportation Agency's current computer hardware consists of:

- One server running Windows Small Business Server 2008;
- Eighteen Lenovo ThinkStation computers running Windows 7 Professional;
- One Sharp SmartBoard running Windows 7 Professional;
- Two laptops, which are shared amongst the staff, running Windows 7 Professional;
- Two networked printers; and
- Three wireless access points.

The Transportation Agency currently has an Office 365 subscription, which includes email service and licenses for the Microsoft Office applications. In addition, the network shared drive on the server is synchronized with Microsoft SharePoint for backup and remote file access. Staff also has remote access to their workstations through a Virtual Private Network and Microsoft Remote Desktop Connection.

The Transportation Agency's phone system is monitored and maintained by The Maynard Group. The Consultant shall coordinate with them to resolve any network related issues affecting the phone service.

Required Services:

REMOTE SERVICES AGREEMENT

1. **Staff Technology Support:** The Consultant's help center and engineering support team will be available to assist all TAMC employees with server, workstation, network, and mobile device support Monday through Friday 6:00 AM - 6:00 PM. If an issue cannot be resolved remotely a senior engineer will be dispatched onsite.
2. **Network Monitoring and Management:** The Consultant's help center technicians will monitor the health and welfare of all manageable network workstations and devices using a Network Monitoring and Management device. The networked workstations and devices will be configured to send alerts to the help center in case of significant problems. Help center technicians will monitor the devices daily, responding automatically to any alerts and resolving those issues remotely, if possible. If onsite service is required, TAMC will be contacted to authorize the onsite work.
3. **Server Platform Monitoring:** The Consultant's technicians will monitor the health and welfare of the server or servers using the network monitoring and management appliance. The network monitoring and management appliance will alert the consultant(s) to any significant problem that arises on the servers and they will respond during normal working hours of 7:30 AM to 5:30 PM, Monday through Friday, excluding published holidays. In addition to responding to alerts generated by the network monitoring and management appliance, the Transportation Agency may contact the consultant(s) at any time for server-side assistance. Consultant's technicians will monitor the servers daily, responding automatically to any server alerts and resolving

those issues remotely, if possible. If onsite service is required, TAMC will be contacted to authorize the onsite work.

4. Business Continuity Server Backup: The Consultant will maintain a software and hardware solution to allow real-time, image backup of each server so that in case of a catastrophic hardware failure that incapacitates the server for any length of time, the consultant can restore the server without data loss. The Consultant will also ensure that the cloud-based backup system (SharePoint) works as intended. If problems arise, they will be resolved remotely. If onsite service is required, TAMC will be contacted to authorize the onsite work.
5. User Management: At the direction of TAMC, the Consultant will add, edit, or delete users, manage user access to server resources, and monitor user data on the servers.
6. Server-based Email Management: The Consultant will manage and monitor the health of cloud-based email system (Office 365), as well as adding, editing, or deleting users, managing organization-wide email lists and user quotas.
7. Routine Maintenance: The Consultant will conduct server-side routine maintenance, such as deleting temporary files, defragmentation and managing file locations is included.
8. Patch Management: The Consultant will manage the installation of required operating system patches on the servers and workstations, ensuring vital security updates and performance-enhancing upgrades are installed as they are made available.
9. Application Management: Any applications installed on the server will be managed remotely by the Consultant.
10. Virus/Spyware/Spam Management: The Consultant shall provide antivirus software that runs on the server and all workstations, which will be managed remotely by the consultant.
11. Disaster Prevention and Disaster Recovery: The Consultant will use industry "best practices" to implement disaster prevention systems to ensure optimal performance of the server or servers. In case of a disaster such as disk failure or virus outbreak, consultant will provide disaster recovery assistance.
12. Monthly Reporting: TAMC will receive detailed monthly reports detailing all the work done by Consultant's technicians and engineers.
13. Custom Client Portal: TAMC will have access to an online portal customized to allow access to service information and to check the status of ongoing issues.
14. Annual IT Evaluation: After the contract is in effect, once a year on the anniversary of the contract or on a mutually agreeable date, Consultant will review the IT infrastructure, conduct targeted interviews and create a detailed annual report for TAMC on the status of the existing technology environment and recommend future enhancements.
15. Response Time: During normal business hours, incoming calls to the Consultant hotline will be answered at that time or a return call placed within 30 minutes if a message is left. Consultant will guarantee a response to all critical alerts within two (2) hours of

notification and to client requests within one (1) hour of initial contact. Onsite response is assured next business day, when necessary.

16. Mobile Device Management and Setup: Consultant will setup mobile devices to work on the TAMC network for receipt and delivery of email, calendar, and contacts, as well as remote connections to user workstations from their mobile devices.
17. Wireless Network Management: Consultant will setup, maintain, and keep secure TAMC's wireless (wifi) network and solve problems related to connectivity and wireless internet coverage.
18. Virtual Private Network Management: Consultant will setup, maintain, and keep secure TAMC's Virtual Private Network (VPN) and solve problems related to connectivity and remote desktop connection.
19. Third-Party Vendor Management: The Consultant will collaborate with and manage other technology and software providers to ensure TAMC is being provided the best service possible. The consultant service team will work with these providers to resolve any network problems.

CYBERPROTECT PREMIUM

1. CyberProtect Premium is designed to fulfill the requirements of the National Institute for Standards and Technology Cybersecurity Framework recommended to be adopted by all organizations, especially government agencies.

The NIST CSF consists of five key components and represents a constantly changing continuum, recognizing that the threat landscape evolves, that networks and people change, and that the framework must be nimble enough to adapt over time:

- **Identify**: An organization needs to understand not only what they are protecting (assets) but also what they are protecting against (threats) and their risk profile.
 - **Protect**: An organization must implement robust systems to protect their assets, including educating users.
 - **Detect**: An organization can't simply build a wall around their systems and hope to keep the threats out. They must assume that threats will penetrate those walls and so therefore must have a way to detect those breaches.
 - **Respond**: An organization must have a document plan of action in case a breach occurs, an Incident Response Plan that outlines the steps and resources needed once a breach occurs.
 - **Recover**: Finally, an organization must be able to recover from a breach in a timely fashion in order to continue to operate, including ensuring that they have good backups of all their critical data.
2. Consultant will provide consulting with TAMC staff to adopt the NIST framework and implement the tools, services and monitoring to comply with the framework.
 3. ATG will deliver ongoing tools and support that support each specific areas of the NIST framework and will continuously monitor and adjust our services to maintain the ever evolving threat landscape as recommended by NIST.
 4. This chart outlines the current NIST framework and the products and services that are aligned for each area:

<u>NIST CSE Component</u>	<u>CyberProtect™ Premium Services</u>
<u>Identity</u>	<ul style="list-style-type: none"> • <u>Real-time asset tracking</u> • <u>Internal and external vulnerability scans</u> • <u>Threat monitoring</u> • <u>Annual Cybersecurity Risk Assessment</u>
<u>Protect</u>	<ul style="list-style-type: none"> • <u>Endpoint malware protection</u> • <u>Block access to known or suspected bad Internet sites</u> • <u>Content filtering</u> • <u>Email filtering for spam and malware</u> • <u>Managed user cybersecurity training</u> • <u>Managed firewall</u>
<u>Detect</u>	<ul style="list-style-type: none"> • <u>Managed detection and response</u> • <u>Network and endpoint scanning</u> • <u>Alerting of suspicious activities on the network</u> • <u>Security Operations Center</u>
<u>Respond</u>	<ul style="list-style-type: none"> • <u>Automated Incident Response</u> • <u>Access to Security Operations Center cybertechs</u>
<u>Recover</u>	<ul style="list-style-type: none"> • <u>Managed Business Continuity and Backup of on-premises servers and Microsoft 365</u>

OPTIONAL TASKS

1. Workstation 5-Year Lease Program: The Consultant will lease workstations to the Transportation Agency, with monthly payments over a five-year period. The consultant will be responsible for maintenance of the hardware and software. The following hardware, with extended warranties for each covering the entire five-year lease program, would be required:
 - a. One workstation capable of running Auto-CAD, with Windows 10;
 - b. Seventeen workstations capable of running standard Microsoft Office, Esri ArcGIS, and Adobe design (e.g. Photoshop and Illustrator) applications, with Windows 10; and
 - c. Two laptops capable of running standard Microsoft Office applications, with Windows 10.

2. Server Migration to Cloud-Based Microsoft Azure / SharePoint: The consultant will migrate the Transportation Agency's current on-site server to a Microsoft Azure virtual machine, with print server capabilities. This will include staff log-in via Active Directory and direct access to shared files in SharePoint through Windows Explorer on the workstation. Consultant will be required to plan the migration, set up and test, schedule a time in coordination with the Transportation Agency to conduct the change-over from the on-site server to the new Azure cloud-based server, and provide staff training.

EXHIBIT B-2: Budget
May 26, 2021

Fee Schedule

TASK	ONE-TIME COSTS	MONTHLY	TOTAL
REQUIRED SERVICES:			
- REMOTE SERVICE AGREEMENT		\$1,450.00	\$87,000.00
<u>- CYBERPROTECT PREMIUM (44 months)</u>	<u>\$3,600.00</u>	<u>\$500.00</u>	<u>\$25,600.00</u>
OPTIONAL TASK 1:			
- WORKSTATION LEASE	\$1,772.00	\$643.00	\$40,352.00
OPTIONAL TASK 2:			
- SERVER MIGRATION	\$7,813.00		\$7,813.00
- AZURE SUBSCRIPTION	\$335.00	\$200.00	\$12,135.00
- SHAREPOINT BACKUP		\$55.00	\$3,300.00
TOTAL WITH OPTIONAL TASKS:			\$176,200.00

Optional Tasks

Consultant shall not commence work or submit any invoices for the identified optional tasks unless and until TAMC has issued a notice to proceed for such work.

After Hours Support

The agreement provides access to after-hours support but does not cover the charge for after-hours work. Any work performed after hours will be billed at the discounted rate of \$200 per hour.

Projects

TAMC may occasionally require services outside of the specific terms of this agreement. Those services will be called "Projects" and Consultant will provide a detailed scope of work and labor quote. TAMC will sign off on the quote before any work is performed and understand that a separate invoice will be generated for the Project work. The discounted billing fee for all work outside the contract is \$150 per hour. Any and all such "Project" work is subject to the total "not to exceed" amount of this contract.