PALMDALE WATER DISTRICT
A CENTURY OF SERVICE

EST. 1918

BOARD OF DIRECTORS

W. SCOTT KELLERMAN
Division 1

DON WILSON
Division 2

CYNTHIA SANCHEZ
Division 3

KATHY MAC LAREN-GOMEZ
Division 4

VINCENT DINO
Division 5

DENNIS D. LaMOREAUX
General Manager

ALESHIRE & WYNDER LLP
Attorneys

ACWA
PROUD MEMBER

June 5, 2024

AGENDA FOR REGULAR MEETING OF THE BOARD OF DIRECTORS OF THE PALMDALE WATER DISTRICT TO BE HELD AT 2029 EAST AVENUE Q, PALMDALE

MONDAY, JUNE 10, 2024

6:00 p.m.

NOTES: To comply with the Americans with Disabilities Act, to participate in any Board meeting please contact Danielle Henry at 661-947-4111 x1059 at least 48 hours prior to a Board meeting to inform us of your needs and to determine if accommodation is feasible.

Additionally, an interpreter will be made available to assist the public in making **comments** under Agenda Item No. 4 and any action items where public input is offered during the meeting if requested at least 48 hours before the meeting. Please call Danielle Henry at 661-947-4111 x1059 with your request. (PWD Rules and Regulations Section 4.03.1 (c))

Adicionalmente, un intérprete estará disponible para ayudar al público a hacer **comentarios** bajo la sección No. 4 en la agenda y cualquier elemento de acción donde se ofrece comentarios al público durante la reunión, siempre y cuando se solicite con 48 horas de anticipación de la junta directiva. Por favor de llamar Danielle Henry al 661-947-4111 x1059 con su solicitud. (PWD reglas y reglamentos sección 4.03.1 (c))

Agenda item materials, as well as materials related to agenda items submitted after distribution of the agenda packets, are available for public review at the District's office located at 2029 East Avenue Q, Palmdale or on the District's website at https://www.palmdalewater.org/governance/board-activity/2023-meeting-agendas-minutes/ (Government Code Section 54957.5). Please call Danielle Henry at 661-947-4111 x1059 for public review of materials.

PUBLIC COMMENT GUIDELINES: **The prescribed time limit per speaker is three-minutes. Please refrain from public displays or outbursts such as unsolicited applause, comments, or cheering. Any disruptive activities that substantially interfere with the ability of the District to conduct its meeting will not be permitted, and offenders will be requested to leave the meeting. (PWD Rules and Regulations, Appendix DD, Sec. IV.A.)**

Each item on the agenda shall be deemed to include any appropriate motion, resolution, or ordinance to take action on any item.

1) Pledge of Allegiance/Moment of Silence.

2) Roll Call.

3) Adoption of Agenda.

4) Public comments for non-agenda items.

5) Presentations:

5.1) None at This Time.

6) Action Items - Consent Calendar (The public shall have an opportunity to comment on any action item on the Consent Calendar as the Consent Calendar is considered collectively by the Board of Directors prior to action being taken.)

6.1) Approval of Minutes of Regular Board Meeting held May 28, 2024.

6.2) Payment of Bills for June 10, 2024.

6.3) Approval of Amendment No. 5 with Hazen and Sawyer for Professional Services for the Design, Permitting, and Construction Inspection for the Drilling and Equipping of Well 36. ($95,892.00 – Budgeted – Project No. 20-622 – Engineering Manager Rogers)

7) Action Items - Action Calendar (The public shall have an opportunity to comment on any action item as each item is considered by the Board of Directors prior to action being taken.)

7.1) Consideration and Possible Action on SharePoint/Teams Migration. ($32,595.00 – Non-Budgeted – Information Technology Manager Stanton)

7.2) Consideration and Possible Action on Implementation of Multi-Factor Authentication (MFA). ($15,800.00 – Non-Budgeted – Information Technology Manager Stanton)

7.3) Consideration and Possible Action on Approval of Amendment No. 2 with AECOM, Inc. for Professional Services for the Littlerock Dam Remediating Maintenance Issues. ($83,135.75 – Budgeted – Project No. 23-607 – Engineering Manager Rogers)

7.4) Consideration and Possible Action on Authorization of the Following Conferences, Seminars, and Training Sessions for Board and Staff Attendance Within Budget Amounts Previously Approved in the 2024 Budget:

a) BizFed Institute 3rd Annual Water Resiliency Forum: Water As An Economic Engine to be held June 26, 2024 in Los Angeles.

b) AV EDGE 2024 Installation Dinner to be held July 11, 2024 in Palmdale.

8) Information Items:

8.1) Reports of Directors:

a) Standing Committees; Organization Appointments; Agency Liaisons:

1) Special District Association North Los Angeles County (SDANLAC) Membership Luncheon – May 29. (Director Dino, Board Liaison)

2) Outreach Committee Meeting – May 30. (Director Dino, Chair/Director Sanchez/Director Wilson, Alt.)

b) General Meetings Reports of Directors.

8.2) Report of General Manager.

8.3) Report of General Counsel.

9) Closed Session Under:

  9.1) Government Code §54957(b)(1):

    a) Public Employee Performance Evaluation: General Manager.

10) Board Members' Requests for Future Agenda Items.

11) Adjournment.

Dennis D. LaMoreaux

DENNIS D. LaMOREAUX,
General Manager

DDL/dh

AGENDA ITEM NO. 6.3

BOARD MEMORANDUM

DATE: June 10, 2024

TO: **BOARD OF DIRECTORS**

FROM: Mr. Scott Rogers, Engineering Manager

VIA: Mr. Dennis D. LaMoreaux, General Manager

RE: ***APPROVAL OF AMENDMENT NO. 5 WITH HAZEN AND SAWYER FOR PROFESSIONAL SERVICES FOR THE DESIGN, PERMITTING, AND CONSTRUCTION INSPECTION FOR THE DRILLING AND EQUIPPING OF WELL 36. ($95,892.00 – BUDGETED – PROJECT NO. 20-622 – ENGINEERING MANAGER ROGERS)***

Recommendation:

Staff recommends that the Board approve Amendment No. 5 with Hazen and Sawyer for Professional Services for the Design, Permitting, and Construction Inspection for the Drilling and Equipping of Well 36.

Alternative Options:

The alternative is to not approve Hazen and Sawyer's proposal.

Impact of Taking No Action:

The District would benefit from beginning to completion for the construction of Well 36 Equipping. The impact of taking no action would result in lack of professional construction management and inspection during construction.

Background:

The original contract with Hazen and Sawyer does not include electrical inspection, instrument installation inspection, or testing. Amendment No. 5 will include Hazen and Sawyer's subconsultant - Ardurra's inspection services including electrical inspection, instrument installation inspection, and testing in the amount of $116,892.00 and of this amount $31,000.00 was included in the original contract amount. Therefore, $85,892.00 represents the additional amount of the construction inspection services and an additional $10,000 to cover the additional project management activities by Hazen and Sawyer due to the extended schedule.

Strategic Plan Initiative/Mission Statement:

This item is under Strategic Initiative No. 1- Water Resource Reliability.

This item directly relates to the District's Mission Statement.

Supporting Documents:

- Hazen and Sawyer, P.C. Proposal.
- Ardurra Group, Inc. Proposal.

Hazen

Hazen and Sawyer
7700 Irvine Center Drive, Suite 200
Irvine, CA 92618 • 949.557.8549

May 24, 2024

Mr. Kevin Yao, P.E.
Senior Engineer
Palmdale Water District
2029 East Avenue Q.
Palmdale, CA 93550

Re: Well 36 Equipping Additional Services - Amendment 4

Dear Kevin:

Following up on your request, we are pleased to submit this request for an amendment to our contract for the subject project. This request is in response to the District's request to add Ardurra to the project team to conduct construction inspection services. Ardurra's proposal to provide construction inspection services is attached to this letter. In summary, their estimate to provide their services is a not-to-exceed amount of $116,892. In our original contract from April of 2021, there is $31,000 allotted for construction inspection services. So, the additional estimated amount is $85,892.

Given the significant schedule delays experienced on the project, we have depleted our project management budget of $52,190. Therefore, we respectfully request an additional $10,000 be included in this amendment to cover the additional project management activities due to the extended schedule.

In summary, we request a contract amendment in the amount of $95,892.

Should you have any questions, please contact me at (916) 769-8753 or via e-mail at DRJones@HazenandSawyer.com.

Very truly yours,

Dave Jones

Dave Jones, PE
Project Director

Cc: Scott Rogers/PWD
Steve Conner/Hazen

ARDURRA

May 20, 2024

Mr. Dave Jones, PE
Vice President
Hazen and Sawyer
drjones@hazenandsawyer.com

REFERENCE: PROPOSAL TO PROVIDE INSPECTION SERVICES FOR EQUIPPING OF WELL 36, PALMDALE WATER DISTRICT

Dear Mr. Jones,

Pursuant to our conversations, Ardurra Group, Inc. (Ardurra) is pleased to present our scope and budget to provide inspection services for Palmdale Water District's Equipping of Well 36. As part of this proposal, we have presented our proposed inspector to be assigned to the project and a proposed fee.

TEAM

Ardurra proposes **Scott Adamson, PE** as Sr. Construction Manager and **Richard Frye** as Sr. Construction Inspector. This is a seasoned team of construction engineering professionals with a long history of filling theses roles on similar projects. We have also included **UES** to provide inspection services for electrical installations.

SCOPE OF SERVICES

Ardurra proposes to attend and provide inspection and observation for key elements of the project as shown below:

CONSTRUCTION COORDINATION AND MEETINGS

- Pre-Construction Meeting and Site Visit
- Weekly Progress Meetings

CRITICAL ACTIVITIES AS-NEEDED OBSERVATION

- Underground Piping and Hydrostatic Testing
- Above-Ground Piping and Hydrostatic Testing
- Mechanical Inspections of Equipment Installations: Pump & Motor; Gauges; Valves
- Structural Inspection: Reinforcement & Concrete for Pump Foundation, Pump House Floor & Walls
- Architectural Inspection: Pump House Walls, Doors, Louvered Openings, and Roof
- HVAC Installations and Testing

- Electrical Equipment, Cable & Raceway Installations and Startup
- Instrumentation Install and Testing

SUBSTANTIAL AND FINAL COMPLETION REVIEW

- Develop a Punch List
- Conduct a Final Inspection with Engineer and Owner
- Review and Approve Final As-builts
- Recommend Final Payment and Substantial Completion

Inspection services will be provided on a periodic basis only during the critical periods identified above. Should the District want daily construction monitoring additional budget will need to be negotiated.

FEE

Per Hazen and Sawyer's direction, we have based our proposed fee on providing inspection and oversight for key elements of the project. Should Ardurra be requested to provide additional services, Ardurra will request additional budget. Based on our understanding of the level of effort requested we have developed the fee table below indicating billing rates and the number of hours anticipated for each of the personnel categories.

Palmdale Water District Well 36 Equipping	Sr. Construction Manager	Sr. Construction Inspector	Electrical Inspection	Total
Rates [1]	$260	$204	$ 174.00	
Construction Coordination and Meetings				
Pre-Construction Meeting and Site Visit	4	4		$ 1,856.00
Bi-Weekly Progress Meetings	10	32	6	$ 10,172.00
				$ 12,028.00
Critical Acitivities As-Needed Observation				
Underground Piping and Hydrostatic Testing		24		$ 4,896.00
Above-Ground Piping and Hydrostatic Testing		24		$ 4,896.00
Mechanical Inspections of Equipment Installations: Pump & Motor, Guages, Valves		24		$ 4,896.00
Structural Inspection: Reinforcement & Concrete for Pump Foundation, Pump House		24		$ 4,896.00
Architectural Inspections: Pump House Walls, Doors, Louvered Openings, and Roof		24		$ 4,896.00
HVAC Installation and Testing		24		$ 4,896.00
Electrical Equipment, Cable, & Raceway		24	200	$ 39,696.00
Instrument Install & Testing	100	24		$ 30,896.00
				$ 99,968.00
Substantial and Final Completion Review				
Develop a Punch-list		8		$ 1,632.00
Conduct a Final Inspection with Engineer and Owner		4		$ 816.00
Review and Approve Final As-builts		8		$ 1,632.00
Recomment Final Payment and Substantial Completion		4		$ 816.00
				$ 4,896.00
Total Time	114	252	206	
Total Project Cost	$ 29,640	$ 51,408	$ 35,844	$ 116,892.00

Footnotes

1. Field personnel rates are inclusive of vehicle, mileage, phone, computer, etc. Inspection rates shown are for prevailing wage projects.
2. Subconsultant Fees are Invoiced At Cost Plus 5% Mark-up.

Ardurra's total fee of **$116,892.00** is all-inclusive of vehicle, mileage, computer, and all other necessary equipment and materials to perform the required tasks. A breakdown of the fees is shown on the Work Breakdown attachment.

We have presented a budget that adequately provides the level of service we believe Hazen and Sawyer is looking for. We would be more than happy to sit down with Hazen and Sawyer and review the proposed budget to see if there are areas within the scope that can be further refined, especially when in receipt of the contractor's approved baseline schedule.

We sincerely appreciate the opportunity to provide this proposal to assist Hazen and Sawyer and Palmdale Water District with this project. Please contact me at (858) 243-4977 should you have any questions or need further information.

Respectfully Submitted,
Ardurra Group, Inc.

Scott

Scott Adamson, PE
Construction Management Group Leader

NOTES

1. Prevailing Wage Rates are subject to increases pursuant to the State of California's Department of Industrial Relations Wage Rate Determinations. Ardurra's Billing Rates will increase in proportion to the DIR increase, plus overhead and profit.

2. **Inspection Overtime:** No weekday, Saturday, holiday or Sunday work is assumed or included. Should any weekday or Saturday overtime inspection be required, it is charged at 1.4 times the rate shown. For Sundays and holidays inspection, billing rates are 1.7 times the above rate, upon the client's prior written approval.

3. The above hourly inspector rates include wages, fringe and general and administrative overhead and fee, as well as typical supplies, tools and equipment required to perform services.

4. The following minimum callout applies to inspection staff, in accordance with Industrial Welfare Commission Order No. 16-2001.
   - Cancellation of 8 hours scheduled inspection after inspector's arrival on site: 4-hour minimum
   - Cancellation of 4 hours scheduled inspection after inspector's arrival on site: 2-hour minimum

5. For contracts involving public works inspection services, Ardurra requires the awarding public agency to complete DIR form PWC-100 solely for Ardurra as the prime contractor specific to the awarded contract name and amount. A half-hour per week, per inspector labor compliance charge will be billed for all Prevailing Wage inspection assignments and is included with our project controls fee.

6. **Escalation:** The rates in this fee proposal are effective through December 31, 2024, except as noted above for Prevailing Wage covered classifications. Should the contract duration be extended beyond December 31, 2024, rates will be subject to prevailing wage increases as noted above, non-prevailing wage salary increases and overhead increases based on current Los Angeles-Riverside-Orange County Consumer Price Index to accommodate inflationary trends, salary adjustments and the general cost of doing business, as mutually agreeable to the parties and approved via contract amendment prior to implementing higher rates. In the event the contract is subject to delays that are beyond Ardurra's control, a request will be made to increase the billing rates to Ardurra's current standard rates, and the client will use all reasonable effort to allow such billing rate increase.

7. **Limitations:** The projected fee is based on the number of estimated working days required for the completion of the work. The estimate may be affected by:
   - Working time duration in excess of the duration indicated above
   - Contractor and subcontractor's efficiency and sequencing of events
   - Unexpected subsurface conditions
   - Unforeseen delays beyond Ardurra's control

8. **Exclusions to Scope and Fee:** The following items are specifically excluded:
   - Legal advice
   - Temporary field office facilities, equipment, furniture, utilities and/or services
   - Engineering support
   - Hazardous materials monitoring and/or testing

- Acceptance and/or Independent Assurance Sampling and Testing (IAST) services
- Specialized software other than Procore, MS Office Suite, MS Project and/or P6

BOARD MEMORANDUM

DATE: June 10, 2024

TO: **BOARD OF DIRECTORS**

FROM: Mr. Jim Stanton, Information Technology Manager

VIA: Mr. Dennis D. LaMoreaux, General Manager

RE: ***CONSIDERATION AND POSSIBLE ACTION ON SHAREPOINT/TEAMS MIGRATION. ($32,595.00 – NON-BUDGETED – INFORMATION TECHNOLOGY MANAGER STANTON)***

Recommendation:

Staff recommends that the Board approve migrating on-premises file shares to SharePoint/Teams Sites.

Alternative Options:

The Board can choose for the District to remain as is with the on-premises file shares.

Impact of Taking No Action:

The impact of taking no action is reduced efficiency and employee frustration.

Background:

Workplace collaboration is at an all-time high and our current configuration highly restricts that. Our current system of on-premises folder and file shares restrict access to those files to a single user. Finance has approached IT and requested a solution that will allow multiple users to be able to access, and modify, existing documents at the same time. The solution is to migrate their department folders and files from on premise file share to cloud based SharePoint and Teams Sites.

Migration to SharePoint Benefits:

1. Saving Money

   Avoid unnecessary spending on apps and tools by using SharePoint as the primary productivity tool for professional needs.

2. Scalability

   The scalability of the tool allows the District to budget costs towards productivity tools.

3. Data Security

   Governments and big organizations trust the SharePoint sites and files are routinely backed up and stored in multiple data centers. Data center locations and back schedules can be chosen by the District.

4. Multipurpose Usage

   A higher level of flexibility and multipurpose utility means that the District can keep using SharePoint as the principal productivity tool while we keep changing roles or creative skills. The District can use a template when one project ends, and you need to start another, similar one. The budget can be minimized by avoiding multiple app purchases.

5. Increased Productivity

   As a District leader, how many hours per week do you think is spent digging through archives and shares to find a file? Whether you're searching inside of a filing cabinet or clicking through an endless sea of folders, it can be mind-numbing and frustrating to devote time during the busy workday to a wild goose chase.

   When all documents are consolidated onto a SharePoint platform, the District can organize each SharePoint site to include only the folders and subfolders needed. This way, users can go straight to the source and will have more time for core responsibilities.

   When users aren't spinning their wheels looking for the data they need, they're able to devote more time to their core responsibilities.

6. Collaboration

   SharePoint is a highly flexible and scalable platform for collaboration with internal or external resources. A central admin user can assign different levels of access permission to individual users of team sites.

Multiple users on a team can work on a single file in a real-time scenario without facing any latency. Another significant function of SharePoint collaboration is to keep flowing decluttered information throughout the sites and subsites. It helps individuals stay updated about the project without going through multiple emails, missed chats, video calls, etc. SharePoint online can be accessed from any device, but it also lets you share documents and files with those in your organization who need access to them, and everyone with an internet connection can access these files from anywhere. In an area that doesn't have Internet, you can still work on your files while you're offline and they'll sync to SharePoint when you get back in an area with Internet connectivity. District team members can work together on the same document at the same time, plus chat with co-collaborators right from within the document, and, if it becomes necessary, they can also revert to a previous version of the file. SharePoint Online keeps a record of the various versions that have been created or worked on.

For the initial migration we would like to use our current Microsoft Vendor, Citrin Cooperman, to assist us with successfully planning and moving the Finance department's current folder and files to SharePoint and Teams sites. Finance currently has the most difficult folder and permissions configuration of all District departments. The knowledge gained from Citrin Cooperman will give IT staff the knowledge and skills necessary to successfully migrate the remaining Departments. The only possible exception to this might be the current Z: drive, District Wide share. Cost for Citrin Cooperman assistance is Twenty-Four Thousand One-Hundred Dollars ($24,100.00).

The software required for the migration is ShareGate. This software will help in the planning and actual migration to SharePoint / Teams sites. Cost Eight Thousand Four-Hundred Ninety-five Dollars ($8,465.00)

Total Project Cost: Thirty-Two Thousand Five-hundred Ninety-Five Dollars ($32,595.00)

Strategic Plan Initiative/Mission Statement:

This item is under Strategic Initiative No. 3 – Systems Efficiency.
This item directly relates to the District's Mission Statement.

Budget:

This item has a one-time cost of approximately Twenty-Four Thousand One-Hundred dollars for vender assistance and Eight Thousand Four-Hundred Ninety-Five dollars software, total project cost Thirty-Two Thousand Five Hundred Ninety-Five dollars ($32,595.00) and is unbudgeted.

Supporting Documents:

- Citrin Cooperman SOW

CITRINCOOPERMAN®

STATEMENT OF WORK

CLIENT	TITLE	SOW	DATE	REVISION
Palmdale Water	Migration to Teams, OneDrive, SharePoint	PAL01-2001	May 22nd 2024	1.0

This Statement of Work, Number PAL01-2001 dated May 22nd 2024 (“SOW”) is entered into by the parties under the provisions of the Consulting Services Agreement dated 10/16/15 (“CSA”) by and between FMT Consultants LLC and Palmdale Water (“Client”) which was assigned to Citrin Cooperman Advisors LLC (“CCA”) on 8/9/23, and, except as otherwise provided in this SOW, all applicable provisions of the CSA are incorporated into this SOW by this reference. In the event there is a conflict between the terms and conditions of the CSA and the SOW, the terms and conditions of the SOW shall control.

This SOW shall remain active and in effect until one of the following conditions have been completed:

1) The allocated Services value has been consumed; or

2) Twelve (12) months have passed from the date in the signature block

Services To Be Performed

CCA will assist client with configuration of Microsoft Teams Migration.

CCA will conform to commercially reasonable standards and practices in the performance of its services under this SOW. All services and deliverables performed or provided by CCA shall be deemed accepted, and payment therefor shall be due and payable in full, if not rejected in writing within thirty (30) days of Client’s receipt of the invoice for such services or deliverables. If Client reasonably rejects any service or deliverable performed or provided by CCA, and CCA determines that correction of the rejected service or deliverable is necessary, CCA will correct and resubmit the same within a reasonable time.

Services Costs

Subject to the CSA provisions regarding the amount of Services and estimates, and based upon the time and estimates and resource assignments in the project plan that follows and assumptions below, CCA estimates the services costs to be $24,100.00. CCA will calculate Service value using the rates listed in the following Table of Rates and Resources.

“Citrin Cooperman” is the brand under which Citrin Cooperman & Company, LLP, a licensed independent CPA firm, and Citrin Cooperman Advisors, LLC serve clients’ business needs. The two firms operate as separate legal entities in an alternative practice structure. Citrin Cooperman is an independent member of Moore North America, which is itself a regional member of Moore Global Network Limited (MGNL).

Rates and Resources	Standard Rate*	Est. Hours
Director	$325	46.0
Senior Consultant, Project Manager	$225	14.0
Consultant	$150	40.0

*Work performed during non-business hours at the request of the Client, after 5:00 p.m. Monday through Friday or any time on Saturday or Sunday is charged at 1.5 times the consultant's standard rate. Should a particular CCA resource be unavailable when required on Client's project, CCA reserves the right to replace said resource with a suitable replacement.

Travel time is not included in the above project costs and will be billed at fifty (50%) percent of the resources standard hourly rate. Client will also reimburse CCA for reasonable travel expenses incurred in connection with this project.

CCA will provide Client with itemized invoices detailing Services rendered and associated expenses.

Services rates listed in the table above are valid at the time of SOW execution. In the event CCA updates standard Services rates during the SOW effective period, CCA will provide 30-days advance notice to Client of the impending rate increase. At that time, the new rates will become effective and FMT will apply the new rates for the remainder of the authorized Services specific to this SOW.

Per the terms of the CSA, client will pay a one-time retention fee of $2,410.00 prior to Services work being performed, which will be invoiced and due upon signature of this Statement of Work.

Project Assumptions

- CCA has prepared a project plan for Client's project. The tasks and estimated CCA work hours are based upon CCA's understanding of Client's requirements, as of the date of this SOW, and the assumptions below. Client's solution may require additional work hours in order to be completed.
- Client will identify an internal resource to assist with overall management and coordination of the services.
- Client's assigned resources will actively participate during the project.
- CCA will be listed as software Partner of Record to better assist client with system support and licensing.
- Project covers analysis of inventory and migration of content for Finance Department ~120GB
- Rearchitecting of content will lead to possible change order.
- Sharegate license will be required for migration tasks at an additional cost
- Basic permissions will be configured based on existing file share permissions.

- Post cutover support is capped at 4 hours without signed scope change request
- User Training will be limited to up to 4 hours
- Client already owns or will procure appropriate Microsoft 365 licensing
- Assumes between 7-8 weeks for project completion
- Assumes creation of one Azure VM for installation of Sharegate

Outside of Scope Work:

The following items are outside the scope of this SOW:

- The utilization of non-out of the box SharePoint Modern features
- Custom branding
- Custom Navigation
- Multiple rounds of mockup design review and feedback
- Advanced granular permissions analysis/deployment
- Data cleanup

Acceptance

Client

By: _ ______________________________ Date: _ ______________________

Name: _ ______________________________ Title: _ ______________________

Citrin Cooperman Advisors LLC

By: _ ______________________________ Date: _ ______________________

Name: _ ______________________________ Title: _ ______________________

Task Name	Duration (da	Work (hrs)	Cost	Pr	Start	Finish	PM	MSFT Dir	MSFT Sta	Full Task
PAL01-1017- Migration to OneDrive, SharePoint	**47d**	**100.00**	**$24,100.00**		**04/01/24**	**06/06/24**	**14**	**46**	**40**	
Initiate	**9.25d**	**8.00**	**$2,050.00**		**04/01/24**	**04/12/24**	**5.5**	**2.5**	**0**	**Initiate**
Team Augmentation	0.5d	0.00	$0.00		04/01/24	04/01/24				Initiate > Team Augmentation
Presales Artifacts Review	1d	0.00	$0.00	3F	04/02/24	04/03/24				Initiate > Presales Artifacts Review
Project Setup	0.5d	1.00	$225.00	4F	04/03/24	04/03/24	1			Initiate > Project Setup
SOW Review and Kickoff Planning	0.5d	3.00	$775.00	5	04/03/24	04/03/24	2	1		Initiate > SOW Review and Kickoff Planning
Introduction Call with Customer	0.25d	0.00	$0.00	6	04/04/24	04/04/24				Initiate > Introduction Call with Customer
Internal KT Prep and Delivery	0.5d	0.50	$162.50	7	04/04/24	04/04/24		0.5		Initiate > Internal KT Prep and Delivery
Solution Architect Project Overview w/Team	0.25d	0.00	$0.00	8F	04/05/24	04/05/24				Initiate > Solution Architect Project Overview w/Team
Draft Implementation Kickoff Presentation	0.5d	2.00	$500.00	9	04/08/24	04/08/24	1.5	0.5		Initiate > Draft Implementation Kickoff Presentation
Implementation Kickoff Meeting	0.25d	1.00	$275.00	10F	04/11/24	04/11/24	0.5	0.5		Initiate > Implementation Kickoff Meeting
Prepare Finalized Project Plan	0.5d	0.50	$112.50	11	04/11/24	04/12/24	0.5			Initiate > Prepare Finalized Project Plan
Manage	**30d**	**16.00**	**$4,400.00**		**04/12/24**	**05/24/24**	**8**	**8**	**0**	Manage
Manage Project	30d	8.00	$1,800.00	2	04/12/24	05/24/24	8			Manage > Manage Project
General Communication	30d	8.00	$2,600.00	2	04/12/24	05/24/24		8		Manage > General Communication
Update Internal Documentation	30d	0.00	$0.00	2	04/12/24	05/24/24				Manage > Update Internal Documentation
Analyze	**18.25d**	**27.00**	**$8,775.00**		**04/08/24**	**05/02/24**	**0**	**27**	**0**	Analyze
Run content analysis report	5d	2.00	$650.00	9	04/08/24	04/12/24		2		Analyze > Run content analysis report
Conduct analysis report review	2d	4.00	$1,300.00	12F	04/24/24	04/26/24		4		Analyze > Conduct analysis report review
Conduct content owner migration review meeting	1d	2.00	$650.00	19	04/26/24	04/29/24		2		
Review meeting results	1d	1.00	$325.00	20	04/29/24	04/30/24		1		
M365 Online environment assessment	1d	4.00	$1,300.00	21	04/30/24	05/01/24		4		
Deliverable: Finalized migration analysis results	1d	2.00	$650.00	22	05/01/24	05/02/24		2		
Deliverable: SharePoint Online environment assessment results and recommendations	0.5d	2.00	$650.00	19F	04/25/24	04/26/24		2		Analyze > Deliverable: SharePoint Online environment assessment results and recommendations
Determine destination architecture	1d	4.00	$1,300.00	24	04/26/24	04/29/24		4		
Prepare migration plan	1d	4.00	$1,300.00	25	04/29/24	04/30/24		4		
Deliverable: Migration Plan	1d	2.00	$650.00	26	04/30/24	05/01/24		2		
Milestone: Analysis & Design	0	0.00	$0.00	24F	04/26/24	04/26/24				Analyze > Milestone: Analysis & Design
Build	**3d**	**4.00**	**$600.00**		**04/26/24**	**05/01/24**	**0**	**0**	**4**	Build
Create destination architecture	3d	4.00	$600.00	28	04/26/24	05/01/24			4	Build > Create destination architecture
Milestone: Build	0	0.00	$0.00	30	05/01/24	05/01/24				Build > Milestone: Build
Deploy	**11d**	**40.00**	**$7,050.00**		**05/01/24**	**05/16/24**	**0**	**6**	**34**	Deploy
Migration Tasks	**11d**	**30.00**	**$4,500.00**		**05/01/24**	**05/16/24**	**0**	**0**	**30**	Deploy > Migration Tasks
Configure Sharegate Tool	5d	2.00	$300.00	31	05/01/24	05/08/24			2	Deploy > Migration Tasks > Configure Sharegate Tool
Configure and start copy job	1d	8.00	$1,200.00	34	05/08/24	05/09/24			8	

Monitor copy job progress	1d	12.00	$1,800.00	35	05/09/24	05/10/24			12	
Remediate any issues	1d	4.00	$600.00	36	05/10/24	05/13/24			4	
User Training	1d	0.00	$0.00	37	05/13/24	05/14/24				
Client UAT	1d	0.00	$0.00	38	05/14/24	05/15/24				
Complete final remediations (if required)	1d	4.00	$600.00	39	05/15/24	05/16/24			4	
Milestone: Migration Tasks	0	0.00	$0.00	34	05/08/24	05/08/24				Deploy > Migration Tasks > Milestone: Migration Tasks
Go Live	**1.25d**	**10.00**	**$2,550.00**		**05/15/24**	**05/16/24**	**0**	**6**	**4**	#UNPARSEABLE
Go Live Support	0.25d	6.00	$1,250.00	#R	05/15/24	05/15/24		2	4	#UNPARSEABLE
User Training	1d	4.00	$1,300.00	43	05/15/24	05/16/24		4		#BLOCKED
Milestone: Go Live	0	0.00	$0.00	44	05/16/24	05/16/24				#BLOCKED
Activate	**13.75d**	**5.00**	**$1,225.00**		**05/16/24**	**06/06/24**	**0.5**	**2.5**	**2**	#BLOCKED
Post Go-Live Support	7d	4.00	$950.00	45	05/16/24	05/28/24		2	2	#BLOCKED
Project Closure/Transition Meeting	7d	1.00	$275.00	45F	05/23/24	06/04/24	0.5	0.5		#BLOCKED
Milestone: Project Closure	0	0.00	$0.00	#R	06/06/24	06/06/24				#UNPARSEABLE

AGENDA ITEM NO. 7.2

BOARD MEMORANDUM

DATE:	June 10, 2024
TO:	**BOARD OF DIRECTORS**
FROM:	Mr. Jim Stanton, Information Technology Manager
VIA:	Mr. Dennis D. LaMoreaux, General Manager
RE:	***CONSIDERATION AND POSSIBLE ACTION ON IMPLEMENTATION OF MULTI-FACTOR AUTHENTICATION (MFA). ($15,800.00 – NON-BUDGETED – INFORMATION TECHNOLOGY MANAGER STANTON)***

Recommendation:

Staff recommends Board approval on implementing Multi-Factor Authentication (MFA) for all District users.

Alternative Options:

The Board can choose for the District to remain as is, but we will lose access to all Microsoft 365 applications and Office 365 sites.

Impact of Taking No Action:

Taking no action would result in lost access to all Microsoft cloud applications: Teams, SharePoint, Word, Outlook, Excel, etc.

Background:

With the recent increase in attacks from both nation state actors and domestic hackers, Microsoft has found it necessary to implement Multi-Factor Authentication (MFA) for all its online resources. This includes our Office 365 licenses. Microsoft is forcing all Tenants to implement MFA by June 30, 2024.

Overview:

Multi-factor authentication (MFA) is a layered approach to securing physical and logical access where a system requires a user to present a combination of two or more different authenticators to verify a user’s identity for login. MFA increases security because even if one authenticator becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space or computer system.

Why is MFA Important?

Implementing MFA makes it more difficult for a threat actor to gain access to business premises and information systems, such as remote access technology, email, and billing systems, even if passwords or PINs are compromised through phishing attacks or other means. Adversaries are increasingly capable of guessing or harvesting passwords to gain illicit access. Password cracking techniques are becoming more sophisticated and high-powered computing is increasingly affordable. In addition, adversaries harvest credentials through phishing emails or by identifying passwords reused from other systems. MFA adds a strong protection against account takeover by greatly increasing the level of difficulty for adversaries.

How Does MFA Work?

MFA requires users to present two or more authentication factors at login to verify their identity before they are granted access. Each additional authentication factor added to the login process increases security. A typical MFA login would require the user to present some combination of the following:

- Something you know: like a password or Personal Identification Number (PIN);
- Something you have: like a smart card, mobile token, or hardware token; and,
- Some form of biometric factor (e.g., fingerprint, palm print, or voice recognition)

For example, MFA could require users to insert a smart card or a bank card into a card reader (first factor) and then enter a password or a PIN (second factor). An unauthorized user in possession of the card would not be able to log in without also knowing the password; likewise, the password is useless without physical access to the card.

We currently have Cisco Duo in place to implement MFA but require an upgrade of our existing Office licenses to Entra ID P1. This will increase our annual 1-09-4155-801 Cloud-Services-MS-Office 360 cost by Ten-Thousand Eight Hundred Dollars ($10,800.00) raising it to Forty-Seven Thousand Eight Hundred Dollars ($47,800.00).

This might cause a slight increase in Cell Phone Stipend costs for individuals that do not currently have a District issued iPad or iPhone to use as the secondary trusted device. Costs to be determined.

Anticipated vendor charges not to exceed Five-Thousand Dollars ($5,000.00). Vendor assistance and costs from Microsoft, Duo and Citrin Cooperman to be minimal.

Unfortunately, as an enterprise organization we cannot utilize any of the “free” personal authenticators. Google, Microsoft, and others charge for enterprise use and the cost is above what we currently pay to have Duo.

Strategic Plan Initiative/Mission Statement:

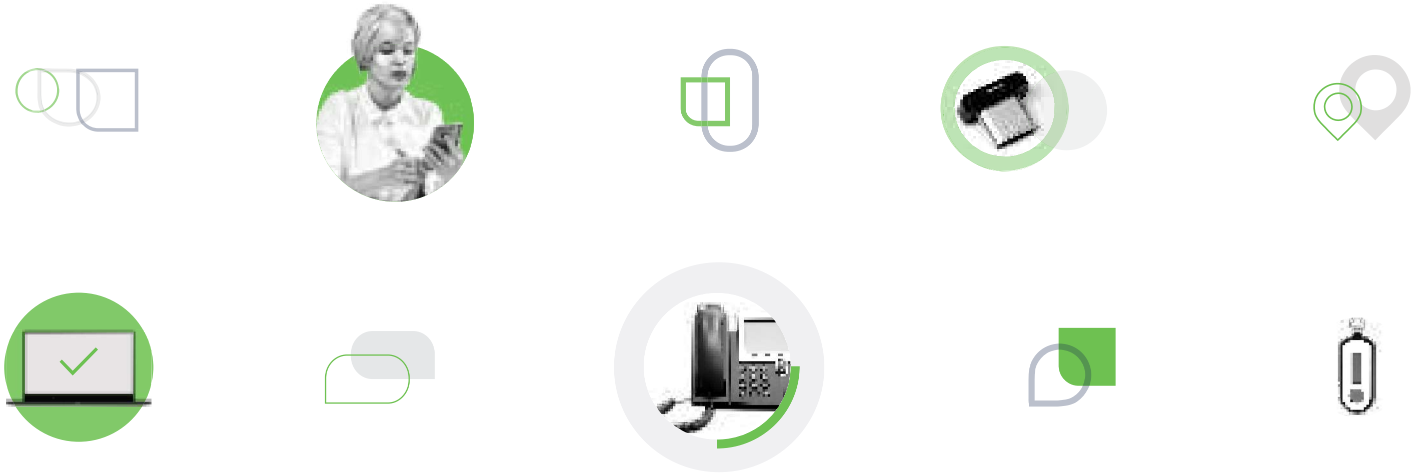
This item is under Strategic Initiative No. 3 – Systems Efficiency.
This item directly relates to the District's Mission Statement.

Budget:

This item is non-budgeted and has a one-time cost of approximately $15,800.00.

Supporting Documents:

- MFA Evaluation Guide



Multi-Factor Authentication Evaluation Guide

What to look for when assessing and comparing
multi-factor authentication solutions

Multi-Factor Authentication Evaluation Guide

What to look for when assessing and comparing multi-factor authentication solutions

Over 80% of the breaches categorized under web application attacks can be attributed to stolen credentials, allowing attackers to login rather than break-in.

VERIZON 2022 DATA BREACH INVESTIGATIONS REPORT

Multi-factor authentication is the simplest, most effective way to make sure users really are who they say they are.

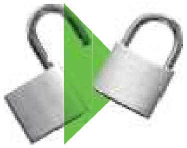
It protects your applications and data against unauthorized access due to credential theft by verifying your users' identities before they access your data. Multi-factor authentication works by requiring multiple factors to be confirmed before permitting access versus just an email and a password. Authentication factors can be something you know, like a password; something you have, like your device or a security key; something you are, like your personal fingerprint (biometrics); somewhere you are, like your location; and your level of access based on adaptive policies.

But, not every MFA solution is the same. Some vendors only provide the bare minimum needed to meet compliance requirements – and lots of hidden costs required for deployment, operation and maintenance. Plus, many traditional solutions are clunky, error-prone and require extensive user training and support – costing your employees time and productivity.

IN THIS GUIDE, YOU'LL GET:

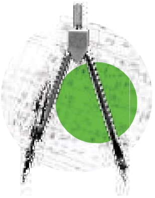
+ A comprehensive set of criteria to customize your evaluation to your organization's needs
+ An overview of the hidden costs of an MFA solution and how to determine your return on investment (ROI)
+ What to look for to ensure your solution can protect against the risk of a data breach
+ A list of resources needed to deploy, provision and integrate your solution
+ An overview of the different strategic business initiatives, and how your solution fits into them

Consider the following criteria when evaluating different multi-factor authentication solutions:



Security Impact

Can your solution protect against unauthorized access and provide visibility of users and devices in your environment? How effectively does the solution reduce the risk of a data breach? Can your solution provide access control for managed and unmanaged devices? Does your solution alert you to unusual or suspicious login activities?



Strategic Business Initiatives

Is your solution compatible with other business initiatives such as enabling remote work or onboarding cloud applications? Does it fulfill compliance requirements?

Total Cost of Ownership

Does your solution provide upfront value, or incur hidden costs to your organization? Can it work with modern and legacy systems? Can the solution help consolidate multiple siloed tools?

Time to Value

How quickly can you get the solution up and running in your environment?

Required Resources

What kind of resources are required to deploy and provision users? Is the solution architected to reduce ongoing administration tasks?

These are some of the big questions you want to ask to find out if an MFA solution is truly the best solution for your business. Let’s dig in deeper into these questions.

Security Impact

The most critical security aspects of an authentication solution are 1) effectiveness against threats related to credential theft, and 2) underlying security and reliability. The primary goal is to reduce the risk of a data breach to your organization. If a solution is easily bypassed or doesn't provide comprehensive protection, it's not worth implementing (at any cost!).

Secure Everything, Everywhere

FOCUS ON REMOTE LOGINS

Before you implement a new security solution, take full inventory of your organization's applications, networks and data that can be accessed remotely. If you can log into an application or a system over the internet, you should protect it with more than just a username and password. VPN, SSH and RDP connections are gateways to your corporate networks and therefore require added layers of protection to prevent unauthorized access. Wherever possible, use **FIDO-based** (Fast IDentity Online, an open industry standard for strong authentication) security keys that leverage **WebAuthn** and provide the highest level of assurance for authentication.

With a modern MFA solution built on **zero trust principles**, you can get a clearer picture of the users and devices that are trying to access your network. It is no longer enough just to verify the user before granting access. Consider verifying the device status as part of the authentication workflow. Ensure your solution can integrate with any custom software, VPNs, cloud-based applications and device management tools.

REDUCE DEPENDENCY ON PASSWORDS

Passwords are a thorn in the side of enterprise security. An average enterprise uses more than 1,000 cloud apps today. That's too many passwords for IT to manage securely, and for users to remember. This results in password fatigue, and it's no surprise that weak and stolen passwords are among the leading causes of a breach. Eliminating passwords from authentication sounds very attractive; however, as with any new technology, it is wise to take a thoughtful approach to adopting passwordless authentication.

Passwordless is a journey that requires incremental changes for both users and IT environments. Ask security vendors how their products can help you embrace a passwordless future without creating security gaps or causing IT headaches.

Enabling a single sign-on (SSO) option along with MFA is a great way to start the passwordless journey without compromising on security.

For end users, SSO provides access to multiple applications with a single login (using one master set combination of username and password) — and reducing the number of passwords eliminates bad password habits such as password reuse. For administrators, SSO serves as a unified point of visibility for authentication and access logs, and an effective policy enforcement point to apply security policies for each application depending on its risk profile.

Username
admin
Password
••••••••••••••••••

If you can log into it over the internet, you should protect it with more than a username and password.

SECURE SENSITIVE DATA

Check that the solution allows you to create and enforce advanced policies and controls that you can apply to environments with sensitive data – whether it is internet-accessible or a private network. Examples include:

- Define how users access sensitive systems, such as servers containing financial data
- Set a stricter policy for servers with customer payment data vs. public file servers

VERIFY DEVICE STATE

Consider a solution that offers comprehensive device verification capabilities across laptops, desktops or mobile devices. The solution should ensure that devices accessing your environment are in compliance with your organization's security criteria. This includes verifying that the devices have critical software patches installed and enabling end-user remediation where applicable.

Check that the solution can leverage telemetry from your endpoint security agents and device management tools as part of posture assessments.

ADAPTIVE POLICIES & CONTROLS

An advanced multi-factor authentication solution lets administrators define rules and levels of access with adaptive controls, balancing security and ease-of-use based on the users, groups, devices, networks and applications involved.

Examples of adaptive policies and controls include:

- Require admins and IT staff to perform two-factor authentication using biometrics or a FIDO-based security key every time they log in to protect privileged access
- Allow users to authenticate less often when using the same device
- Block login attempts from foreign countries where you don't do business, and block access from anonymous networks, like Tor
- Allow users to only access critical applications from corporate managed devices

While traditional solutions such as firewalls and network access control (NAC) can do this, they're typically limited to protecting your on-premises resources. But by focusing only on the local network perimeter, these solutions leave many security gaps and zero coverage for cloud applications. Look for a solution that offers protections beyond a traditional network-based perimeter and truly protects access from any device and from any location.

Check that your provider offers different authentication methods to fit every user's need.

VISIBILITY & ANALYTICS

Ask your provider if your solution gives you insight into your users and the devices they use to access your organization's apps and data. An advanced authentication solution should give you an at-a-glance picture of the security profile of all devices in your environment, letting you take action to protect against known vulnerabilities. Because data is only as useful as it is accessible, make sure your dashboard provides a comprehensive bird's-eye view along with the ability to quickly zoom or filter into more granular information.

Ensure your solution comes with detailed logs about your users, devices, administrators and authentication methods. The solution should allow these logs to easily export to your SIEM tools and help create custom reports, ideal for security analysts and compliance auditors.

Choose a solution that gives you visibility into authentication attempts, including data on IP addresses, anonymous networks, blacklisted countries and more – useful for determining where and when certain attacks may occur. Ask if the provider can detect and automatically alert administrators in case of risky login behavior or suspicious events, such as new device enrollment for authentication or login from an unexpected location.

FLEXIBILITY

It's expensive to rip and replace a solution, so choose one that can scale to support new users, integrations and devices – no matter where they are, including on-premises and in the cloud. Check that your provider offers different authentication methods, including smartphone apps, biometrics, phone callback, passcodes and hardware tokens to fit every user's need.

AVAILABILITY

A security solution is only as valuable as it is available, and resilient against security incidents and downtime. A cloud-based MFA provider should maintain their solution independent from your systems. That way, even if you're breached, access to your applications is still securely managed by your provider.

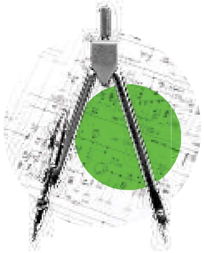
To protect against downtime, your provider's service should be distributed across multiple geographic regions, providers and power grids for seamless failover. Reliable vendors should demonstrate **99.99% uptime**, guaranteed by strong service level agreements (SLA).

Check that your provider offers different authentication methods to fit every user's need.

Ensure your solution comes with detailed logs about your users, devices, administrators and authentication methods.

Strategic Business Initiatives

When evaluating a new security solution, consider how it may integrate with ongoing or future business initiatives, including legacy systems, bring your own device (BYOD), remote work or the adoption of cloud applications. Other business drivers to consider include compliance regulation requirements, which vary by industry and location.



CLOUD ADOPTION TODAY

Most of your applications and servers might be on-premises, but some may migrate to the cloud in the near future. Check that the authentication solution can easily integrate with your cloud applications. Additionally, if you're moving away from managing software and hardware on-premises, then you should consider adopting a cloud-based authentication solution that can scale as needed. Make sure your authentication solution protects what's important both today and in the future.

BRING YOUR OWN DEVICE (BYOD) – REMOTE WORK PROTECTION

Many organizations are allowing employees to use their personal devices to get work done. When evaluating authentication solutions, consider how compatible they are with your BYOD environment. Can users use their own devices to complete authentication?

Check that your authentication solution provides a mobile app that works with all of the different types of mobile and remote devices your employees use, including Windows, Apple iOS and Android. For flexibility, ensure the solution works with other methods like security keys, mobile push, code generators and phone callback.

Can your authentication solution detect potential vulnerabilities in the devices your employees use? Ask your provider how you can get greater visibility and control into your cloud and mobile environment, without requiring users to enroll their personal devices in enterprise mobility solutions (like mobile device management/MDM).

If it's not easy to use, your users won't use it. Evaluate the usability of your mobile app, for both your users (enrollment, activation and daily authentication) and administrators (user and solution management).

If it's not easy to use,
your users won't use it.

MONITORING & REPORTING

Ensure your solution comes with detailed logs about your users' activity so you can create custom reports, ideal for security analysis and compliance auditors. Armed with details about jailbroken statuses, patch levels, browsers and more, you can also take action to prevent opening up your network to known vulnerabilities. Monitoring also gives you insight into any user behavior anomalies or geo-impossible logins – if your user logs in from one location, and then logs in from another location around the world, your security team will know.

Every organization's environment is unique. Check if the solution provider offers advanced machine learning-based behavioural analytics that can create a risk profile for your specific organization and notify administrators of any unusual login activity.

VALIDATION & COMPLIANCE

If you deal with any type of sensitive data, like personally identifiable information (PII), protected health information (PHI), customer payment data, etc., you need to ensure your two-factor solution can meet any **compliance regulation** requirements.

Additionally, your MFA provider must be able to provide an up-to-date proof of compliance report for your auditors. Ask your provider if their company and solution is audited annually or regularly by an independent third-party auditor.

Check that the vendor's cloud-based service uses PCI DSS (Payment Card Industry Data Security Solution), ISO (International Organization for Standardization) 270001 and SOC (Service Organization Controls) 2 compliant service providers. It only takes one weak link in the security chain of contractors for a breach to affect your organization.

Remember, it only takes one weak link in the security chain for a breach to affect your organization.

Total Cost of Ownership

The total cost of ownership (TCO) includes all direct and indirect costs of owning a product – for a multi-factor solution, that may include hidden costs, such as upfront, capital, licensing, support, maintenance, operating and many other unforeseen expenses over time, like professional services and ongoing operation and administration costs.

How can you be sure you're getting the best security return on your investment? Consider:

Upfront Costs

See if your vendor's purchasing model requires that you pay per device, user or integration – this is important if your company plans to scale and add new applications or services in the future. Many hosted services provide a per-user license model, with a flat monthly or annual cost for each enrolled user. When investigating licensing costs, make sure to confirm whether licenses are named (locked to a single user ID) or transferable, whether there are add-on charges for additional devices or integrations configured, or delivery charges for different factor methods. Estimate how much it will cost to deploy multi-factor authentication to all of your apps and users.

Look for vendors with simple subscription models, priced per user, with flexible contract times.

ADMINISTRATIVE SOFTWARE/HARDWARE

Is this included in the software license? Additional management software is often required – without this, customers can't deploy MFA. Does the service require the purchase and configuration of hardware within your environment? Confirm the initial and recurring costs for this equipment, and research the typical time and labor commitment necessary to set up these tools. For administrative access with tiered permissions based on license version, confirm all functionality you depend on is available, or collect a complete list of necessary upcharges.

VENDOR CONSOLIDATION

While network environments with a traditional perimeter defense model rely on a handful of key services to maintain visibility and enforce security standards, the growth of SaaS adoption has resulted in many piecemeal solutions to cover the expanded needs of securing cloud-based data and assets. Secure access includes strong authentication through MFA to validate users and may also include:

+ Endpoint management or mobile device management tools for defending against device compromise threats
+ Single sign-on portals to centralize and simplify login workflows for users
+ Log analysis tools to identify and escalate potential security threats
+ Multiple dashboards to manage disparate services and cover unsupported applications, and more

Along with the redundant costs that can accrue from these overlapping services, each added tool increases complexity and the chances of human error or oversight. Finding a solution with comprehensive utility for secure access can reduce both initial and ongoing management labor costs.

Upfront Costs

(continued)

AUTHENTICATORS

Do you have to purchase hardware authentication devices? Physical tokens add inventory, management, and shipping costs to consider. For mobile authenticators, confirm if there is any per-device cost for soft tokens, or if an unlimited number of enrolled devices is permitted for each user license.

DATA CENTER COSTS

Do you have to purchase servers? Server hosting costs can add up: power, HVAC (heating, cooling and air conditioning), physical security, personnel, etc. A cloud-based solution will typically include these costs in the licensing model.

HIGH AVAILABILITY CONFIGURATION

Is this also included in your software license? By setting up duplicate instances of your software and connecting a load balancer with the primary instance, you can end up tripling your software costs. Setting up a redundant or disaster recovery configuration can also increase costs significantly, and some vendors charge additional licensing fees for business continuity.

Deployment Fees

DEPLOYMENT & CONFIGURATION

Find out if you can deploy the solution using your in-house resources, or if it will require professional services support and time to install, test and troubleshoot all necessary integrations.

END USER ENROLLMENT

Estimate how long it will take each user to enroll, and if it requires any additional administrative training and helpdesk time. Discuss with your vendor the typical deployment timeframe expected with your use case, and seek feedback from peers to validate how this aligns with their experience. Look for an intuitive end user experience and simple enrollment process that doesn't require extensive training. Token-based solutions are often more expensive to distribute and manage than they are to buy.

ADMINISTRATOR SUPPORT

To make it easy on your administrators, look for drop-in integrations for major apps, to cut time and resources needed for implementation. Also confirm the availability of general-purpose integrations for the most common authentication protocols to cover edge use cases, along with APIs to simplify integration for web applications. See if you can set up a pilot program for testing and user feedback – simple integrations should take no longer than 15 minutes.

Token-related help desk tickets can account for 25% of the IT support workload.

Ongoing Costs

PATCHES, MAINTENANCE & UPGRADES

Annual maintenance can raise software and hardware costs, as customers must pay for ongoing upgrades, patches and support. It's often the responsibility of the customer to search for new patches from the vendor and apply them. Look for a vendor that automatically updates the software for security and other critical updates, saving the cost of hiring a team.

One of the benefits of SaaS and cloud-hosted services is that servers, maintenance and monitoring are covered by the provider's network and security engineers, lightening the load for your team. Depending on your solution, you may have to manually upgrade to the latest version.

You should also consider the frequency of updates — some vendors may only update a few times a year, which can leave you susceptible to new vulnerabilities and exploits. Choose a vendor that updates often, and ideally rolls out automatic updates without any assistance from your team.

ADMINISTRATIVE MAINTENANCE

Consider the costs of employing full-time personnel to maintain your MFA solution. Does your provider maintain the solution in-house, or is it up to you to hire experts to manage it?

Estimate how long it takes to complete routine administrative tasks. Is it easy to add new users, revoke credentials or replace tokens? Routine tasks, like managing users, should be simple. Sign up for a trial and take it for a test run before deploying it to all of your users.

SUPPORT & HELP DESK

Live support via email, chat and/or phone should also be included in your vendor's service – but sometimes support costs extra. Consider how much time is required to support your end users and helpdesk staff, including troubleshooting time.

Gartner estimates that password reset inquiries comprise anywhere between 30% to 50% of all helpdesk calls. And according to Forrester, 25% to 40% of all helpdesk calls are due to password problems or resets. Forrester also determined that large organizations spend up to $1 million per year on staffing and infrastructure to handle password resets alone, with labor cost for a single password reset averaging $70.

If a solution requires extensive support from your IT or infrastructure teams, will you get charged for the time spent supporting your on-premises MFA solution? Estimate that cost and factor it into your budget.

Modern Solutions

High value, upfront costs

- + Simple subscription model
- + Free authentication mobile app
- + No fees to add new apps or devices
- + No data center/server maintenance
- + High availability configuration
- + Automatic security and app updates
- + Administrative panel included
- + User self-service portal included
- + User, device and application access policies and controls
- + Device health and posture assessments
- + Device context from third-party security solutions
- + Passwordless authentication
- + User behavior analytics
- + Single sign-on (SSO) and cloud support

Traditional Solutions

Potentially low upfront costs, not much value

LOTS OF HIDDEN COSTS:

- – Additional cost to add new apps or users
- – Administrative software/hardware
- – Authenticators – tokens, USB, etc.
- – Data center and server maintenance
- – High availability configuration
- – Administrative support
- – Patches, maintenance and upgrades
- – Helpdesk support

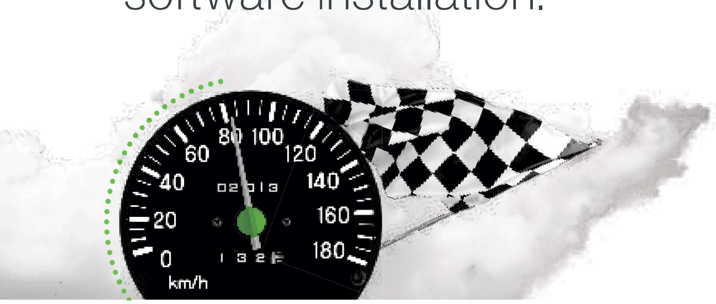
Time to Value

Time to value, or time to security, refers to the time spent implementing, deploying and adapting to the solution. Determine how long it takes before your company can start realizing the security benefits of a multi-factor authentication solution. This is particularly important after a recent breach or security incident.

Proof of Concept

Setting up a MFA pilot program lets you test your solution across a small group of users, giving you the ability to gather valuable feedback on what works and what doesn't before deploying it to your entire organization.

Cloud-based services deploy faster because they don't require hardware or software installation.



Deployment

Walk through likely implementation scenarios so you can estimate the time and costs associated with provisioning your user base. Cloud-based services provide the fastest deployment times because they don't require hardware or software installation, while on-premises solutions tend to take more time and resources to get up and running.

Most security professionals don't have time to write their own integration code. Choose a vendor that supplies drop-in integrations for all major **cloud apps**, **VPNs**, **Unix** and **MS** remote access points. You'll also want to look for a vendor that enables you to automate functionality and export logs in real time.

Also, to save on single sign-on (SSO) integration time, check that your MFA solution supports the Security Assertion Markup Language (SAML) authentication standard that delegates authentication from a service provider or application to an identity provider.

Onboarding & Training Users

A vendor's enrollment process is often a major time sink for IT administrators. Make sure you walk through the entire process to identify any potential issues.

For enterprises, bulk enrollment may be a more time-efficient way to sign up a large amount of users. To support your cloud apps, ensure your MFA solution lets you quickly provision new users for cloud apps by using existing on-premises credentials.

See if the solution requires hardware or software for each user, or time-consuming user training. Token deployment can require a dedicated resource, but easy self-enrollment eliminates the need to manually provision tokens.

With a mobile cloud-based solution, users can quickly download the app themselves onto their devices. A solution that allows your users to download, enroll and manage their own authentication devices using only a web browser can also save your deployment team's time.

Required Resources

Consider the time, personnel and other resources required to integrate your applications, manage users and devices, and maintain/monitor your solution. Ask your provider what they cover and where you need to fill in the gaps.

Application Support

Some MFA solutions require more time and personnel to integrate with your applications, whether on-premises or cloud-based.

Check that they provide extensive documentation, as well as APIs and SDKs so you can easily implement the solution into every application that your organization relies on.

User & Device Management

Like any good security tool, your MFA solution should give administrators the power they need to support users and devices with minimal hassle.

Look for a solution with a centralized administrative dashboard for a consolidated view of your two-factor deployments, and enables admins to:

+ Easily generate bypass codes for users that forget or lost their phones
+ Add and revoke credentials as needed, without the need to provision and manage physical tokens

Ask your provider if they offer a self-service portal that allows users to manage their own accounts, add or delete devices, and other simple tasks.

Maintenance

Make sure that your solution requires minimal ongoing maintenance and management for lower operating costs. Cloud-hosted solutions are ideal because the vendor handles infrastructure, upgrades and maintenance.

Can you use your existing staff to deploy and maintain this solution, or will you need to hire more personnel or contractors to do the job? Ask your vendor if monitoring or logging is included in the solution.

A solution that requires many additional resources to adapt and scale may not be worth the cost and time. Evaluate whether your solution allows you to easily add new applications or change security policies as your company needs evolve.

Can your staff deploy and maintain the solution, or will you need to hire more personnel or contractors?

The Duo Advantage

Duo Security's **MFA solution** combines intuitive usability with advanced security features to protect against the latest attack methods and to provide a frictionless authentication experience.

Security Impact

TRUSTED USERS

Duo's authentication is built on the foundation of **zero trust**. Duo verifies the identity of users and protects against breaches due to phishing and other password attacks with an advanced MFA solution, verifying trust in multiple ways before granting access. Duo's contextual **user access policies** let you create custom controls to further protect access to your applications based on type of users, devices and apps.

Learn more about **Trusted Users**.

TRUSTED DEVICES

When organizations deploy Duo, **device trust** becomes a part of the authentication workflow during the user login process for protected applications. This enables Duo to provide **in-depth visibility** across managed and unmanaged devices, however and from wherever the users connect to these applications. Duo also verifies the **security health** and **management status** of endpoints before granting access to your applications, and blocks access if the device is unhealthy or does not meet your security requirements.

You can easily ensure that users maintain appropriate device hygiene, whether by updating the OS patch levels or browser versions, checking for presence of device certificates, or enabling security features such as enterprise antivirus (AV) agents and disk encryption.

Learn more about **Trusted Devices**.

SECURE EVERY APPLICATION

To secure **every type of application**, Duo's solution easily and quickly integrates with virtual private networks (VPNs) and remote access gateways like CA SiteMinder, Juniper, Cisco, Palo Alto Networks, Citrix and more; **enterprise cloud apps** like Microsoft O365, Salesforce, Google Apps, AWS and Box; and on-premises and **web apps** like Epic, Splunk, Confluence, Shibboleth and more. Duo provides APIs and client libraries for everything else, including your custom and proprietary software.

Learn more about **Every Application**.

Duo verifies the identity of your users with two-factor authentication, and the security health of their devices before they connect to your applications.

Security Impact

(continued)

START YOUR PASSWORDLESS JOURNEY

Going passwordless means establishing a strong assurance of a user's identity without relying on passwords, allowing them to authenticate using biometrics, security keys or a mobile device. Duo will help you get to a passwordless future starting with reducing the number of logins. With Duo's secure cloud-based **single sign-on** (SSO), you can leverage your existing identity provider for faster provisioning and improved accuracy whether in the cloud or on-premises, allowing your users to log in just once to securely access your organization's applications.

Duo's **passwordless authentication** solution will improve user experience, reduce IT overhead, and strengthen security posture. Duo uniquely takes its **passwordless solution** a step further by enabling organizations to implement a **passwordless authentication** that's secure and usable. Duo ensures that a risky device (unknown, jailbroken or out of date) cannot be used to authenticate without a password. In addition, Duo continually monitors logins and new enrollments to automatically detect anomalies and alerts the administrators in case your environment is compromised.

Learn more about **Passwordless**.

ADAPTIVE POLICIES & CONTROLS

Security policies for every situation. Duo's granular advanced policy controls provide zero trust protection to environments with sensitive data, whether on-premises or in the cloud. With Duo, you can create custom **access policies** based on role, device, location and many other contextual factors that are the bedrock of a strong zero trust security framework.

Duo verifies the identity of your users with multi-factor authentication and the security health of their devices before they connect to your applications. With Duo, IT administrators may also create complex policy rules that continuously monitor logins to identify and flag unusual activity.

“

We are a very open organization and want employees to work from anywhere. Box manages highly sensitive data for some of the largest organizations in the world. As a result of this, we need to ensure the highest level of protection for all user interactions with our services. We also need to meet an extremely high bar for security standards while making it easy for users to be productive.
Duo helps us do just that.”

Mark Schooley
Senior Director, IT Operations & Engineering

box

VISIBILITY & ANALYTICS

Duo's **dashboard, reports and logs** make it easy to monitor every user, on any device, anywhere, so you can identify security risks before they lead to compromised information. Get visibility into authentication attempts, including data on IP addresses, anonymous networks, blacklisted countries and more from Duo's admin panel.

Duo gives you **complete visibility** and helps you inventory every endpoint accessing your applications and provides data on operating system, platform, browser and plugin versions, including passcode, screen lock, full disk encryption and rooted/jailbroken status. You can easily search, filter and export a list of devices by OS, browser and plugin, and refine searches to find out who's susceptible to the latest iOS or Android vulnerability.

Duo **Trust Monitor** is a security analytics feature that identifies and surfaces risky, potentially insecure user behavior in a customer's Duo deployment. If a user significantly deviates from their individualized behavioral profile, Duo Trust Monitor will surface the case as behaviorally anomalous.

FLEXIBILITY

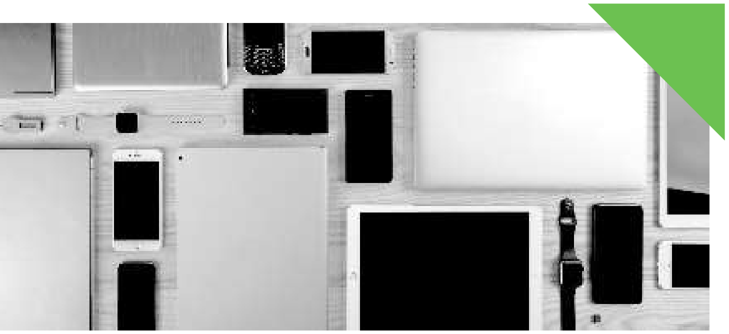
As a cloud-based solution, it's easy to provision new users and protect new applications with Duo as your company grows, because there are no limits or additional charges per application. We believe that if you're protecting a user's access to your most important applications, you shouldn't be penalized or charged more to protect them everywhere. Easily onboard new users with Duo's **self-enrollment**, bulk enrollment or Active Directory synchronization options.

There are a variety of ways Duo's MFA can work. You can use a smartphone, landline (such as your office or home phone), tablet or hardware token. **Authentication methods** include mobile push, biometrics, time-based one-time passcodes, bypass codes, security tokens, SMS passcodes and callback.

Learn about **User Provisioning**.

AVAILABILITY

Duo's Service Level Agreements (SLA) guarantees a **99.99% uptime** and is distributed across multiple geographical locations for a seamless failover. Duo is maintained independently from your systems keeping you safe even if your systems are breached.



Duo gives you insight into the security posture of both corporate and personal devices used to connect to company applications and services.

Strategic Business Initiatives

CLOUD ADOPTION

By leveraging a scalable cloud-based platform rather than relying on on-premises hardware requiring setup and costly maintenance, Duo can be deployed rapidly; and it's easy to scale with your growing users and applications. Duo also supports SAML cloud apps via secure single sign-on, including Google Apps, Amazon Web Services, Box, Salesforce and Microsoft Office 365.

WORKFORCE PRODUCTIVITY

Duo provides a better end user experience for accessing applications by reducing workflow friction and increasing workplace productivity. Duo offers low-friction authentication methods such as Duo Push, biometrics and FIDO security keys. Duo also offers the ability to apply intelligent policies to reduce how often a user is prompted to authenticate, using features such as **remembered device**. Duo is focused on enabling users to be productive without compromising on security thereby achieving the right balance for your organization.

BRING YOUR OWN DEVICE (BYOD) - REMOTE WORK PROTECTION

The **Duo Mobile app** (iOS, Android) and the **Device Health app** (Windows, MacOS) are BYOD-friendly for **remote access** and can be used on many different devices. Duo can maintain your device inventory so you have clear visibility into what device is connecting, when and from where. Users can download the app on their personal device without enrolling in device management solutions, ensuring user privacy.

MONITORING AND REPORTING

Duo's detailed user, administrator and telephony security logs can be easily imported into a security information and event management (SIEM) tool for log analysis, or viewed via **Duo's Admin API** for real-time log access. In addition, **Duo Trust Monitor** employs machine learning–behavioral analytics to simplify risk detection in case of anomalous login activity.

VALIDATION AND COMPLIANCE

Duo's full-time security team is experienced in running large-scale systems security, and comprises top mobile, app and network security experts. Duo's operational processes are SOC 2 compliant. Duo's multi-factor authentication cryptographic algorithms are also validated by NIST and FIPS. Duo has achieved ISO (the international security standard) 27001:2013, 27017:2015 & 27018:2019 Certification.

Duo can also help your business meet various **compliance requirements and regulatory framework guidelines**. Duo Push satisfies Electronic Prescription of Controlled Substance (EPCS) requirements for two-factor authentication in the healthcare industry, while Duo's one-time passcodes meet FIPS 140-2 compliance for government agencies.

Duo **Federal Editions** are built to enable customer compliance with FIPS 140-2 compliant authentication standards and align with National Institute of Standards and Technology (NIST) SP 800-63-3 guidelines. Duo Federal editions meet Authentication Assurance Level 2 (AAL2) with Duo Push or Duo Mobile Passcode for both iOS and Android devices out of the box and by default with no additional configuration required. Duo also supports AAL3 authenticators such as the FIPS Yubikey from Yubico.

Duo **Device Trust** enables organizations to check and enforce the device security and compliance posture prescribed by standards such as PCI-DSS, HIPAA and the NIST cybersecurity framework.

Learn more about **Security & Reliability**

Duo's full-time security team is experienced in running large-scale systems security. Duo's diverse research and engineering teams comprises top mobile, app and network security experts and have worked at Fortune 500 companies, government agencies and financial firms.

Total Cost of Ownership (TCO)

While traditional security products require on-premises software or hardware hosted in a data center, Duo offers security in a software as a service (SaaS) model through a cloud-based platform.

NO UPFRONT COSTS

With Duo's multi-factor authentication, you get the most upfront value with no hidden costs such as upfront, capital, licensing, support, maintenance, operating and many other unforeseen expenses over time. Duo offers a simple subscription model priced per user, billed annually, with no extra fees for new devices or applications.

+ Easy deployment with the help of Duo's drop-in integrations for all major apps and APIs, and an administrative panel for user and solution management
+ Automatic application updates, with patch management, maintenance and live support at no extra cost
+ Advanced features that let you customize policies and controls, as well as get detailed device health data
+ Conext leveraged from endpoint security agents and device management systems
+ Self remediation to ensure devices meet your security requirements
+ Insight on user login behavior in your environment and the ability to flag anomalous login attempts
+ First steps on the journey to eliminate passwords and improve security with passwordless authentication
+ A secure single sign-on (SSO) and authentication solution in one

Other solutions may appear to come with a lower price tag, but the layers of hidden costs can add up fast, rapidly tripling TCO and offering less value overall.

Other solutions may appear to come with a lower price tag, but the layers of hidden costs can add up fast, rapidly tripling TCO and offering less value overall. With Duo's MFA, you get the most upfront value with no hidden costs, including:

ADMINISTRATIVE SOFTWARE/HARDWARE

Duo's subscription-based model eliminates hefty software licensing fees and includes administrator management tools, meaning there's no need to pay for top-dollar management software to use it.

AUTHENTICATORS

Users can download the Duo Mobile app to any device, eliminating the need to shell out for a fleet of devices to deploy to your workforce. Duo also offers several authentication methods based on specific use cases; along with Duo Push, Verified Duo Push, end users can authenticate via U2F, biometrics, tokens, passcodes and more.

NO DATA CENTER COSTS

Because Duo is cloud-based, you don't need to buy servers and absorb all of the costs that come with running a data center.

HIGH-AVAILABILITY CONFIGURATION

Where some vendors require you to purchase additional licenses for business continuity and high availability, Duo offers high availability configuration, disaster recovery and data center management tools without busting your budget.

DEPLOYMENT & CONFIGURATION

Duo makes deployment and configuration a snap. Your in-house resources can install, test and troubleshoot Duo in just minutes.

END USER ENROLLMENT

With Duo, end user enrollment is a breeze — end users can simply download the Duo Mobile app for free, enrolling themselves to get started with Duo in seconds.

ADMINISTRATIVE SUPPORT

Duo offers easy deployment with the help of drop-in integrations for all major apps and APIs, and an administrative panel for user and solution management.

PATCHES, MAINTENANCE & UPGRADES

Duo offers automatic application updates, with patch management, maintenance and live support at no extra cost.

ADMINISTRATIVE MAINTENANCE

Duo makes routine tasks like adding new users, revoking credentials or replacing tokens quick and easy, meaning your administrative resources won't have to do another full-time job to maintain your Duo deployment.

SUPPORT & HELPDESK

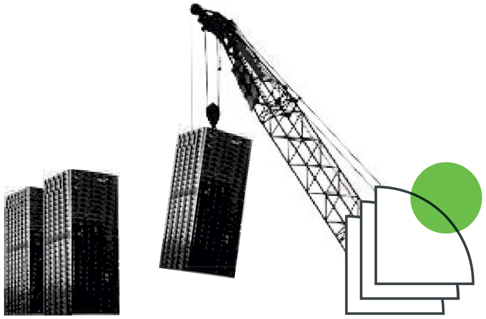
Duo has an extensive library of free resources to answer any and all questions you may have. Duo also offers live support at no extra cost, and with **Duo Care** premium support, you can receive 24/7 white glove service for a small fee.

BUDGET CONSOLIDATION

With Duo, you can replace the need for multiple different hardware and software security solutions that solve for isolated use cases, like authentication, network access control, endpoint security, vulnerability assessment tools, etc. with a single cloud service that provides multi-factor authentication, device trust, single sign-on and adaptive policies and controls.

Duo's trusted access solution provides a comprehensive security platform that eliminates the need — and budget — for many disparate access management tools that may prove difficult to fully integrate. The value is in consolidation, filtering out as much of the noise as possible and giving a comprehensive dashboard that gives a birds-eye view and the ability to quickly zoom in to the granular details where attention is needed. MFA is one step in securing access, and as we've grown and developed, we've built on that to cover more steps.

Duo is flexible enough to scale quickly, letting you easily add new apps, users, or change security policies as you grow.



Time to Value

PROOF OF CONCEPT

Duo lets you try before you buy, helping you set up pilot programs before deploying to your entire organization, with extensive documentation and knowledge articles to help guide you through the evaluation stage. **View Duo's documentation**.

DEPLOYMENT

For faster and easier deployment, Duo provides drop-in integrations for all major **cloud apps**, **VPNs**, **UNIX** and **MS** remote access points, as well as support for **web SDK and APIs**. Quickly **provision new users** with bulk enrollment, self-enrollment, Microsoft Active Directory synchronization, or with the use of **Duo Access Gateway** for cloud-based applications.

ONBOARDING & TRAINING USERS

Duo's authentication app, **Duo Mobile**, allows users to quickly download the app onto their devices, while a **self-service portal** also lets users manage their own accounts and devices via an easy web-based login, reducing help desk tickets and support time.

Required Resources

APPLICATION SUPPORT

Duo integrates easily with your on-premises or cloud-based applications, with no need for extra hardware, software or agents. Duo's extensive documentation, APIs and SDKs make for seamless implementation, reducing the need for a dedicated IT or security team.

USER & DEVICE MANAGEMENT

Duo's administrative panel allows admins to support users and devices using one centralized dashboard. Log into the web-based portal to manage user accounts and devices, generate bypass codes, add phones to users and more. Duo's self-service portal enables users to manage their own devices, reducing administrative support time for simple tasks.

MAINTENANCE

As a cloud-hosted solution, Duo covers the infrastructure and maintenance, letting you focus on your core business objectives. Since security and other updates are rolled out frequently and automatically to patch for the latest vulnerabilities, you don't need to hire a dedicated team to manage the solution. Duo's solution is flexible enough to scale quickly, letting you easily add new applications, users or change security policies as needed.

Dedicated, Responsive Support

To answer your questions before, during and after your Duo deployment, you can count on our fully staffed, in-house **Duo Support** team.

Our responsive support team members have the security expertise to quickly assist you with any specific integration needs. Duo's customer support service is included with your solution at no extra charge, with no support contracts required. In addition, we offer extensive **knowledge base** articles to help troubleshoot and quickly fix known issues.

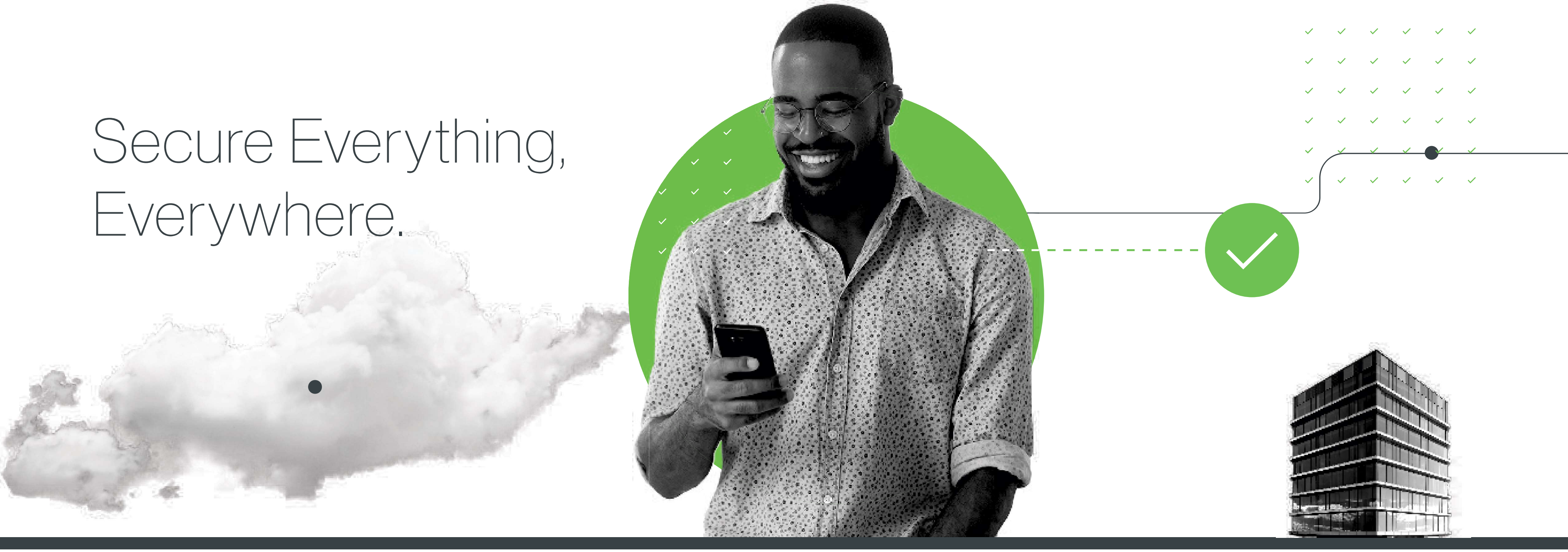
Our **end-user guide** and detailed **documentation** are frequently updated and helpful resources available on Duo.com. For more advanced deployments and specific SLA requirements, we provide **Duo Care**, a premium customer support service with extended coverage and a dedicated Customer Success team.

The Duo Customer Success team equips you with everything you need to roll out your Duo deployment, including a customized launch kit to help with security policies, user training, solution architecture design and more.

Duo is flexible enough to scale quickly, letting you easily add new apps, users, or change security policies as you grow.

> "Duo increased our security and was an easy tool to deploy; every organization should consider it immediately."
>
> **Chad Spiers**
> Director of Information Security, Sentara Healthcare

Secure Everything, Everywhere.



At Duo, we combine security expertise with a user-centered philosophy to provide multi-factor authentication, endpoint remediation and secure single sign-on tools for the modern era. It's so simple and effective, you get the freedom to focus on your mission and leave protecting it to us.

Duo is built on the promise of doing the right thing for our customers and each other. This promise is as central to our business as the product itself. Our four guiding principles are the heart of the sensibility: Easy, Effective, Trustworthy, Enduring.

Duo Security makes security painless, so you can focus on what's important. Duo's scalable, cloud-based trusted access platform addresses security threats before they become a problem, by verifying the identity of your users and the health of their devices before they connect to the applications you want them to access.

Experience advanced multi-factor authentication, endpoint visibility, custom user policies and more with your free 30-day trial. You'll see how easy it is to secure your workforce, from anywhere on any device with Duo MFA.

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and secure access provider. Duo comprises a key pillar of Cisco Secure's Zero Trust offering, the most comprehensive approach to securing access for any user, from any device, to any IT application or environment. Duo is a trusted partner to more than 25,000 customers globally, including Bird, Facebook, Lyft, University of Michigan, Yelp, Zillow and more. Founded in Ann Arbor, Michigan, Duo also has offices in Austin, Texas; San Francisco, California; and London.

DUO

Duo.com

AGENDA ITEM NO. 7.3

BOARD MEMORANDUM

DATE:	June 10, 2024
TO:	**BOARD OF DIRECTORS**
FROM:	Mr. Scott Rogers, Engineering Manager
VIA:	Mr. Dennis D. LaMoreaux, General Manager
RE:	***CONSIDERATION AND POSSIBLE ACTION ON APPROVAL OF AMENDMENT NO. 2 WITH AECOM, INC. FOR PROFESSIONAL SERVICES FOR THE LITTLEROCK DAM REMEDIATING MAINTENANCE ISSUES. ($83,135.75 – BUDGETED – PROJECT NO. 23-607 – ENGINEERING MANAGER ROGERS)***

Recommendation:

Staff recommends that the Board authorize staff to amend the Professional Services Contract with AECOM, Inc. for Professional Services for the Littlerock Dam Remediating Maintenance Issues. Additionally, the hourly rates (attached) for AECOM have increased but no cost increases are expected for the remaining work from the original contract.

Alternative Options:

The alternative is to not award AECOM's proposal.

Impact of Taking No Action:

The impact of taking no action would result in not providing a work plan to meet the California Department of Fish and Wildlife (CDFW) requests.

Background:

The Littlerock Dam has overflowed due to heavy rainfall the past two years causing the existing valve house access road to be partially washed out in several locations. The washouts have caused the existing pipe culverts to be swept away due to the dam overflow. PWD staff was allowed to restore the access road under an emergency repair basis allowed by the CDFW in 2023. However, when the dam overflowed due to heavy rainfall again in April 2024, the CDFW has now requested PWD provide an engineering solution for the access road repair.

Staff prepared a Request for Proposal (RFP) to invite qualified consultants with experience in hydraulic analysis and access road repair. The District received two proposals and one no bid. The engineering staff evaluated the proposals and selected AECOM's proposal based on the qualifications of the firm and project managers' experience with Littlerock Dam. AECOM's project manager was involved with the dam's remediation in the early 1990's. AECOM team's experience with Littlerock Dam will bring institutional knowledge and continuity to this project. The firm will provide the District with a work plan for the access road repair requested to be addressed by the

CDFW. AECOM will also provide access road alternatives evaluation, hydraulic analysis, split channel analysis, and cost estimates.

Strategic Plan Initiative/Mission Statement:

This item is under Strategic Initiative No. 1- Water Resource Reliability.

This item directly relates to the District's Mission Statement.

Budget:

This item is budgeted under Project No. 23-607.

Supporting Documents:

- AECOM, Inc. Proposal
- AECOM, Inc. Hourly Rate Increase

AECOM

AECOM
300 Lakeside Drive
Suite 400
Oakland, CA 94612
aecom.com

May 7, 2024

Mr. Scott Rogers, P.E.
Engineering Manager
Palmdale Water District
2029 East Avenue Q
Palmdale, CA 93550

Subject: Littlerock Dam, PWD Project No. 2023-005
Task 800 – Access Road Repair Assessment – Amendment
Draft Proposed Scope of Work and Fee Estimate

Dear Mr. Rogers:

As discussed in the meeting held on April 23, 2024, this letter presents our draft proposed scope of work and fee estimate for a separate task to evaluate permanent repair of an existing washed-out access road downstream from Littlerock Dam. There are two locations where the stream crosses the access road that will need permanent repair to pass runoff from the Littlerock Dam spillway when it is overtopping. The extent of the access road repairs is approximately 750 feet overall including the two stream crossings. Figure 1 shows the approximate Littlerock Dam access road repair limits and location of the stream crossings.

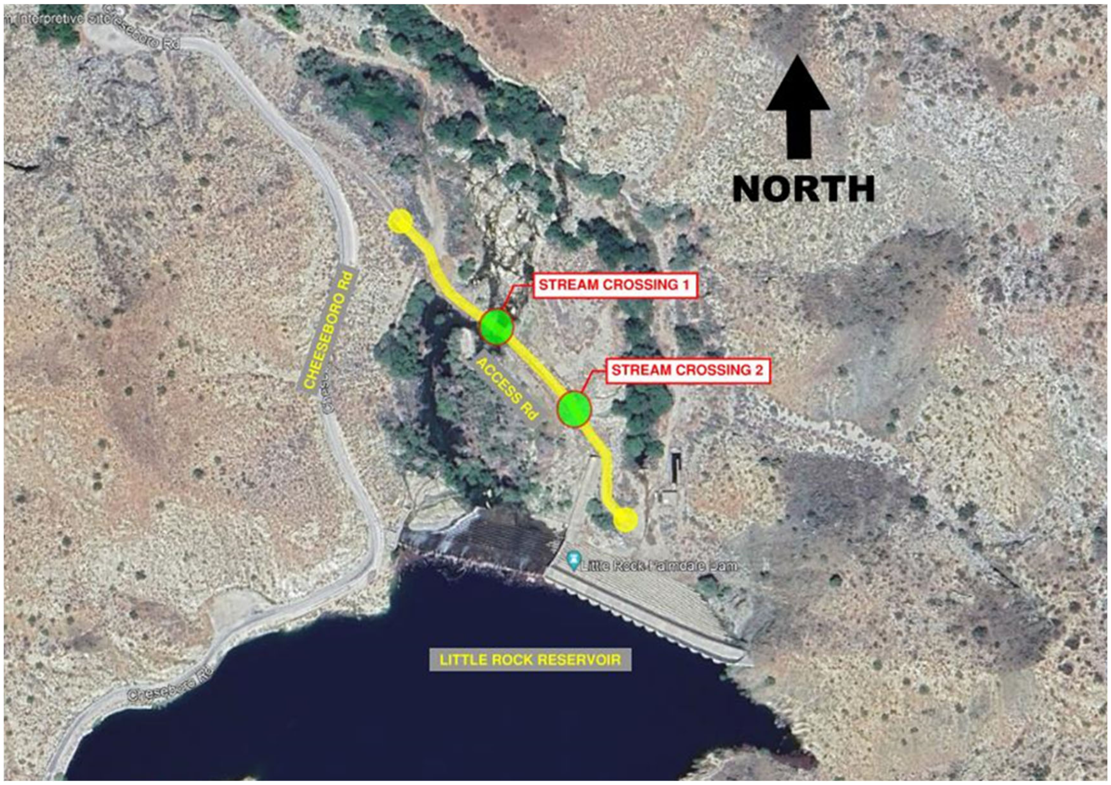


FIGURE 1 – Site Area

An alternatives assessment will be provided to develop three conceptual design alternatives. It is understood that vehicle passage along the downstream access road is not necessary when the spillway is overtopping. Therefore, a concrete ford will be considered as a viable alternative. A hydraulic evaluation of the proposed concepts will also be provided to support the proposed permanent repairs at the stream crossings. Our proposed scope of work and fee estimate for this access road and permanent repairs assessment are presented below.

PROPOSED SCOPE OF WORK

Task 800 - Access Road Permanent Repairs

Task 801 – Data Review & Site Visit

AECOM will conduct a one-day site visit for an AECOM road engineer and a geotechnical engineer of the area that includes a 750-foot section of the existing access road and the two existing stream crossings. The site visit will document existing conditions of the access road, stream crossings, and geologic conditions of the site. A field report with photos and findings will be prepared and submitted to Palmdale Water District (PWD).

Deliverables

- Field Report

Task 802 – Alternatives Evaluation

Three alternative concepts will be evaluated in this scope of work: (1) concrete ford at each crossing, (2) concrete ford combined with culverts, and (3) bridge. All alternatives require hydraulic evaluation. A hydraulic analysis will be provided for each alternative based on a 100-yr design flood event (as reported in the February 1993 Final Design Summary Report, Proposed Dam Modifications, by Woodward-Clyde Consultants). Below is a detailed description of the work performed for the alternatives evaluation task.

802.1 Access Road Alternatives Evaluation

It is understood that vehicle passage of the downstream access road is not necessary when the dam crest is overtopping at the spillway and when the downstream runoff is conveyed through the two existing stream crossings. It is also noted that permanent repairs to the access road are necessary to prevent future damage and/or erosion of the access road embankment after a design flood event. The design requirement is for the access road to not wash out after overtopping of the spillway for an assigned design flood event.

Below is a list of design parameters that will be used in the evaluation:

- The road is gated and is not open to the public. No public access is allowed.
- The access road is 12 feet wide with 3 feet shoulder backing on each side and the roadway section will be a gravel surface road except where overtopping of the road is anticipated.
- The access road will be replaced the same as the existing alignment, without turnouts.
- Access requirements for PWD maintenance vehicles is when the spillway is not overtopping and when water is not conveyed through the stream crossings.
- Design vehicle is a rough terrain crane and the access road does not need to be designed for a drop-deck type truck. Federal Surface Transportation Assistance Act (STAA) trucks and/or California legal trucks will not use this road.
- A concrete ford will be evaluated as an alternative.
- A concrete ford combined with a series of culverts to pass lower flows [less than 6,200cfs (recently recorded flow)] will be evaluated as an alternative.
- A bridge will be evaluated as an alternative. The bridge concept will consider simple spans of less than 150 feet and does not include a structural evaluation. Conceptual design of bridge footings are also not included in this scope of work.

The following conceptual plans will be developed for each concept:

- Existing Conditions and Vicinity Map
- Roadway Plan and Profile
- Typical Sections

802.2 Hydraulic Analysis

The proposed alternatives will be designed to pass a 100-year flood event. A hydraulic analysis for each alternative will be provided based on a 100-yr design flood event (as reported in the February 1993 Final Design Summary Report, Proposed Dam Modifications, by Woodward-Clyde Consultants) to show an estimated design water elevation along with flows and velocities to support the proposed roadway alternatives. Preliminary hydraulic calculations will be developed and submitted along with the alternatives evaluation.

802.3 Split Channel Analysis

A two-dimensional (2D) hydraulic model of the stream crossings from the base of the dam to about 500 feet downstream of the crossings will be developed using the U.S. Army Corps of Engineers Hydraulic Engineering Center's River Analysis System (HEC-RAS). The model will be used to evaluate three scenarios: (1) existing conditions terrain with the 100-year flood, (2) proposed conditions based on one selected alternative with the 100-year flood, and (3) one additional scenario to be selected during the work under Tasks 802.1 and 802.2. We note that this analysis is likely to involve iterations with these two tasks. The results of the 2D model will show which areas downstream of the dam become inundated during the 100-year event along with the water surface elevations, depth of flow, and velocities of flow near the crossing, which will be used to inform the development of the alternative concepts.

802.4 Cost Estimates

Rough order of magnitude (ROM) cost estimates will be developed after the HEC-RAS analysis is complete. ROM will be provided for each alternative based on bid tabs and previous construction contracts within the area.

Assumptions

- Digital terrain data is based on topographic data available to the public.
- Hydrologic data and flow data is based on the February 1993 Final Design Summary Report, Proposed Dam Modifications, by Woodward-Clyde Consultants.
- Palmdale Water District will provide the flood of record for comparison.
- Only the three alternatives listed above will be evaluated.
- The 100-yr flood event is 19,100cfs as reported in the February 1993 Final Design Summary Report, Proposed Dam Modifications, by Woodward-Clyde Consultants. Based on early evaluation and due diligence in the development of this scope of work, a significant number of 8 to 10-foot diameter culverts would be required to convey an event of this size.

Deliverables

- ➢ Three conceptual alternatives in 11x17 .pdf format (Electronic Submittal).
- ➢ Hydraulic calculations supporting the design of the proposed alternatives.
- ➢ Figures in 11x17 .pdf format showing flow depth and flow velocity results from the 2D HEC-RAS model for the three scenarios (six figures total).
- ➢ Three rough order of magnitude cost estimates in MS excel format.

Task 803 – Client and Teams Meetings

A total of three team meetings are included in this scope of work as listed below:

- A kick-off meeting;
- An alternatives meeting; and,
- One additional meeting.

Meeting agendas will be prepared before the meeting. Meeting minutes will also be developed and distributed to the project team to document design decisions and assigned action items.

One conceptual alternative will be selected based on these meetings to be included in a Draft Selected Alternative tech memo (Task 804).

Deliverables

- ➢ Meeting agendas and minutes.

Task 804 – Tech Memo

A selected alternative tech memo will be developed based on PWD's reviews and team meetings. The selected alterative will be described along with assumptions and recommendations for further study. The alternatives that are eliminated will be briefly described to show they were considered and to provide documentation of which factors led to their elimination from further consideration. The tech memo will include discussion of the inputs, assumptions, and results from the hydraulics calculations and the 2D model in Tasks 802.2 and 802.3. Comments from the alternatives meeting will be incorporated in the design and updated in the tech memo.

Deliverables

- ➢ One final conceptual alternative in 11x17 .pdf format (Electronic Submittal).
- ➢ Draft and Final Selected Alternative Tech Memo.

MILESTONE SCHEDULE

TASK DELIVERABLE	DATE
Task 801 - Field Report	5/24/2024
Task 802 - Plans, Calculation, and ROM estimates	6/14/2024
Task 803 – Selected Alternative	6/21/2024
Task 804 – Draft Selected Alternative Tech Memo and Concept plans	7/5/2024
Task 804 - Final Selected Alternative Tech Memo	7/21/2024

This schedule is based on an assumed NTP date of 5/15/2024.

FEE ESTIMATE

We propose to carry out the work for this access road and permanent repairs analysis and selected concept as an amendment to our existing Agreement with the District dated March 2, 2023. The estimated fee is summarized below:

Tasks 100 – 600 (original Agreement, 3/2/23):	$140,468
Task 700 - Electrical Failure Analysis (Amendment):	$ 14,180
Task 800 – Access Road Permanent Repairs Analysis (Amendment):	$ 83,135
Total Estimated Cost:	**$237,783**

The details of the fee estimate are attached. Based on a May 6 email from Mr. Scott Jones, our 2024 billing rates have been escalated 5% above our 2023 rates, which are included in our attached fee estimate. Similar to our original agreement, the work for access road and permanent repairs analysis will be performed on a time-and-materials basis.

For this amendment, Mike Forrest will continue as Project Manager. Please contact Mike at michael.forrest@aecom.com or at 925.998.6875 with any questions.

Sincerely,

Michael P. Forrest.

Mike Forrest, PE, GE
Vice President
Project Manager

Theodore Feldsher

Theodore Feldsher, P.E., G.E.
Vice President
Dams/Water Resources Section Manager

Attachment:
Fee Estimate

	TASK ORDER 800 – ACCESS ROAD PERMANENT REPAIRS	Mike Forrest	Ramesh S.	Kevin Oaks	Shannon Leonard	To be Determined	Aditya Zutshi	To Be Determined	Doug Wright	Syed Kazmi	Total Hours	Total Labor Cost	Other Direct Costs (Travel)	**Total Est. Cost**
		Project Manager	Principal	Project Engineer (Roads)	Hydraulic Engineer*	QA/QC (Principal)	Project Engineer (Geotechnical)	Staff Engineer	Senior CAD/GIS/ Graphics	Principal (Structures)				
	Billing Rate ($/Hr) - Escalated to 2024 (5%)	$ 336.00	$ 336.00	$ 262.50	$ 288.75	$ 336.00	$ 262.50	$ 168.00	$ 168.00	$ 336.00				
801.0	Data Review and Site Visit			12	4		10	6	4		36	$8,610	$ 800	**$9,410**
802.0	Alternatives Evaluation:													
802.1	Access Road Alternatives Evaluation		6	28		4	6	48		4	96	$21,693		**$21,693**
802.2	Hydraulic Evaluation			2	14	2		4			22	$5,912		**$5,912**
802.3	Split Channel Analysis				56				12		68	$18,186		**$18,186**
802.4	Cost Estimates		2	8		2		16		4	32	$7,476		**$7,476**
803.0	Client and Team Meetings	2	2	8	3		3				18	$5,098		**$5,098**
804.1	Selected Alternative Draft Memo	4	2	12	12	3	3	8			44	$11,771		**$11,771**
804.2	Selected Alternative Final Memo	2	2	6				4			14	$3,591		**$3,591**
														$0
	HOURS	8	14	76	89	11	22	86	16	8	330			
	COST	$ 2,688.00	$ 4,704.00	$ 19,950.00	$ 25,698.75	$ 3,696.00	$ 5,775.00	$ 14,448.00	$ 2,688.00	$ 2,688.00		$ 82,335.75	$800.00	**$83,135.75**

*New category and rate.

AECOM

300 Lakeside Drive, Suite 400
Oakland, CA 94612
510.893.3600

May 15, 2024

Palmdale Water District
Attention: Mr. Scott Rogers, P.E.
Engineering Manager
2029 East Avenue Q
Palmdale, CA 93550

Subject: Littlerock Dam Remediating Maintenance Issues - PWD Project No: 2023-005
Request for Billng Rate Increase for 2024

Dear Mr. Rogers:

As discussed, this letter requests a 4 percent rate increase for our services on the subject project for 2024. AECOM's rates have increased from the time the original contract was signed in March 2023. The 2023 and the proposed 2024 rates are shown in the attachment.

We request that the 2024 rates become effective starting on Monday, April 29, 2024.

Please include this requested rate increase in a PWD amendment.

Please contact me if you have any questions.

Sincerely,
AECOM TECHNICAL SERVICES

Michael P. Forrest.

Michael P. Forrest, P.E., G.E.
Project Manager

Attachment: AECOM Rate Table

Cc: Kevin Yao, PWD
Ted Feldsher, AECOM

Littlerock Dam Remediating Maintenance Issues - PWD Project No: 2023-005
AECOM Rate Table

Category	2023 Hourly Rate	2024 Houry Rate*
Principal/QC	$320.00	$333.00
Project Manager	$320.00	$330.00
Hydraulic Engineer (new category)	---	$286.00
Project Engineer	$250.00	$260.00
Staff Engineer	$160.00	$166.00
CAD/Civil	$160.00	$166.00
Admin.	$100.00	$104.00

*Rounded to nearest dollar.

AGENDA ITEM NO. 7.4

Conference/Training Request

Event Name/Date(s):

3rd Annual Water Resiliency Forum: Water As An Economic Engine/June 26, 2024/L.A.

REQUESTED BY:

First Name	Last Name	Date

ACCOMMODATION INFORMATION (If applicable)

Rooms and rates are subject to availability. Complete and submit this form as soon as possible as reservation blocks at host hotels book quickly. In the event that the host hotel is full, every effort will be made to secure a room at the nearest hotel within comparable rates.

Arrival Date	Departure Date	No. of Guests	Room Type
			Single/King Bed

Dietary Restrictions?
If yes, please provide specifics in additional info. box

○ Yes ● No

Smoking Room?

○ Yes ● No

Flight Needed?
If yes, please provide DL# and D.O.B. in additional info. box

□ Yes □ No

Flight Numbers

Departure/Return Times

ADDITIONAL INFORMATION/ REQUESTS

Supervisor Approval (If applicable)

Processed By:

REGISTER NOW

BizFed Institute

Defining the Voice of Business

3rd Annual Water Resiliency Forum: Water As An Economic Engine

June 26th

Metropolitan Water District

700 Alameda St, Los Angeles, CA 90012

8:30 AM - 12 PM

Thank You To Our Sponsors!!

Title

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

Deluxe

CORDOBA CORPORATION

Community

WEST BASIN MUNICIPAL WATER DISTRICT

Grassroots

INFRAMARK

For More Information Contact:

blaine.bacher@bizfedinstitute.org

kevin.harbour@bizfedinstitute.org

Dr. Chris Thornberg • Founder, Beacon Economics

FEATURED SPEAKER

Dr. Thornberg founded Beacon Economics LLC in 2006. Under his leadership the firm has become one of the most respected research organizations in California serving public and private sector clients across the US. Dr. Thornberg also served as Director of the UC Riverside School of Business Center for Economic Forecasting and Development and was an Adjunct Professor at the School from 2015-2023.

He became nationally known for forecasting the subprime mortgage market crash that began in 2007 and was one of the few economists on record to predict the global economic recession that followed. Amidst the 2020 Covid- 19 shock, Dr Thornberg correctly predicted the rapid "V" shaped economic recovery, the inflation that resulted from excessive government stimulus, as well as the sharp hikes in interest and mortgage rates currently impacting U.S. markets.

Karla Nemeth • Director, California Department of Water Resources

KEYNOTE SPEAKER

Karla Nemeth was appointed Director of the California Department of Water Resources by Governor Edmund G. Brown Jr. on January 10, 2018 and was reappointed by Governor Gavin Newsom on June 28, 2019. DWR operates and maintains the CA State Water Project, manages floodwaters, monitors dam safety, conducts habitat restoration, and provides technical assistance and funding for projects for local water needs. Nemeth oversees the Department and its mission to manage and protect California's water resources, working with other agencies in order to benefit the State's people and to protect, restore and enhance the natural and human environments.

Nemeth worked at the CA Natural Resources Agency as Governor Brown's deputy secretary and senior advisor for water policy since 2014. She was Bay Delta Conservation Plan project manager from 2009 to 2014.

Clint Olivier • CEO, BizFed Central Valley
MODERATOR: Panel 1 - Expanding Urban & Agricultural Partnerships

Former Fresno City Council Member Clint Olivier was first elected in 2010 by an overwhelming majority to serve a district of more than 70,000 people in California's fifth-largest city. Olivier represented the Seventh District for two terms, making hundreds of decisions concerning Fresno's billion-dollar-plus budget while advocating passionately for issues important to both his neighbors as well as the business community. During his time in office, Olivier used his extensive knowledge of public and media relations to lead the charge on numerous local and statewide issues.

Nina Hawk • Chief, Bay-Delta Resources
PANELIST: Panel 1 - Expanding Urban & Agricultural Partnerships

Nina Hawk is Bay-Delta Initiatives group manager /chief of Bay-Delta resources for the Metropolitan Water District of Southern California. In this role, she is responsible for managing the development and implementation of Metropolitan's Bay-Delta strategy, including the Bay-Delta Initiatives Program. Hawk joined Metropolitan in 2020 as the Bay-Delta Initiatives policy manager to provide strategic oversight on Bay-Delta programs and projects, including Metropolitan's Bay-Delta Science Program. She also has represented Metropolitan's interests on issues such as the Delta Conveyance program, voluntary agreements, Sites Reservoir, and major statewide/Bay-Delta policy forums.

William Bourdeau • Executive VP, Harris Farming
PANELIST: Panel 1 - Expanding Urban & Agricultural Partnerships

William Bourdeau is executive vice president of Harris Farms, owner of Bourdeau Farms, director of the Westlands Water District, director of American Pistachio Growers, and chairman of the Valley Future Foundation. He has been around farming his entire life and currently works for Harris Farms overseeing over 20,000 acres of diversified crops. He has become involved in many local organizations and currently serves as the Vice Chair of the San Luis & Delta-Mendota Water Authority, Chair of the CA Water Alliance, Chair of San Joaquin Valley Sun, Director at the Westland Water District and a Board member of the Fresno State Agricultural Foundation.

Mike Wade • Executive Director, CA Farm Water Coalition
PANELIST: Panel 1 - Expanding Urban & Agricultural Partnerships

Wade currently serves as the executive director of the California Farm Water Coalition (CFWC) where he has devoted over 20 years to advocating for the needs of farmers and advancing CA agriculture. His extensive background in policy, communications and management has been a great support to farmers. Prior to his role at CFWC, Wade served as executive director of the Merced County Farm Bureau for 11 years and program director of the California Farm Bureau Federation for two and a half years.

Scott Houston • Director, West Basin MWD
MODERATOR: Panel 2 - Keeping Water Safe, Reliable and Affordable

Scott Houston is an elected member of the Board of Directors of West Basin Municipal Water District. First elected in 2014, Director Houston represents the Division IV cities of Culver City, El Segundo, Malibu, West Hollywood and a portion of Hawthorne, and the unincorporated Los Angeles County communities of Del Aire, Marina del Rey, Topanga, and Wiseburn. He is Immediate Past President of the board, Chair of the Finance and Administration Committee, and Member of the Public Information and Education Committee and Ethics Committee. Houston has served as board president in 2019 and 2023.

Maria Mehranian • Managing Partner, Cordoba Corp.,
PANELIST: Panel 2 - Keeping Water Safe, Reliable and Affordable

Maria Mehranian is Managing Partner of Cordoba Corp., CA based full-service engineering, construction management and program management firm specializing in the delivery of infrastructure projects in the transportation, water, energy, and education sectors with offices throughout CA. Cordoba is ranked by ENR as a Top 50 Program Management Firm and a Top 100 Construction Management-for-Fee Firm in the nation, as well as a Top 100 Design firm in CA. For nearly 40 years, Maria has dedicated her career to building Cordoba Corporation into one of the nation's top specialty services firms with its staff of engineers, designers, environmental specialists, and construction professionals from all over the world.

Robert Sausedo • President & CEO, Community Build

PANELIST: Panel 2 - Keeping Water Safe, Reliable and Affordable

Robert Sausedo is the President and CEO of Community Build Inc., a 27-year-old legacy organization in South Los Angeles. A native Angeleno, Sausedo has been engaged and involved with civic matters that impact youth, economic development, social justice and literacy for over 30 years. He, along with several of his colleagues, led a post-1992 Civil Unrest effort to rebuild and expand the Jefferson – Vassie D. Wright Memorial Branch Library in the Jefferson Park community of Los Angeles. Prior to joining CBI, Mr. Sausedo served as Deputy for Agency and Review for LA County Board of Supervisor Mark Ridley-Thomas. His responsibilities included a broad portfolio covering economic development, community engagement, commission appointments and development.

Conference/Training Request

Event Name/Date(s):

AV EDGE 2024 Installation Dinner/July 11, 2024/Palmdale

REQUESTED BY:

First Name	Last Name	Date

ACCOMMODATION INFORMATION (If applicable)

Rooms and rates are subject to availability. Complete and submit this form as soon as possible as reservation blocks at host hotels book quickly. In the event that the host hotel is full, every effort will be made to secure a room at the nearest hotel within comparable rates.

Arrival Date	Departure Date	No. of Guests	Room Type
			Single/King Bed

Dietary Restrictions?
If yes, please provide specifics in additional info. box

○ Yes ○ No

Smoking Room?

○ Yes ○ No

Flight Needed?
If yes, please provide DL# and D.O.B. in additional info. box

□ Yes □ No

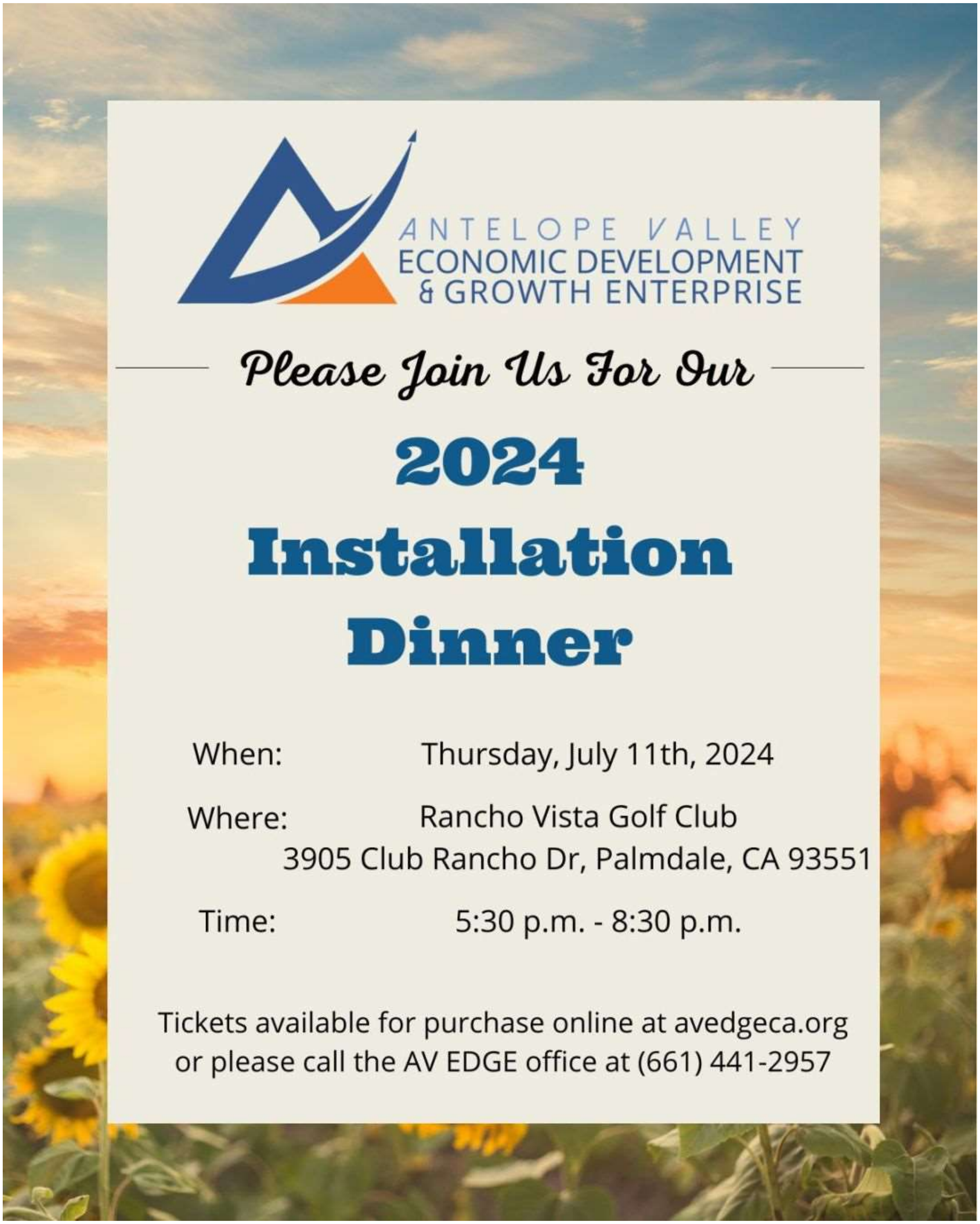
Flight Numbers

Departure/Return Times

ADDITIONAL INFORMATION/ REQUESTS

Supervisor Approval (If applicable)

Processed By:



ANTELOPE VALLEY
ECONOMIC DEVELOPMENT
& GROWTH ENTERPRISE

Please Join Us For Our

2024 Installation Dinner

When: Thursday, July 11th, 2024

Where: Rancho Vista Golf Club
3905 Club Rancho Dr, Palmdale, CA 93551

Time: 5:30 p.m. - 8:30 p.m.

Tickets available for purchase online at avedgeca.org or please call the AV EDGE office at (661) 441-2957

AGENDA ITEM NO. 8.1

MINUTES OF MEETING OF THE OUTREACH COMMITTEE OF THE PALMDALE WATER DISTRICT, MAY 2, 2024

A meeting of the Outreach Committee of the Palmdale Water District was held Thursday, May 2, 2024, at 2029 East Avenue Q, Palmdale, CA 93550. Chair Dino called the meeting to order at 1:30 p.m.

1) Roll Call.

Attendance:

Committee:
Vincent Dino, Chair
Cynthia Sanchez, Committee Member

Others Present:

Dennis LaMoreaux, General Manager
Dennis Hoffmeyer, Finance Manager
Claudia Bolanos, Resource and Analytics Spvsr.
Trisha Guerrero, Management Analyst

2) Adoption of Agenda.

It was moved by Committee Member Sanchez, seconded by Chair Dino, and unanimously carried by all members of the Committee present at the meeting to adopt the agenda, as written.

3) Public Comments for Non-Agenda Items.

There were no public comments for non-agenda items.

4) Action Items: (The Public Shall Have an Opportunity to Comment on Any Action Item as Each Item is Considered by the Committee Prior to Action Being Taken.)

4.1) Consideration and Possible Action on Proposal from Katz & Associates for Media Training. ($11,000.00 – Not-to-Exceed – Public Affairs Director Shay)

General Manager LaMoreaux provided an overview of the proposal received from Katz & Associates for the recommended media training for staff and the Board of Directors in relation to the Pure Water Antelope Valley Demonstration Facility and the scheduled groundbreaking date of June 20, 2024 after which it was moved by Committee Member Sanchez, seconded by Chair Dino, and unanimously carried by all members of the Committee present at the meeting to approve the proposal from Katz & Associates for Media Training in the not-to-exceed amount of $11,000.00.

5) Board Members' Requests for Future Agenda Items.

There were no requests for future agenda items.

6) Date of Next Committee Meeting.

It was determined that the next Outreach Committee meeting will be held May 30, 2024, at 10:00 a.m.

7) Adjournment.

There being no further business to come before the Outreach Committee, the meeting was adjourned at 1:34 p.m.

Chair

MINUTES OF MEETING OF THE OUTREACH COMMITTEE OF THE PALMDALE WATER DISTRICT, MARCH 18, 2024

A meeting of the Outreach Committee of the Palmdale Water District was held Monday, March 18, 2024, at 2029 East Avenue Q, Palmdale, CA 93550. Chair Dino called the meeting to order at 10:30 a.m.

1) Roll Call.

Attendance:

Committee:
Vincent Dino, Chair
Cynthia Sanchez, Committee Member

Others Present:

Dennis LaMoreaux, General Manager
Adam Ly, Assistant General Manager
Judy Shay, Public Affairs Director
Joe Marcinko, Operations Manager
Claudia Bolanos, Resource and Analytics Spvsr.
Don Wilson, Committee Member Alternate
Danielle Henry, Executive Assistant
Patricia Guerrero, Management Analyst
0 members of the public

2) Adoption of Agenda.

It was moved by Committee Member Sanchez, seconded by Chair Dino, and unanimously carried by all members of the Committee present at the meeting to adopt the agenda, as written.

3) Public Comments for Non-Agenda Items.

There were no public comments for non-agenda items.

4) Action Items: (The Public Shall Have an Opportunity to Comment on Any Action Item as Each Item is Considered by the Committee Prior to Action Being Taken.)

4.1) Consideration and Possible Action on Approval of Minutes of Meeting Held July 25, 2023.

It was moved by Committee Member Sanchez, seconded by Chair Dino, and unanimously carried by all members of the Committee present at the meeting to approve the minutes of the Outreach Committee meeting held July 25, 2023, as written.

4.2) Discussion of 2024 Outreach Activities. (Public Affairs Director Shay)

a) Outreach Report.

Public Affairs Director Shay provided a detailed overview of the written Outreach Report of current events through March 12 including press releases, print publications, customer outreach, social media highlights, and participation in various events including filming with Three Leaves Media Production for new PWD videos, Coffee with Director Kellerman, and the February SDANLAC membership luncheon which brought the highest attendance, and then stated that the District's Public Affairs team won the CAPIO award and was featured in CSDA Magazine; that she's been appointed to a second term on the ACWA Communications Committee; and that the most clicked article on ACWA's website in January was regarding the resignation of former Director Dizmang.

b) Upcoming Events/2024 Plans.

She then stated that upcoming events include the Water Ambassadors Academy on April 3, 10, 17 & 20, Let's Talk H2O! 2024 Water Supply on May 2, Littlerock Dam's 100th anniversary celebration on June 1, and the Pure Water AV Demonstration Facility groundbreaking on June 18 followed by a brief discussion of Littlerock Dam's 100th anniversary celebration attendance.

5) Reports.

5.1) Water-Use Efficiency Activities. (Resource and Analytics Supervisor Bolanos)

Resource and Analytics Supervisor Bolanos reported that staff participated in three classroom presentations earlier this year and that additional presentations are scheduled this week; that the Water-Wise Workshop: Spring Bloom was held on March 14; and that staff is preparing a poster contest for Earth Day.

She then provided a presentation on the Water-Wise Landscape Conversion Program, including before and after photos of the landscape conversions and details of the reduced water usage and customer savings and then stated that 60 applications were received in 2023 of which 43 were completed totaling a conversion of 54,593 sq. ft. and $84,507 awarded in rebates.

5.2) Lobbying Activities. (Assistant General Manager Ly)

Assistant General Manager Ly stated that a copy of the 2024 Legislative Report has been distributed and then provided a brief legislative update on ACA 2 regarding the transfer of 3% of water in state revenues into the Water and Wildfire Resiliency Fund, on AB 1573 regarding updating the model landscape ordinance every 3 years, on AB 1820 regarding the requirement by local agencies to provide development fees within 10 business days, on AB 2257 regarding Prop 218 responses to timely submitted written objections, on SCA 7 regarding employees' right to organize and join a union, on SB 1210 regarding prohibiting a utility connection charge from exceeding 1% of the reported building permit value, on SB 1255 regarding requiring the State Water Board to develop a needs analysis of the public water systems on or before May 1, 2025, and on SB 1330 regarding urban water use objective variances.

He then stated that Reeb Government Relations is currently working on an updated report on bills relating to the District and suggested that the Committee Members meet with Mr. Reeb during the upcoming ACWA Spring Conference.

6) Board Members' Requests for Future Agenda Items.

There were no requests for future agenda items.

7) Date of Next Committee Meeting.

It was determined that the next Outreach Committee meeting will be held April 15, 2024, at 10:30 a.m.

8) Adjournment.

There being no further business to come before the Outreach Committee, the meeting was adjourned at 10:53 a.m.

Chair