COASTSIDE COUNTY WATER DISTRICT

766 MAIN STREET

HALF MOON BAY, CA 94019

REGULAR MEETING OF THE BOARD OF DIRECTORS

Tuesday, December 8, 2020 - 7:00 p.m.

AGENDA

On March 17, 2020, the Governor issued Executive Order N-29-20 suspending certain provisions of the Ralph M. Brown Act in order to allow for local legislative bodies to conduct their meetings telephonically or by other electronic means. Pursuant to the Shelter-in-Place Order issued by the San Mateo County Health Officer on March 16, 2020, as revised on March 31, 2020, the statewide Shelter-in-Place Order issued by the Governor in Executive Order N-33-20 on March 19, 2020, and the CDC's social distancing guidelines which discourage large public gatherings, the Boardroom will not be open for the December 8, 2020 Regular Meeting of the Coastside County Water District. This meeting will be conducted remotely via teleconference.

The Public may watch and/or participate in the public meeting by joining the meeting through the Zoom Videoconference link provided below. The public may also join the meeting by calling the below listed teleconference phone number.

How to Join Online or by Phone

The meeting will begin at 7:00 p.m.

Whether you participate online or by telephone, you may wish to "arrive" early so that staff can address any technology questions prior to the start of the meeting.

ONLINE:

Join Zoom Meeting
https://zoom.us/j/93778260596?pwd=aEpRcFlnaHdQM21PSEJQWjNiN09TQT09

Meeting ID: 937 7826 0596
Passcode: 184355

One tap mobile
+16699006833,,93778260596#,,,,,,0#,,184355# US (San Jose)

Dial by your location
+1 669 900 6833 US (San Jose)

Meeting ID: 937 7826 0596
Passcode: 184355

Find your local number: https://zoom.us/u/adZt3d9LjB

Procedures to make a public comment with Zoom Video/Conference – As a reminder, all participants except the Board Members and Staff are muted on entry.

- ***From a computer:*** *(1) Using the Zoom App. at the bottom of your screen, click on "Participants" and then "Raise Hand". Participants will be called to comment in the order in which they are received. Begin by stating your name and place of residence.*

  OR

- *(2) Using the Zoom App, at the bottom of your screen click on "Chat" and then type that you wish to make a comment into the Chat Box. Ensure that the "To:" field is populated by either "Everyone" or "the Moderator". Begin by stating your name and place of residence.*

- ***From a phone:*** *Using your keypad, dial *9, and this will notify the Moderator that you have raised your hand. Begin by stating your name and place of residence. The Moderator will call on you by stating the last 4 digits of your phone number. If you wish to block your phone number dial *67 prior to dialing in. If your phone number is not displayed, the Moderator will call you by Caller number.*

The Coastside County Water District (CCWD) does not discriminate against persons with disabilities. Upon request, the agenda and agenda packet materials can be provided in a format to accommodate special needs. If you require a copy of the agenda or related materials in an alternative format to accommodate a disability, or if you wish to attend this public meeting and will require special assistance or other special equipment, please call the District at (650) 726-4405 in advance and we will make every reasonable attempt to provide such an accommodation.

All public records relating to an open session item on this agenda, which are not exempt from disclosure pursuant to the California Public Records Act, that are distributed to a majority of the legislative body will be available for public inspection at the CCWD District Office, located at 766 Main Street, Half Moon Bay, CA at the same time that the public records are distributed or made available to the legislative body.

This agenda and accompanying materials can be viewed on Coastside County Water District's website located at: www.coastsidewater.org.

The Board of the Coastside County Water District reserves the right to take action on any item included on this agenda.

1) ROLL CALL

2) PLEDGE OF ALLEGIANCE

3) PUBLIC COMMENT

At this time members of the public may address the Board of Directors on issues not listed on the agenda which are within the purview of the Coastside County Water District. Comments on matters that are listed on the agenda may be made at the time the Board is considering each item. Each speaker is allowed a maximum of three (3) minutes and must complete and submit a speaker slip. The President of the Board will recognize each speaker, at which time the speaker should proceed to the podium, give their name and address and provide their comments to the Board.

4) SPECIAL ORDER OF BUSINESS (attachment)

Administration of Oath of Office to Newly Re-elected Directors Glenn Reynolds and Ken Coverdell and Newly Elected Director John Muller.

5) CONSENT CALENDAR

The following matters before the Board of Directors are recommended for action as stated by the General Manager. All matters listed hereunder constitute a Consent Calendar, are considered as routine by the Board of Directors, and will be acted upon by a single vote of the Board. There will be no separate discussion of these items unless a member of the Board so requests, in which event the matter shall be removed from the Consent Calendar and considered as a separate item.

A. Approval of disbursements for the month ending November 30, 2020:
Claims: $761,123.30; Payroll: $173,375.04 for a total of $934,498.34 (attachment)
- *November 2020 Monthly Financial Claims reviewed by and approved by Director Coverdell*

B. Acceptance of Financial Reports (attachment)
C. Approval of Minutes of November 10, 2020 Regular Board of Directors Meeting (attachment)
D. Installed Water Connection Capacity and Water Meters Report (attachment)
E. Total CCWD Production Report (attachment)
F. CCWD Monthly Sales by Category Report-November 2020 (attachment)
G. Monthly Planned Plant or Tank Discharge and New Water Line Flushing Report (attachment)
H. Monthly Rainfall Reports (attachment)
I. SFPUC Hydrological Report for the Month of October 2020 (attachment)
J. Water Service Connection Transfer Report – November 2020 (attachment)

6) MEETINGS ATTENDED / DIRECTOR COMMENTS

7) GENERAL BUSINESS

A. Election of Coastside County Water District Board President and Vice-President (attachment)
B. Approval of Coastside County Water District Response to Grand Jury Report Entitled "Ransomeware: It Is Not Enough To Think You Are Protected." (attachment)

8) MONTHLY INFORMATIONAL REPORTS

A. Superintendent of Operations Report (attachment)
B. Water Resources Report (attachment)

9) DIRECTOR AGENDA ITEMS – REQUESTS FOR FUTURE BOARD MEETINGS

10) ADJOURNMENT

CERTIFICATE OF THE CHIEF ELECTIONS OFFICER

State of California
SS.
County of San Mateo

I, MARK CHURCH, Chief Elections Officer of the County of San Mateo, State of California, do hereby certify that:

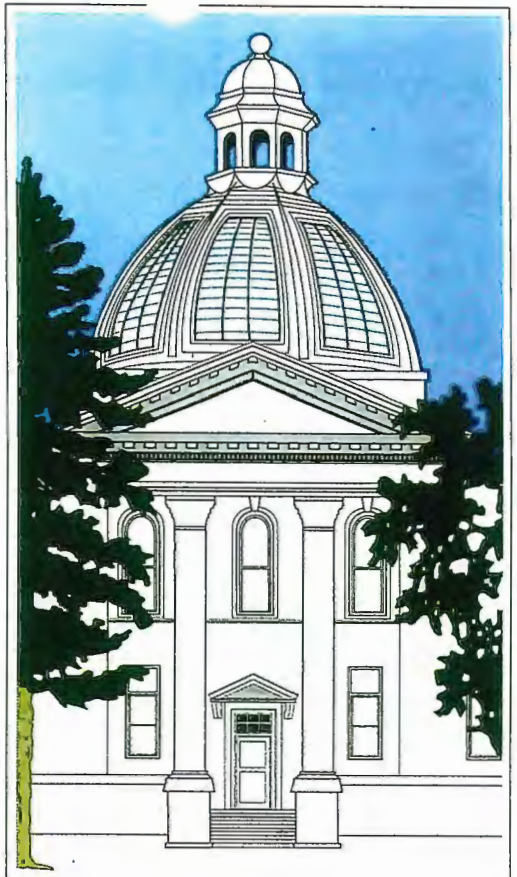
WHEREAS, the number of nominees for the Office of Member, Board of Directors, does not exceed the number of offices required by law to be filled at the Presidential General Election within the COASTSIDE COUNTY WATER DISTRICT ZONES 1, 3, and 4, held on November 3, 2020, the time within which nominations may be made has expired, and a petition signed by ten percent (10%) of the voters or 50 voters, whichever is the smaller number, requesting that said election be held, was not presented to the Chief Elections Officer within the time provided by law.

NOW, THEREFORE, pursuant to Elections Code §10515, the following qualified persons as listed below, are required to be appointed to three (3) seats for four (4) year terms:

Zone 1: Glenn Reynolds
Zone 3: Kenneth Lee Coverdell
Zone 4: John Muller

IN WITNESS WHEREOF, I hereunto affix my hand and seal this 3rd day of December, 2020, and file this date with the General Manager of the COASTSIDE COUNTY WATER DISTRICT.

MARK CHURCH
Chief Elections Officer &
Assessor-County Clerk-Recorder



COUNTY OF SAN MATEO
CERTIFICATION OF ELECTION

This is to certify that

Glenn Reynolds

was appointed to the office of

Member, Board of Directors

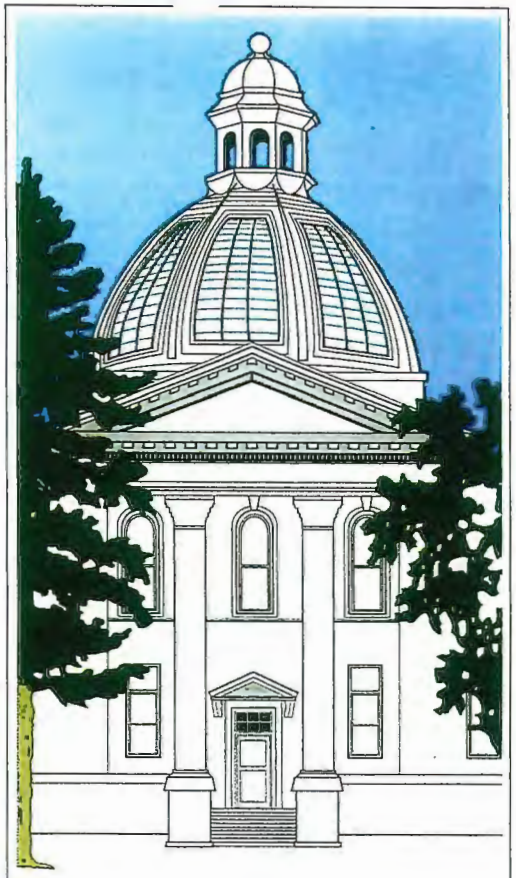
Coastside County Water District

Zone 1

In lieu of holding the Presidential General Election in San Mateo County on the 3rd day of November, 2020.

In witness whereof, I have hereunto set my hand and affixed my official seal this 3rd day of December, 2020.

MARK CHURCH
Chief Elections Officer &
Assessor-County Clerk-Recorder



COUNTY OF SAN MATEO
CERTIFICATION OF ELECTION

This is to certify that

Kenneth Lee Coverdell

was appointed to the office of

Member, Board of Directors

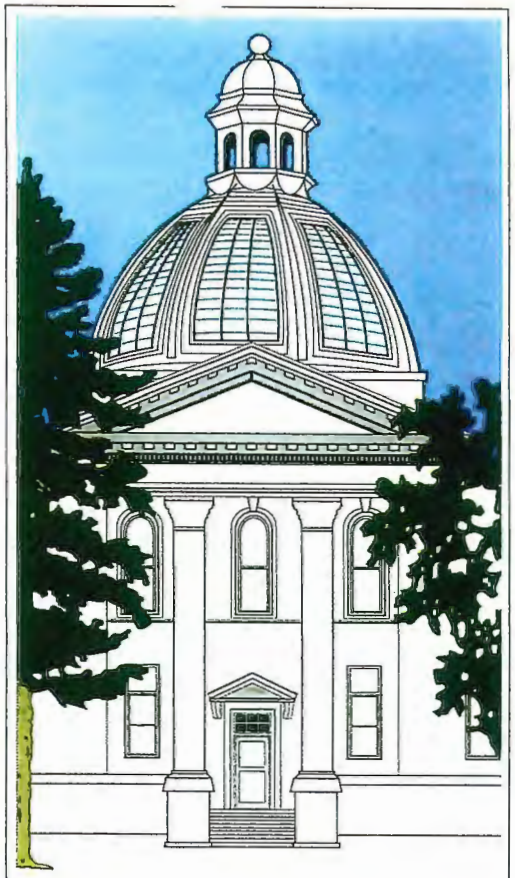
Coastside County Water District

Zone 3

In lieu of holding the Presidential General Election in San Mateo County on the 3rd day of November, 2020.

In witness whereof, I have hereunto set my hand and affixed my official seal this 3rd day of December, 2020.

MARK CHURCH
Chief Elections Officer &
Assessor-County Clerk-Recorder



COUNTY OF SAN MATEO
CERTIFICATION OF ELECTION

This is to certify that

John Muller

was appointed to the office of

Member, Board of Directors

Coastside County Water District

Zone 4

In lieu of holding the Presidential General Election in San Mateo County on the 3rd day of November, 2020.

In witness whereof, I have hereunto set my hand and affixed my official seal this 3rd day of December, 2020.

MARK CHURCH
Chief Elections Officer &
Assessor-County Clerk-Recorder

OATH OF OFFICE

FOR

MEMBER OF BOARD OF DIRECTORS
COASTSIDE COUNTY WATER DISTRICT

I_____, do solemnly swear (or affirm) that I will support and defend the Constitution of the United States and the Constitution of the State of California against all enemies, foreign and domestic; that I will bear true faith and allegiance to the Constitution of the United States and the Constitution of the State of California; that I take this obligation freely, without any mental reservation or purpose of evasion, and that I will well and faithfully discharge the duties upon which I am about to enter.

Date December 8, 2020

_____
(Name)

Sworn to (or affirmed) before me

_____
Chris R. Mickelsen, President
Board of Directors
Coastside County Water District

COASTSIDE COUNTY WATER DISTRICT
CLAIMS FOR NOVEMBER 2020

CHECKS			
CHECK DATE	**CHECK NO.**	**VENDOR**	**AMOUNT**
11/02/2020	28859	CITY OF HALF MOON BAY	$ 1,275.00
11/02/2020	28860	NORTH AMERICAN TITLE CO, INC	$ 1,500.00
11/10/2020	28861	ADP, INC.	$ 720.20
11/10/2020	28862	HEALTH BENEFITS ACWA-JPIA	$ 43,791.73
11/10/2020	28863	AT&T	$ 6,186.81
11/10/2020	28864	AT&T LONG DISTANCE	$ 1,756.85
11/10/2020	28865	AZEVEDO FEED INC.	$ 993.92
11/10/2020	28866	CALIFORNIA C.A.D. SOLUTIONS, INC	$ 5,445.00
11/10/2020	28867	CALIFORNIA SPECIAL DISTRICT	$ 7,805.00
11/10/2020	28868	COMCAST	$ 222.30
11/10/2020	28869	RECORDER'S OFFICE	$ 101.00
11/10/2020	28870	JAMES COZZOLINO, TRUSTEE	$ 200.00
11/10/2020	28871	HMB GRADING & PAVING INC.	$ 10,996.25
11/10/2020	28872	HASSETT HARDWARE	$ 2,396.95
11/10/2020	28873	HUE & CRY, INC.	$ 24.00
11/10/2020	28874	KOFFLER ELECTRICAL MECHANICAL APPARATUS REPAIR	$ 214.55
11/10/2020	28875	MASS MUTUAL FINANCIAL GROUP	$ 1,050.00
11/10/2020	28876	VERIZON CONNECT NWF, INC.	$ 247.00
11/10/2020	28877	PACIFIC GAS & ELECTRIC CO.	$ 69,734.66
11/10/2020	28878	REPUBLIC SERVICES	$ 562.20
11/10/2020	28879	SAN FRANCISCO WATER DEPT.	$ 343,324.62
11/10/2020	28880	SAN MATEO CTY TAX COLLECTOR	$ 308.34
11/10/2020	28881	SAN MATEO CTY TAX COLLECTOR	$ 516.28
11/10/2020	28882	SAN MATEO CTY TAX COLLECTOR	$ 102.80
11/10/2020	28883	STANDARD INSURANCE COMPANY	$ 577.17
11/10/2020	28884	TEAMSTERS LOCAL UNION #856	$ 1,331.00
11/10/2020	28885	TPX COMMUNICATIONS	$ 2,046.63
11/10/2020	28886	TRI COUNTIES BANK	$ 5,361.87
11/10/2020	28887	VALIC	$ 6,280.00
11/10/2020	28888	US BANK NA	$ 2,088.32
11/24/2020	28889	A-1 SEPTIC TANK SERVICE	$ 650.00
11/24/2020	28890	ANALYTICAL ENVIRONMENTAL SERVICES	$ 27,226.39
11/24/2020	28891	ANDREINI BROS. INC.	$ 38,596.73
11/24/2020	28892	AT&T	$ 148.92
11/24/2020	28893	AZTEC GARDENS, INC.	$ 218.00
11/24/2020	28894	BADGER METER, INC.	$ 66.00
11/24/2020	28895	BALANCE HYDROLOGICS, INC	$ 5,151.61
11/24/2020	28896	BAY AREA AIR QUALITY MGMT DIST	$ 412.00
11/24/2020	28897	BAY AREA AIR QUALITY MGMT DIST	$ 434.00
11/24/2020	28898	BAY ALARM COMPANY	$ 1,287.84
11/24/2020	28899	BFI OF CALIFORNIA, INC.	$ 554.69
11/24/2020	28900	BIG CREEK LUMBER	$ 640.81
11/24/2020	28901	KRYSTLE A. RENEER	$ 18,250.00
11/24/2020	28902	CALCON SYSTEMS, INC.	$ 13,058.01
11/24/2020	28903	CALIFORNIA C.A.D. SOLUTIONS, INC	$ 900.00
11/24/2020	28904	CHEMTRADE CHEMICALS US LLC	$ 5,106.72
11/24/2020	28905	PETTY CASH	$ 49.04
11/24/2020	28906	COMMUNICATION LEASING SERVICES, INC	$ 1,035.87
11/24/2020	28907	CUMMINS, INC	$ 925.60
11/24/2020	28908	DATAPROSE, LLC	$ 3,531.82
11/24/2020	28909	DE LAGE LANDEN FINANCIAL SERVICES, INC.	$ 876.14
11/24/2020	28910	MICHAEL DE MEO	$ 2,785.59
11/24/2020	28911	HUGH DOHERTY, JR	$ 176.90
11/24/2020	28912	HUGH DOHERTY, JR	$ 176.90
11/24/2020	28913	GRAINGER, INC.	$ 135.88
11/24/2020	28914	KELLY HOFFMAN-DAVIS	$ 43.70
11/24/2020	28915	HMB BLDG. & GARDEN INC.	$ 29.49
11/24/2020	28916	HANSONBRIDGETT. LLP	$ 10,319.00
11/24/2020	28917	IRON MOUNTAIN	$ 1,010.12
11/24/2020	28918	IRVINE CONSULTING SERVICES, INC.	$ 4,754.05
11/24/2020	28919	GLENNA LOMBARDI	$ 104.00

11/24/2020	28920	MASS MUTUAL FINANCIAL GROUP	$	1,050.00
11/24/2020	28921	MILLER SPATIAL SERVICES, LLC	$	16,000.00
11/24/2020	28922	MISSION UNIFORM SERVICES INC.	$	210.92
11/24/2020	28923	MONTEREY COUNTY LAB	$	1,180.00
11/24/2020	28924	MTA PARTS, INC.	$	433.56
11/24/2020	28925	OCCUPATIONAL HEALTH CENTERS OF CALIFORNIA, A MEDICAL CORP.	$	221.00
11/24/2020	28926	OFFICE DEPOT	$	441.77
11/24/2020	28927	PACIFICA COMMUNITY TV	$	300.00
11/24/2020	28928	PAPE MACHINERY EXCHANGE	$	2,077.37
11/24/2020	28929	PAULO'S AUTO CARE	$	229.74
11/24/2020	28930	RAFTELIS FINANCIAL CONSULTANTS, INC.	$	2,165.00
11/24/2020	28931	RAY A MORGAN COMPANY INC.	$	1,833.22
11/24/2020	28932	MULTI SERVICE TECHNOLOGY SOLUTIONS, INC.	$	300.00
11/24/2020	28933	REDWOOD TRADING POST	$	1,200.78
11/24/2020	28934	ROBERTS & BRUNE CO.	$	1,116.28
11/24/2020	28935	ROGUE WEB WORKS, LLC	$	424.00
11/24/2020	28936	SAN MATEO CTY PUBLIC HEALTH LAB	$	176.00
11/24/2020	28937	CALIFORNIA DEPARTMENT OF TAX AND FEE ADMINISTRATION	$	854.70
11/24/2020	28938	STETSON ENGINEERS, INC.	$	12,436.48
11/24/2020	28939	TEAMSTERS LOCAL UNION #856	$	1,331.00
11/24/2020	28940	JAMES TETER	$	1,325.00
11/24/2020	28941	UNIVAR SOLUTIONS USA INC.	$	3,590.00
11/24/2020	28942	UPS STORE	$	241.05
11/24/2020	28943	VALIC	$	6,280.00
11/24/2020	28944	JUAN CARLOS SALAZAR	$	3,360.00
11/24/2020	28945	WIENHOFF & ASSOCIATES, INC.	$	800.00
11/24/2020	28946	WRA, INC.	$	7,727.02
11/24/2020	28947	PAOLA FERRARI	$	17.12
11/24/2020	28948	ARANZAZU CASAL	$	375.55
11/24/2020	28949	MICHAEL P. SULLIVAN JR.	$	50.92
11/24/2020	28950	PRESIDIO SYSTEMS, INC.	$	847.76
		SUBTOTAL CLAIMS FOR MONTH	$	724,412.51

WIRE PAYMENTS

MONTH		VENDOR		AMOUNT
11/13/2020	DFT0000329	PUB. EMP. RETIRE SYSTEM	$	14,237.84
11/25/2020	DFT0000330	PUB. EMP. RETIRE SYSTEM	$	14,333.82
11/30/2020		BANK AND CREDIT CARD FEES	$	8,139.13
		SUBTOTAL WIRE PAYMENTS FOR MONTH	$	36,710.79

TOTAL CLAIMS FOR THE MONTH	**$**	**761,123.30**

Coastside County Water District

Monthly Budget Report

Account Summary

For Fiscal: 2020-2021 Period Ending: 11/30/2020

		November Budget	November Activity	Variance Favorable (Unfavorable)	Percent Variance	YTD Budget	YTD Activity	Variance Favorable (Unfavorable)	Percent Variance	Total Budget
Revenue										
RevType: 1 - Operating										
1-4120-00	Water Revenue	1,054,363.00	1,019,233.03	-35,129.97	-3.33 %	5,886,512.00	6,142,236.23	255,724.23	4.34 %	12,096,000.00
	Total RevType: 1 - Operating:	**1,054,363.00**	**1,019,233.03**	**-35,129.97**	**-3.33 %**	**5,886,512.00**	**6,142,236.23**	**255,724.23**	**4.34 %**	**12,096,000.00**
RevType: 2 - Non-Operating										
1-4170-00	Water Taken From Hydrants	4,165.00	6,153.46	1,988.46	47.74 %	20,825.00	33,681.31	12,856.31	61.73 %	50,000.00
1-4180-00	Late Notice - 10% Penalty	0.00	0.00	0.00	0.00 %	0.00	-2.89	-2.89	0.00 %	25,000.00
1-4230-00	Service Connections	833.00	648.24	-184.76	-22.18 %	4,165.00	2,902.89	-1,262.11	-30.30 %	10,000.00
1-4920-00	Interest Earned	4,688.00	2,500.16	-2,187.84	-46.67 %	23,438.00	16,224.93	-7,213.07	-30.78 %	56,250.00
1-4930-00	Tax Apportionments/County Checks	75,000.00	88,211.53	13,211.53	17.62 %	75,000.00	91,778.21	16,778.21	22.37 %	750,000.00
1-4950-00	Miscellaneous Income	0.00	0.00	0.00	0.00 %	1,750.00	96.78	-1,653.22	-94.47 %	7,000.00
1-4955-00	Cell Site Lease Income	14,500.00	17,981.72	3,481.72	24.01 %	72,500.00	78,747.60	6,247.60	8.62 %	179,000.00
1-4965-00	ERAF Refund - County Taxes	0.00	0.00	0.00	0.00 %	175,000.00	232,692.69	57,692.69	32.97 %	375,000.00
	Total RevType: 2 - Non-Operating:	**99,186.00**	**115,495.11**	**16,309.11**	**16.44 %**	**372,678.00**	**456,121.52**	**83,443.52**	**22.39 %**	**1,452,250.00**
	Total Revenue:	**1,153,549.00**	**1,134,728.14**	**-18,820.86**	**-1.63 %**	**6,259,190.00**	**6,598,357.75**	**339,167.75**	**5.42 %**	**13,548,250.00**
Expense										
ExpType: 1 - Operating										
1-5130-00	Water Purchased	268,702.00	243,436.62	25,265.38	9.40 %	1,621,263.00	1,661,061.16	-39,798.16	-2.45 %	2,341,560.00
1-5230-00	Nunes T P Pump Expense	3,417.00	6,037.43	-2,620.43	-76.69 %	17,081.00	22,304.00	-5,223.00	-30.58 %	41,000.00
1-5231-00	CSP Pump Station Pump Expense	25,000.00	78,598.77	-53,598.77	-214.40 %	240,000.00	246,356.60	-6,356.60	-2.65 %	350,000.00
1-5232-00	Other Trans. & Dist Pump Expense	1,750.00	2,675.43	-925.43	-52.88 %	8,750.00	12,034.42	-3,284.42	-37.54 %	21,000.00
1-5233-00	Pilarcitos Canyon Pump Expense	7,500.00	777.05	6,722.95	89.64 %	10,600.00	3,054.82	7,545.18	71.18 %	43,000.00
1-5234-00	Denniston T P Pump Expense	6,800.00	776.67	6,023.33	88.58 %	34,000.00	4,893.45	29,106.55	85.61 %	110,000.00
1-5242-00	CSP Pump Station Operations	1,375.00	502.35	872.65	63.47 %	6,875.00	3,514.46	3,360.54	48.88 %	16,500.00
1-5243-00	CSP Pump Station Maintenance	3,083.00	2,106.48	976.52	31.67 %	15,415.00	12,975.08	2,439.92	15.83 %	37,000.00
1-5246-00	Nunes T P Operations - General	7,500.00	11,083.16	-3,583.16	-47.78 %	37,500.00	44,542.26	-7,042.26	-18.78 %	90,000.00
1-5247-00	Nunes T P Maintenance	10,417.00	16,514.59	-6,097.59	-58.53 %	52,081.00	80,072.21	-27,991.21	-53.75 %	125,000.00
1-5248-00	Denniston T P Operations-General	4,583.00	2,833.35	1,749.65	38.18 %	22,919.00	6,895.05	16,023.95	69.92 %	55,000.00
1-5249-00	Denniston T.P. Maintenance	8,000.00	79.96	7,920.04	99.00 %	76,000.00	70,500.79	5,499.21	7.24 %	132,000.00
1-5250-00	Laboratory Expenses	6,250.00	3,773.05	2,476.95	39.63 %	31,250.00	20,194.88	11,055.12	35.38 %	75,000.00
1-5260-00	Maintenance - General	26,000.00	20,706.26	5,293.74	20.36 %	142,000.00	134,101.70	7,898.30	5.56 %	348,500.00
1-5261-00	Maintenance - Well Fields	1,000.00	1,596.42	-596.42	-59.64 %	14,000.00	1,609.44	12,390.56	88.50 %	30,000.00
1-5263-00	Uniforms	2,500.00	1,118.47	1,381.53	55.26 %	5,000.00	8,321.67	-3,321.67	-66.43 %	10,000.00
1-5318-00	Studies/Surveys/Consulting	10,000.00	2,497.87	7,502.13	75.02 %	50,000.00	32,568.87	17,431.13	34.86 %	150,000.00
1-5321-00	Water Resources	2,167.00	0.00	2,167.00	100.00 %	10,831.00	110.26	10,720.74	98.98 %	26,000.00

		November Budget	November Activity	Variance Favorable (Unfavorable)	Percent Variance	YTD Budget	YTD Activity	Variance Favorable (Unfavorable)	Percent Variance	Total Budget
1-5322-00	Community Outreach	1,000.00	4,300.00	-3,300.00	-330.00 %	19,000.00	16,332.41	2,667.59	14.04 %	58,400.00
1-5381-00	Legal	8,333.00	7,655.00	678.00	8.14 %	41,665.00	43,050.00	-1,385.00	-3.32 %	100,000.00
1-5382-00	Engineering	5,500.00	13,281.60	-7,781.60	-141.48 %	27,500.00	38,501.22	-11,001.22	-40.00 %	66,000.00
1-5383-00	Financial Services	2,000.00	1,000.00	1,000.00	50.00 %	11,000.00	8,775.00	2,225.00	20.23 %	22,000.00
1-5384-00	Computer Services	17,625.00	16,372.08	1,252.92	7.11 %	88,125.00	88,399.35	-274.35	-0.31 %	211,500.00
1-5410-00	Salaries/Wages-Administration	101,942.00	84,337.84	17,604.16	17.27 %	509,710.00	404,922.57	104,787.43	20.56 %	1,223,311.00
1-5411-00	Salaries & Wages - Field	125,117.00	112,149.12	12,967.88	10.36 %	625,585.00	611,814.75	13,770.25	2.20 %	1,501,399.00
1-5420-00	Payroll Tax Expense	15,975.00	12,251.16	3,723.84	23.31 %	79,875.00	67,047.54	12,827.46	16.06 %	191,701.00
1-5435-00	Employee Medical Insurance	41,645.00	38,607.60	3,037.40	7.29 %	208,225.00	192,849.39	15,375.61	7.38 %	511,400.00
1-5436-00	Retiree Medical Insurance	5,661.00	5,316.77	344.23	6.08 %	28,305.00	25,152.65	3,152.35	11.14 %	69,562.00
1-5440-00	Employees Retirement Plan	41,353.00	31,301.93	10,051.07	24.31 %	206,765.00	197,920.10	8,844.90	4.28 %	496,240.00
1-5445-00	Supplemental Retirement 401a	0.00	0.00	0.00	0.00 %	0.00	0.00	0.00	0.00 %	35,000.00
1-5510-00	Motor Vehicle Expense	6,250.00	5,210.90	1,039.10	16.63 %	31,250.00	29,378.70	1,871.30	5.99 %	75,000.00
1-5620-00	Office & Billing Expenses	28,792.00	30,511.84	-1,719.84	-5.97 %	153,956.00	145,723.86	8,232.14	5.35 %	363,500.00
1-5625-00	Meetings / Training / Seminars	2,750.00	1,795.00	955.00	34.73 %	13,750.00	3,706.84	10,043.16	73.04 %	33,000.00
1-5630-00	Insurance	13,250.00	12,290.38	959.62	7.24 %	66,250.00	59,510.86	6,739.14	10.17 %	159,000.00
1-5687-00	Membership, Dues, Subscript.	7,092.00	7,017.50	74.50	1.05 %	35,456.00	47,097.43	-11,641.43	-32.83 %	85,100.00
1-5688-00	Election Expenses	30,000.00	0.00	30,000.00	100.00 %	30,000.00	0.00	30,000.00	100.00 %	30,000.00
1-5689-00	Labor Relations	500.00	0.00	500.00	100.00 %	2,500.00	0.00	2,500.00	100.00 %	6,000.00
1-5700-00	San Mateo County Fees	2,100.00	0.00	2,100.00	100.00 %	10,300.00	5,597.42	4,702.58	45.66 %	25,000.00
1-5705-00	State Fees	3,000.00	1,700.70	1,299.30	43.31 %	15,000.00	1,700.70	13,299.30	88.66 %	36,500.00
	Total ExpType: 1 - Operating:	**855,929.00**	**780,213.35**	**75,715.65**	**8.85 %**	**4,599,782.00**	**4,352,591.91**	**247,190.09**	**5.37 %**	**9,301,173.00**
ExpType: 4 - Capital Related										
1-5715-00	Debt Service/CIEDB 11-099	0.00	0.00	0.00	0.00 %	268,811.00	268,811.40	-0.40	0.00 %	335,825.00
1-5716-00	Debt Service/CIEDB 2016	0.00	0.00	0.00	0.00 %	234,969.00	234,968.81	0.19	0.00 %	323,357.00
1-5717-00	Chase Bank - 2018 Loan	0.00	0.00	0.00	0.00 %	370,586.00	370,586.23	-0.23	0.00 %	433,567.00
	Total ExpType: 4 - Capital Related:	**0.00**	**0.00**	**0.00**	**0.00 %**	**874,366.00**	**874,366.44**	**-0.44**	**0.00 %**	**1,092,749.00**
	Total Expense:	**855,929.00**	**780,213.35**	**75,715.65**	**8.85 %**	**5,474,148.00**	**5,226,958.35**	**247,189.65**	**4.52 %**	**10,393,922.00**
	Report Total:	**297,620.00**	**354,514.79**	**56,894.79**		**785,042.00**	**1,371,399.40**	**586,357.40**		**3,154,328.00**

COASTSIDE COUNTY WATER DISTRICT
MONTHLY INVESTMENT REPORT
November 30, 2020

RESERVE BALANCES	**Current Year as of 11/30/2020**	**Prior Year as of 11/30/2019**
CAPITAL AND OPERATING RESERVE	$8,581,227.00	$8,535,763.40
RATE STABILIZATION RESERVE	$250,000.00	$250,000.00
TOTAL DISTRICT RESERVES	**$8,831,227.00**	**$8,785,763.40**

ACCOUNT DETAIL

ACCOUNTS WITH TRI COUNTIES BANK		
CHECKING ACCOUNT	$3,422,284.31	$3,494,954.07
CSP T & S ACCOUNT	$136,639.97	$104,520.42
MONEY MARKET GEN. FUND (Opened 7/20/17)	$19,448.02	$19,443.48
LOCAL AGENCY INVESTMENT FUND (LAIF) BALANCE	$5,252,054.70	$5,166,045.43
DISTRICT CASH ON HAND	$800.00	$800.00
TOTAL ACCOUNT BALANCES	**$8,831,227.00**	**$8,785,763.40**

This report is in conformity with CCWD's Investment Policy.

COASTSIDE COUNTY WATER DISTRICT
CAPITAL IMPROVEMENT PROJECTS - STATUS REPORT
FISCAL YEAR 2020/2021

11/30/2020

* Approved June 2020

		Status	Approved* CIP Budget FY 20/21	Actual To Date FY 20/21	Projected Year-End FY20/21	Variance vs. Budget	% Completed	Project Status/ Comments
Equipment Purchases & Replacement								
06-03	SCADA/Telemetry/Electrical Controls Replacement	ongoing	$ 50,000		$ 50,000	$ -	0%	
19-04	Valve truck	ion order	$ 225,000		$ 225,000	$ -	0%	Board approved September 2020
22-05	Planning Software	open	$ 60,000		$ 60,000	$ -	0%	
Facilities & Maintenance								
99-01	Meter Change Program	ongoing	$ 20,000		$ 20,000	$ -	0%	
Pipeline Projects								
13-02	Pipeline Replacement Under Creek at Pilarcitos Ave (Strawflower)	In design	$ 750,000	$ 45,551	$ 750,000	$ -	0%	
14-01	Highway 92 - Replacement of Welded Steel Line	Open	$ 100,000	$ 35,735	$ 100,000	$ -	36%	for design only
21-10	El Granada Highlands (below Tank #2) Lot Purchase	Open	$ 500,000	$ 406,966	$ 500,000	$ -	100%	Escrow for lot purchase closed 12.2.2020
Pump Stations / Tanks / Wells								
21-07	District-Wide Tank Improvement Project	Open	$ 600,000	$ 3,075	$ 600,000	$ -	n/a	
21-02	Pilarcitos Reservoir Spillway-Pump/Emergency Generator	On order	$ 100,000		$ 100,000		0%	Board approved September 2020
19-05	Tanks - THM Control	Ongoing	$ 60,000		$ 60,000		0%	
21-11	Tank Cathodic Protection Project	Open	$ 40,000		$ 40,000	$ -	0%	
Water Supply Development								
14-25	Denniston/San Vicente Water Supply Development	ongoing	$ 300,000	$ 122,148	$ 300,000	$ -	41%	
Water Treatment Plants								
20-14	Nunes Water Treatment Plant Improvement Project	In Design	$ 700,000	$ 371,799	$ 700,000	$ -	74%	
21-04	Nunes/Denniston Turbidimeter Replacement	Completed	$ 35,000	$ 32,498	$ 32,498	$ 2,502	100%	Board approved August 2020
UNSCHEDULED/NEW CIP ITEMS FOR CURRENT FISCAL YEAR 2020/2021								
NN-00	Unscheduled CIP		$ 100,000		$ 100,000	$ -	0%	
	NEW FY2020/2021 CIP TOTAL		**$ 3,640,000**	**$ 1,017,773**	**$ 3,637,498**	**$ -**		
FY2019/2020 CIP Carryover Projects								
21-08	Asset Management/GIS software	in process	$ 60,000	32,500	$ 60,000	$ -	50%	
20-07	District Office Improvements	in process	$ 60,000	41,754	$ 60,000	$ -	60%	
18-13	Denniston WTP and Tank Road Repairs and Paving	in process	$ 400,000	$ 431,085	$ 431,085	$ (31,085)	100%	
14-01	Highway 92 - Replacement of Welded Steel Line-Phase 1	open	$ 700,000		$ 700,000	$ -	0%	
20-08	Highway 1 Crossings (Silver/Terrace/Grandview/Spindrift)	pre-design	$ 30,000	12,144	$ 30,000	$ -	15%	
13-05	Denniston WTP and Booster Station Standby Power	in process	$ 300,000	394,857	$ 394,857	$ (94,857)	90%	Partial budget included in FY2019-2020
30-00	Computer Software upgrades	ongoing		8,630	$ 8,630	$ (8,630)		
08-08	PRV Replacment Program	in process		19,077	$ 19,171	$ (19,171)		
20-17	Garcia Avenue Emergency Pipeline Replacement	closed		25,088	$ 25,088	$ (25,088)	100%	

COASTSIDE COUNTY WATER DISTRICT
CAPITAL IMPROVEMENT PROJECTS - STATUS REPORT
FISCAL YEAR 2020/2021

11/30/2020

* Approved June 2020

		Status	Approved* CIP Budget FY 20/21	Actual To Date FY 20/21	Projected Year-End FY20/21	Variance vs. Budget	% Completed	Project Status/ Comments
14-27	Grandview 2 Inch Replacement	in design		4,973	$ 4,973	$ (4,973)	90%	design only near completion
18-01	Pine Willow Oak Pipeline Replacement	in design		4,992	$ 4,992	$ (4,992)	90%	design only near completion
FY2019/2020 CARRYOVER PROJECTS			**$ 1,550,000**	**$ 975,099**	**$ 1,738,796**	**$ (188,796)**		

Green = approved by the Board/in process

TOTAL - FY 2020/2021 CIP + PRIOR YEAR CARRYOVER	**$ 5,190,000**	**$ 1,992,872**	**$ 5,376,294**	**$ (188,796)**	

Legal Cost Tracking Report
12 Months At-A-Glance

Acct. No.5681
Patrick Miyaki - HansonBridgett, LLP
Legal

Month	Admin (General Legal Fees)	Water Supply Develpmnt	Recycled Water	Transfer Program	CIP	LABOR & EMPLOYMENT	Election (CVRA)	Litigation	Infrastructure Project Review (Reimbursable)	TOTAL
Nov-19	3,948						6,905		665	11,518
Dec-19	3,801			365			2,814			6,980
Jan-20	12,289						8,071			20,360
Feb-20	4,256	1,855		245			2,527			8,883
Mar-20	3,990	1,295				1,050	840			7,175
Apr-20	6,353	1,085				665				8,103
May-20	4,011					840				4,851
Jun-20	4,248			70		1,085				5,403
Jul-20	6,940			1,061						8,001
Aug-20	13,125	1,715		270						15,110
Sep-20	10,699			759						11,458
Oct-20	6,655			313	3,351					10,319
TOTAL	**80,314**	**5,950**	**0**	**3,083**	**3,351**	**3,640**	**21,157**	**0**	**665**	**118,160**

Engineer Cost Tracking Report
12 Months At-A-Glance

Acct. No. 5682
JAMES TETER
Engineer

Month	Admin & Retainer	CIP	Studies & Projects	TOTAL	Reimburseable from Projects
Dec-19	480	676		**1,156**	
Jan-20	480	676	254	**1,410**	254
Feb-20	480	4,344	2,197	**7,021**	2,197
Mar-20	480	4,563		**5,043**	
Apr-20	480			**480**	
May-20	480			**480**	
Jun-20	480		1,268	**1,748**	1,268
Jul-20	480		1,183	**1,663**	1,183
Aug-20	480		3,803	**4,283**	3,803
Sep-20	480		169	**649**	169
Oct-20	480		1,494	**1,974**	1,494
Nov-20	480		845	**1,325**	845
TOTAL	**5,760**	**10,259**	**11,212**	**27,230**	**11,212**

Calcon T&M Projects Tracking

11/30/2020

Project No.	Name	Status	Proposal Date	Approved Date	Project Budget	Project Actual thru 6/30/20	Project Billings FY2020-2021
Closed Projects:							
CAL-13-01	EG Tank 2 Recoating Project	Closed	9/30/13	10/8/13	$8,220.00	$ 8,837.50	
CAL-13-02	Nunes Control System Upgrades	Closed	9/30/13	10/8/13	$46,141.00	$ 55,363.60	
CAL-13-03	Win 911 and PLC Software	Closed	9/30/13	10/8/13	$9,717.00	$ 12,231.74	
CAL-13-04	Crystal Springs Surge Tank Retrofit	Closed	11/26/13	11/27/13	$31,912.21	$ 66,572.54	
CAL-13-06	Nunes Legacy Backwash System Removal	Closed	11/25/13	11/26/13	$6,516.75	$ 6,455.00	
CAL-13-07	Denniston Backwash FTW Valves	Closed	11/26/13	11/27/13	$6,914.21	$ 9,518.28	
CAL-14-01	Denniston Wash Water Return Retrofit	Closed	1/28/14	2/14/14	$13,607.00	$ 13,591.60	
CAL-14-02	Denniston Calrifier SCADA Data	Closed	4/2/14	4/7/14	$4,125.00	$ 4,077.50	
CAL-14-03	Nunes Surface Scatter Turbidimeter	Closed	4/2/14	4/7/14	$2,009.50	$ -	
CAL-14-04	Phase I Control System Upgrade	Closed	4/2/14	4/7/14	$75,905.56	$ 44,459.14	
CAL-14-06	Miramar Control Panel	Closed	8/28/14	8/28/14	$37,953.00	$ 27,980.71	
CAL-14-08	SFWater Flow & Data Logger/Cahill Tank	Closed	8/20/2014	8/20/2014	$1,370.00	$ 1,372.00	
CAL-15-01	Main Street Monitors	Closed				$ 6,779.42	
CAL-15-02	Dennistion To Do List	Closed				$ 2,930.00	
CAL-15-03	Nunes & Denniston Turbidity Meters	Closed			$6,612.50	$ 12,536.12	
CAL-15-04	Phase II Control System Upgrade	Closed	6/23/2015	8/11/2015	$195,000.00	$ 202,227.50	
CAL-15-05	Permanganate Water Flow	Closed				$ 1,567.15	
CAL-16-04	Radio Network	Closed	12/9/2016	1/10/2017	$126,246.11	$ 139,200.68	
CAL-16-05	El Granada Tank No. 3 Recoating	Closed	12/16/2016		$6,904.50	$ 6,845.00	
CAL-17-03	Nunes Valve Control	Closed	6/29/2017	7/11/2017	$73,281.80	$ 79,034.35	
CAL-17-04	Denniston Booster Pump Station	Closed	7/27/2017	8/8/2017	$21,643.75	$ 29,760.00	
CAL-17-05	Crystal Springs Pump Station #3 Soft Start	Closed	7/27/2017	8/8/2017	$12,213.53	$ 12,178.13	
CAL-18-04	Tank Levels Calibration Special	Closed	3/5/2018	3/5/2018	$8,388.75	$ 10,700.00	
CAL-18-05	Pilarcitos Stream Flow Gauge -Well 1 120 Service Power	Closed	3/22/2018	3/22/2018	$3,558.13	$ 3,997.40	
CAL-17-06	Nunes Flocculartor & Rapid Mix VFD Panels	Closed	12/6/2017	12/12/2017	$29,250.75	$ 30,695.66	
CAL-17-01	Crystal Springs Leak Valve Control	Closed	2/8/2017	2/14/2017	$8,701.29	$ 18,055.88	
CAL-17-02	Crystal Springs Requirements & Addtl Controls	Closed	2/8/2017	2/14/2017	$38,839.50	$ 41,172.06	
CAL-18-02	Nunes Plant HMI V2	Closed	11/12/2018		$10,913.14	$ 9,434.90	
CAL-18-03	CSP Breakers & Handles		3/7/2018	3/7/2018	$25,471.47	$ 49,837.52	
CAL-18-06	Nunes VFD Project		9/6/2018	9/6/2018	$2,381.51	$ 895.50	
CAL-19-01	CSP Cla-Val Power Checks		2/4/2019	2/4/2019	$15,067.91	$ 40,475.94	
CAL-19-02	CSP Wet Well		4/1/2019	4/1/2019	$12,960.24	$ 12,853.20	
CAL-19-03	Pilarcitos Flow Meter Project		4/1/2019	4/1/2019	$14,493.75	$ 17,616.84	
	CSP Main Breaker						
CAL-19-04	SCADA Systems		10/15/2019	10/15/2019	$104,000.00	$ 114,250.00	
	Spare 350/500 Pumps					$ 3,327.09	
	CSP Main Breaker					$ 5,220.00	
		Closed Projects - Subtotal (pre FY2019-2021)			$960,319.86	$1,102,049.95	
FY 2020-2021 Open Projects:							
		Open Projects - Subtotal			$0.00	$0.00	$0.00
Other: Maintenance							
	Tanks						
	Crystal Springs Maintenance						$ 1,312.19
	Nunes Maintenance						$ 21,633.96
	Denniston Maintenance						$ 8,830.26
	Distribution System						$ 32,874.93
	Wells						
		Subtotal Maintenance					$ 64,651.34
		TOTAL FY 2020/21					$ 64,651.34

EKI Environment & Water
Engineering Services Billed Through November 30, 2020

		Contract Date	Not to Exceed Budget	Status	FY 2018-2019	FY 2019-2020	FY2020-2021
CIP Project Management							
Fiscal Year 2018-2019		10.19.2018	$ 25,000.00	Complete			
Fiscal Year 2018-2019		1.14.2019	$ 40,000.00	Complete			
Fiscal Year 2018-2019		3.12.2019	$ 75,000.00	Complete			
Fiscal Year 2019-2020		7.29.2019	$ 180,000.00	Open	$ 123,410.00	$ 104,108.97	$ 1,138.80
Pipeline Projects (Ferdinand) - T2			$ 2,000.00		$ 18,220.42	$ 13,476.55	
Tank Seismic Projects - T3					$ 16,676.92	$ 19,249.53	
Hydraulic Modeling - T4					$ (4,385.04)	$ 20,570.20	
Fiscal Year 2020-2021		8.13.2020	$ 100,000.00				$ 31,269.42
Sub Total - CIP Project Management Services			$ 422,000.00		$ 163,452.66	$ 157,405.25	$ 32,408.22
Highway 1 South Pipeline Replacement Project	**16-02**	9.20.2018	$ 25,000.00	Complete	$ 17,680.45		
Ferdinand Avenue Pipeline Replacement Design	**14-31**	2.12.2019	$ 29,000.00	Complete	$ 27,824.37	$ 1,169.10	
Casa Del Mar Main Replacement (Phase 1) and Grand Boulevard Pipeline/PRV Loop Design	**14-32**	2.12.2019	$ 28,500.00	Complete	$ 27,297.34	$ 1,195.22	
Denniston Culvert Replacement and Paving Project Design	**18-13**	7.1.2019	$ 16,400.00	Open	$ 804.96	$ 21,296.34	
Denniston Culvert Replacement-Engineering Services during Construction	**18-13**	7.8.2020	$ 48,800.00	Open			$ 47,647.17
Construction Inspection Services for Ferdinand Avenue Water Main Replacement Project	**14-31**	7.1.2019	$ 32,300.00	Complete		$ 32,300.00	
Pine Willow Oak Water Main Replacement Project	**18-01**	7.29.2019	$ 69,700.00	Open		$ 49,906.63	$ 4,991.74
Grandview Water Main Replacement Project (Design, Bid Support, construction support)	**14-27**	7.29.2019	$ 56,100.00	Open		$ 42,095.19	$ 4,972.76
Pilarcitos Creek Crossing Water Main Replacement Preliminary Design	**13-02**	8.27.2019	$ 104,600.00	Open		$ 95,332.59	
Pilarcitos Creek Crossing Water Main Replacement Design	**13-02**	7.14.2020	$ 82,900.00	Open			$ 21,895.64
Grandview/Silver/Terrace/Spindrift Under Hwy 1 PreDesign	**20-08**	10.15.2019	$ 45,600.00	Open		$ 18,217.30	$ 868.92
Total - All Services			**$ 960,900.00**		**$ 237,059.78**	**$ 418,917.62**	**$ 112,784.45**

COASTSIDE COUNTY WATER DISTRICT

766 MAIN STREET

HALF MOON BAY, CA 94019

MINUTES OF THE REGULAR MEETING OF THE BOARD OF DIRECTORS

November 10, 2020

On March 17, 2020, the Governor issued Executive Order N-29-20 suspending certain provisions of the Ralph M. Brown Act in order to allow for local legislative bodies to conduct their meetings telephonically or by other electronic means. Pursuant to the Shelter-in-Place Order issued by the San Mateo County Health Officer on March 16, 2020, as revised on March 31, 2020, the statewide Shelter-in-Place Order issued by the Governor in Executive Order N-33-20 on March 19, 2020, and the CDC's social distancing guidelines which discourage large public gatherings, the Boardroom was not open for the November 10, 2020 Regular Meeting of the Coastside County Water District. The Regular Meeting was conducted remotely via teleconference.

The Public was able to watch and/or participate in the public meeting by joining the meeting through the Zoom Video Conference link provided. The public was also able to join the meeting by calling a provided teleconference phone number.

1) ROLL CALL – President Chris Mickelsen called the meeting to order at 7:00 p.m. participating in roll call via Zoom Video Conference: Directors Jim Larimer, Ken Coverdell, Bob Feldman, and Vice-President Glenn Reynolds.

Also participating: Mary Rogren, General Manager, Patrick Miyaki, Legal Counsel; James Derbin, Superintendent of Operations; Cathleen Brennan, Water Resource Analyst; Gina Brazil, Office Manager, Denise Ford, Administrative Assistant/Recording Secretary, and Nancy Trujillo, Accounting Manager.

Dave Irvine, Irvine Consulting, was identified as a participant in the meeting.

Members of the public: John Muller.

2) **PLEDGE OF ALLEGIANCE**

3) PUBLIC COMMENT – There were no public comments.

4) CONSENT CALENDAR

A. Approval of disbursements for the month ending October 31, 2020: Claims: $1,313,010.45; Payroll: $260,999.89 for a total of $1,574,010.34
B. Acceptance of Financial Reports
C. Approval of Minutes of October 13, 2020 Regular Board of Directors Meeting
D. Installed Water Connection Capacity and Water Meters Report
E. Total CCWD Production Report
F. CCWD Monthly Sales by Category Report-October 2020
G. Monthly Planned Plant or Tank Discharge and New Water Line Flushing Report
H. Monthly Rainfall Reports
I. SFPUC Hydrological Report for the Month of September 2020
J. Notice of Completion for Denniston Reservoir Maintenance Dredging Project for Year 2020
K. Notice of Completion for Denniston Culvert Replacement and Paving Project
L. Water Service Connection Transfer Report – October 2020

President Mickelsen reported that he had reviewed the monthly financial claims and found all to be in order.

ON MOTION BY Director Coverdell and seconded by Vice-President Reynolds, the Board voted by roll call vote to approve the Consent Calendar:

Director Larimer	**Aye**
Vice-President Reynolds	**Aye**
Director Coverdell	**Aye**
Director Feldman	**Aye**
President Mickelsen	**Aye**

5) MEETINGS ATTENDED/DIRECTOR COMMENTS

Vice-President Reynolds reported that he attended a meeting of a CA-NV AWWA advisory committee that is providing guidance to the State Water Resources Control Board on its revisions to the State Cross Connection and Backflow program.

6) GENERAL BUSINESS

A. <u>Resolution 2020-05 – A Resolution of the Board of Directors of the Coastside County Water District Expressing Appreciation to Jim Larimer for his Leadership and Dedicated Service</u>

Ms. Rogren expressed her appreciation and acknowledged Director Larimer for his numerous contributions to the District. Director Larimer originally served as a Director from November 2001 to November 2011 and then in March 2019, was once again appointed to service on the Board of Directors to fulfill the remainder of the term created by the resignation of Arnie Glassberg. Each of the Directors made a brief statement acknowledging the special attributes Director Larimer contributed to the District during his term.

ON MOTION BY Director Coverdell and seconded by Vice-President Reynolds, the Board voted by roll call vote to Approve Resolution 2020-05 expressing appreciation to Director Jim Larimer for his leadership and dedicated service.

Director Larimer	**Aye**
Vice-President Reynolds	**Aye**
Director Coverdell	**Aye**
Director Feldman	**Aye**
President Mickelsen	**Aye**

B. <u>Resolution 2020-06 – Resolution for Acceptance of Treasury Management Services with Tri Counties Bank and Related Actions</u>

The District originally contracted with First National Bank in November 2003 and then in July 2017, First National Bank was purchased by Tri Counties Bank. Tri Counties Bank requested that the District accept the Tri-Counties Bank Treasury Management Services Agreement and related actions in order to update the bank paperwork.

ON MOTION BY Vice-President Reynolds and seconded by Director Feldman, the Board voted by roll call vote to approve Resolution 2020-06 for accepting Treasury Management Services with Tri Counties Bank and related actions.

Director Larimer	**Aye**
Vice-President Reynolds	**Aye**
Director Coverdell	**Aye**
Director Feldman	**Aye**
President Mickelsen	**Aye**

7) **MONTHLY INFORMATION REPORTS**

A. <u>General Manager's Report</u>

Mr. Rogren proudly announced the District had been selected as a top ACWA 2020 Outreach winner for ACWA region 5. The District staff sent numerous letters to legislators on issues supported by ACWA and that impact the water community.

The District will be acknowledged with other regional winners at the ACWA 2020 Fall Virtual Conference in December.

B. <u>Superintendent of Operations Report</u>

Mr. Derbin reviewed the operations highlights for the month of October 2020.

8) CLOSED SESSION

Pursuant to California Government Code Section 54957
Threat to Public Services or Facilities
Consultation with District Counsel

Upon returning to open session it was reported that no action was taken in the closed session.

9) DIRECTOR AGENDA ITEMS-REQUESTS FOR FUTURE BOARD MEETINGS

10) ADJOURNMENT-The Board Meeting was adjourned at 8:21 p.m.

Respectfully submitted,

_____
Mary Rogren, General Manager
Secretary to the District

_____
Chris Mickelsen, President
Board of Directors

COASTSIDE COUNTY WATER DISTRICT

Installed Water Connection Capacity & Water Meters

FY 2021 Meters

Installed Water Meters	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Total
HMB Non-Priority													
0.5" capacity increase													
5/8" meter	1				1								**2**
3/4" meter													
1" meter													
1 1/2" meter													
2" meter													
3" meter													
HMB Priority													
0.5" capacity increase													
5/8" meter													
3/4" meter													
1" meter													
1 1/2" meter													
2" meter													
County Non-Priority													
0.5" capacity increase													
5/8" meter	1	2											**3**
3/4" meter													
1" meter													
County Priority													
5/8" meter													
3/4" meter													
1" meter													
1.5" meter													
Totals	2	2	0	0	1								**5**

5/8" meter = 1 connection
3/4" meter = 1.5 connections
1" meter = 2.5 connections
1.5" meter = 5 connections
2" meter = 8 connections
3" meter= 17.5 connections

FY 2020 Capacity (5/8" connection equivalents)	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Totals
HMB Non-Priority	1				1								**2**
HMB Priority													
County Non-Priority	1	2											**3**
County Priority													
Total	2	2	0	0	1								**5**

TOTAL CCWD PRODUCTION (MG) ALL SOURCES- FY 2021

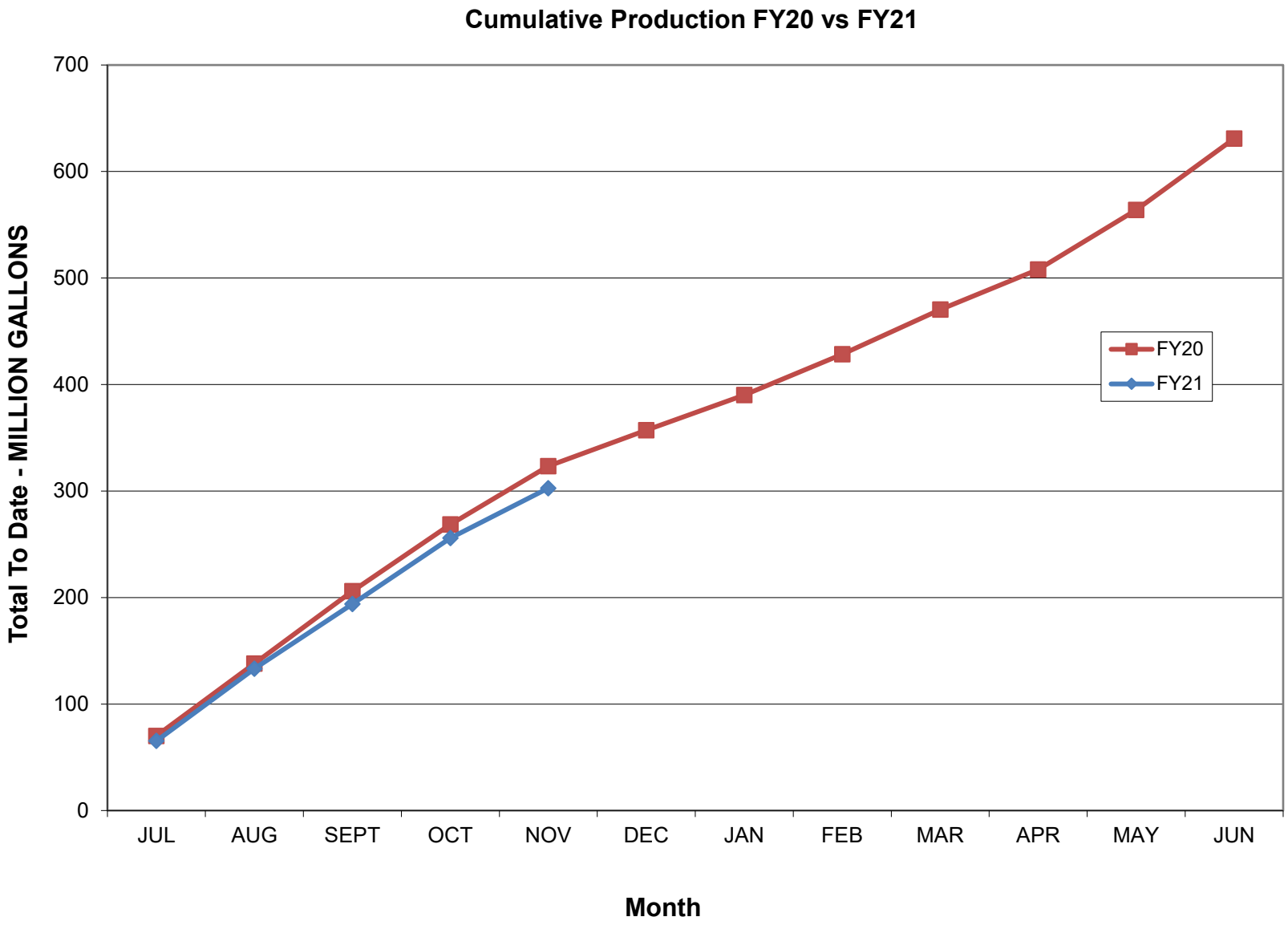
	CCWD Sources			SFPUC Sources				
	DENNISTON WELLS	DENNISTON RESERVOIR	PILARCITOS WELLS	PILARCITOS LAKE	CRYSTAL SPRINGS RESERVOIR	RAW WATER TOTAL	UNMETERED WATER	TREATED TOTAL
JUL	0.02	2.83	0.00	28.80	36.06	67.71	2.35	65.36
AUG	0.00	0.00	0.00	49.75	20.27	70.02	2.25	67.78
SEPT	0.00	0.00	0.00	1.31	60.84	62.15	1.31	60.84
OCT	0.00	0.00	0.00	0.00	63.97	63.97	2.11	61.86
NOV	0.00	0.00	3.91	14.39	29.52	47.82	0.93	46.90
DEC								
JAN								
FEB								
MAR								
APR								
MAY								
JUN								
TOTAL	0.02	2.83	3.91	94.25	210.66	311.67	8.94	302.73
% MONTHLY TOTAL	0.0%	0.0%	8.2%	30.1%	61.7%	100.0%	1.9%	98.1%
% ANNUAL TO DATE TOTAL	0.0%	0.9%	1.3%	30.2%	67.6%	100.0%	2.9%	97.1%

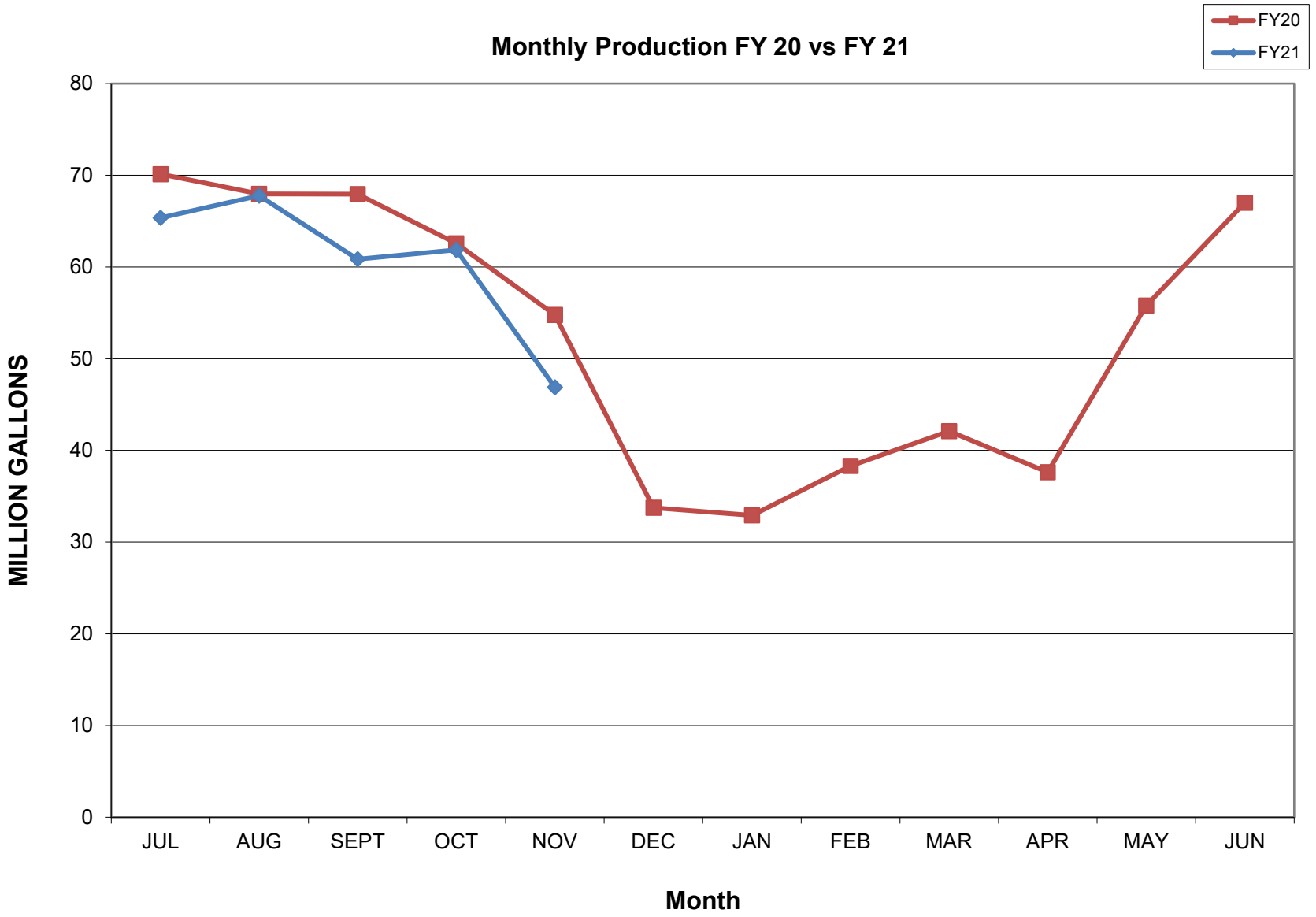
CCWD vs SFPUC- month	8.2%
CCWD vs SFPUC- annual	2.2%

12 Month Running Treated Total **625.95**

TOTAL CCWD PRODUCTION (MG) ALL SOURCES- FY 2020

	CCWD Sources			SFPUC Sources				
	DENNISTON WELLS	DENNISTON RESERVOIR	PILARCITOS WELLS	PILARCITOS LAKE	CRYSTAL SPRINGS RESERVOIR	RAW WATER TOTAL	UNMETERED WATER	TREATED TOTAL
JUL	1.61	28.25	0.00	22.27	20.58	72.71	2.58	70.13
AUG	1.44	22.18	0.00	20.20	26.36	70.18	2.21	67.97
SEPT	1.43	19.67	0.00	19.19	30.98	71.27	3.32	67.95
OCT	0.27	5.45	0.00	9.91	48.70	64.33	1.74	62.59
NOV	0.17	19.16	8.61	0.00	29.39	57.33	2.56	54.77
DEC	0.02	18.87	13.91	0.00	4.10	36.90	3.16	33.74
JAN	0.00	18.92	14.65	0.00	1.79	35.36	2.45	32.92
FEB	1.69	27.02	12.07	1.73	0.23	42.74	4.44	38.30
MAR	0.89	18.88	13.07	3.63	8.30	44.77	2.66	42.11
APR	0.07	16.42	0.00	14.09	10.06	40.64	3.01	37.63
MAY	0.24	18.20	0.00	0.00	41.16	59.60	3.82	55.79
JUN	1.35	10.60	0.00	0.00	58.81	70.76	3.74	67.02
TOTAL	9.18	223.62	62.31	91.02	280.46	666.59	35.68	630.92
% TOTAL	1.4%	33.5%	9.3%	13.7%	42.1%	100.0%	5.35%	0.0%


Cumulative Production FY20 vs FY21
Total To Date - MILLION GALLONS
700
600
500
400
300
200
100
0
JUL
AUG
SEPT
OCT
NOV
DEC
JAN
FEB
MAR
APR
MAY
JUN
Month
FY20
FY21


Monthly Production FY 20 vs FY 21
FY20
FY21
MILLION GALLONS
80
70
60
50
40
30
20
10
0
JUL
AUG
SEPT
OCT
NOV
DEC
JAN
FEB
MAR
APR
MAY
JUN
Month

Coastside County Water District Monthly Sales By Category (MG)
FY2021

	JUL	AUG	SEPT	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	MG to Date
RESIDENTIAL	34.24	32.73	32.19	32.12	28.27								**159.55**
COMMERCIAL	2.86	2.67	2.64	3.03	2.58								**13.78**
RESTAURANT	1.01	1.06	1.01	1.19	1.06								**5.33**
HOTELS/MOTELS	2.19	2.04	2.02	2.13	1.71								**10.10**
SCHOOLS	0.76	0.68	0.61	0.67	0.46								**3.18**
MULTI DWELL	3.14	3.01	2.83	2.98	2.70								**14.67**
BEACHES/PARKS	0.76	0.85	0.60	0.52	0.57								**3.29**
AGRICULTURE	5.31	4.65	4.73	5.92	4.42								**25.04**
RECREATIONAL	0.24	0.24	0.23	0.23	0.20								**1.15**
MARINE	0.64	0.59	0.53	0.56	0.46								**2.79**
RES. IRRIGATION	1.70	1.66	1.56	1.51	1.10								**7.53**
DETECTOR CHECKS	0.01	0.00	0.01	0.01	0.00								**0.03**
NON-RES. IRRIGATION	6.73	5.04	2.23	2.31	1.26								**17.57**
RAW WATER	7.92	6.89	7.00	8.07	6.82								**36.69**
PORTABLE METERS	0.53	0.26	0.33	0.30	0.26								**1.68**
CONSTRUCTION	0.38	0.38	0.31	0.39	0.30								**1.76**
TOTAL - MG	**68.43**	**62.77**	**58.83**	**61.93**	**52.17**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**304.13**
Non Residential Usage	34.19	30.04	26.64	29.81	23.90	0.00	0.00	0.00	0.00	0.00	0.00	0.00	
Running 12 Month Total					**609.09**								
12 mo Residential					335.17								
12 mo Non Residential					273.92								

FY2020

	JUL	AUG	SEPT	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	MG to Date
RESIDENTIAL	21.97	44.43	30.29	31.11	27.59	22.40	22.20	20.32	23.93	25.08	28.62	33.08	**331.01**
COMMERCIAL	3.67	3.29	3.33	3.34	3.07	2.97	2.79	2.70	2.81	2.13	2.27	2.46	**34.83**
RESTAURANT	1.82	1.71	1.57	1.67	1.38	1.23	1.43	1.25	1.18	0.48	0.57	0.80	**15.10**
HOTELS/MOTELS	2.74	2.62	2.70	2.79	2.26	1.93	1.95	1.86	1.78	0.47	0.78	1.43	**23.30**
SCHOOLS	0.62	0.60	0.77	0.94	0.60	0.33	0.16	0.30	0.51	0.31	0.23	0.52	**5.88**
MULTI DWELL	2.74	3.02	2.79	2.89	2.53	2.36	2.51	2.37	2.51	2.65	2.74	2.84	**31.95**
BEACHES/PARKS	0.65	0.90	0.81	0.70	0.60	0.24	0.22	0.20	0.30	0.08	0.09	0.32	**5.11**
AGRICULTURE	6.57	6.34	7.37	9.90	7.57	3.86	3.25	4.35	5.84	4.50	6.84	5.90	**72.30**
RECREATIONAL	0.33	0.26	0.25	0.20	0.21	0.18	0.18	0.17	0.18	0.18	0.19	0.23	**2.55**
MARINE	0.66	0.65	0.65	0.52	0.53	0.43	0.57	0.47	0.43	0.32	0.42	0.54	**6.18**
RES. IRRIGATION	1.41	1.93	1.82	1.54	1.43	0.60	0.40	0.41	1.12	0.63	1.31	1.62	**14.23**
DETECTOR CHECKS	0.01	0.01	0.01	0.02	0.03	0.01	0.07	0.00	0.01	0.01	0.01	0.00	**0.18**
NON-RES. IRRIGATION	4.19	4.97	2.46	2.13	2.17	0.10	0.01	0.09	0.14	0.09	0.28	5.66	**22.27**
RAW WATER	7.06	8.62	9.08	8.09	6.01	1.53	0.00	0.00	1.99	2.09	5.62	7.28	**57.36**
PORTABLE METERS	0.26	0.40	0.30	0.26	0.34	0.11	0.02	0.07	0.14	0.05	0.26	0.03	**2.22**
CONSTRUCTION	0.07	0.11	0.14	0.13	0.12	0.08	0.09	0.24	0.26	0.22	0.28	0.36	**2.10**
TOTAL - MG	**54.76**	**79.86**	**64.35**	**66.22**	**56.42**	**38.35**	**35.84**	**34.79**	**43.12**	**39.29**	**50.49**	**63.09**	**626.57**

MONTH **Nov-20**

Coastside County Water District Monthly Discharge Report

EMERGENCY MAIN AND SERVICE REPAIRS

	Date Reported Discovered	Date Repaired	Location	Pipe Class	Pipe Size & Type	Estimated Water Loss (MG)
1	**11/26/2020**	**11/26/20**	**411 Wave Ave**	**Main**	**6" CI**	**0.012**
2						
3						
4						
5						
6						
7						
8						
					Totals	**0.012**

OTHER DISCHARGES

Total Volumes (MG)	
Flushing Program	0.034
Reservoir Cleaning	
Automatic Blowoffs	0.196
Dewatering Operations	
Other (includes flow testing)	0.002

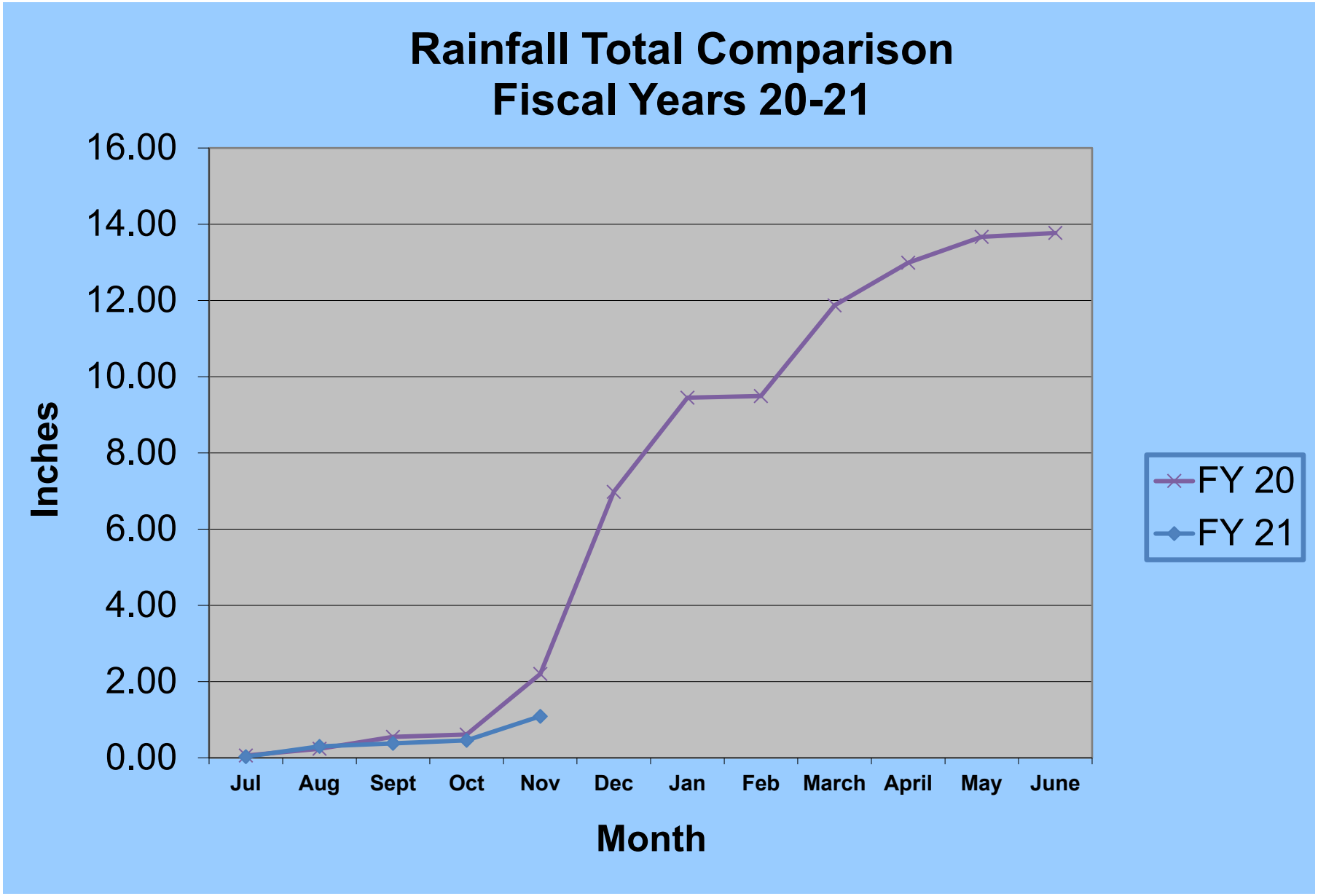
PLANNED DISCHARGES GRAND TOTAL (MG)

0.232

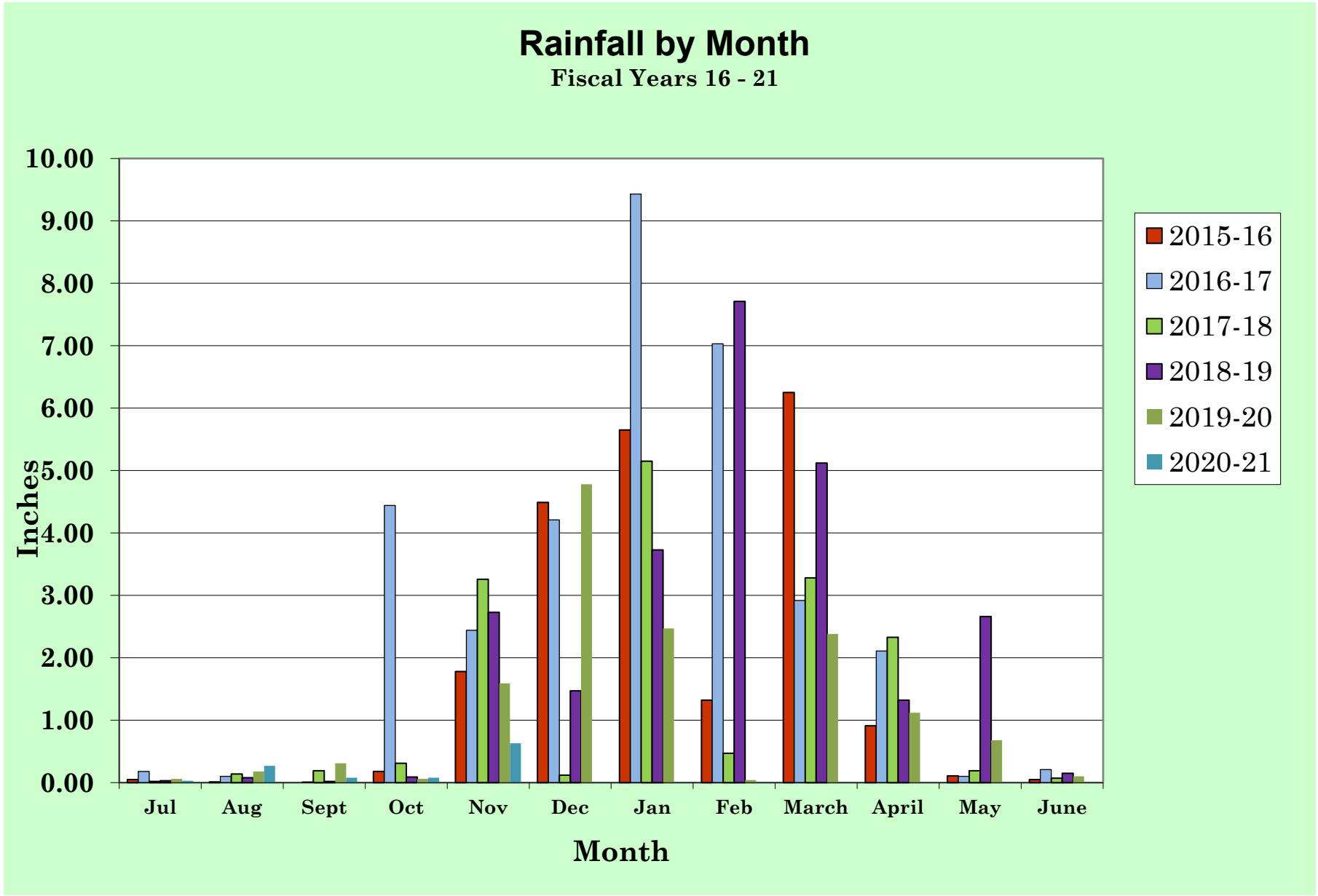
Coastside County Water District
766 Main Street
July 2020 - June 2021

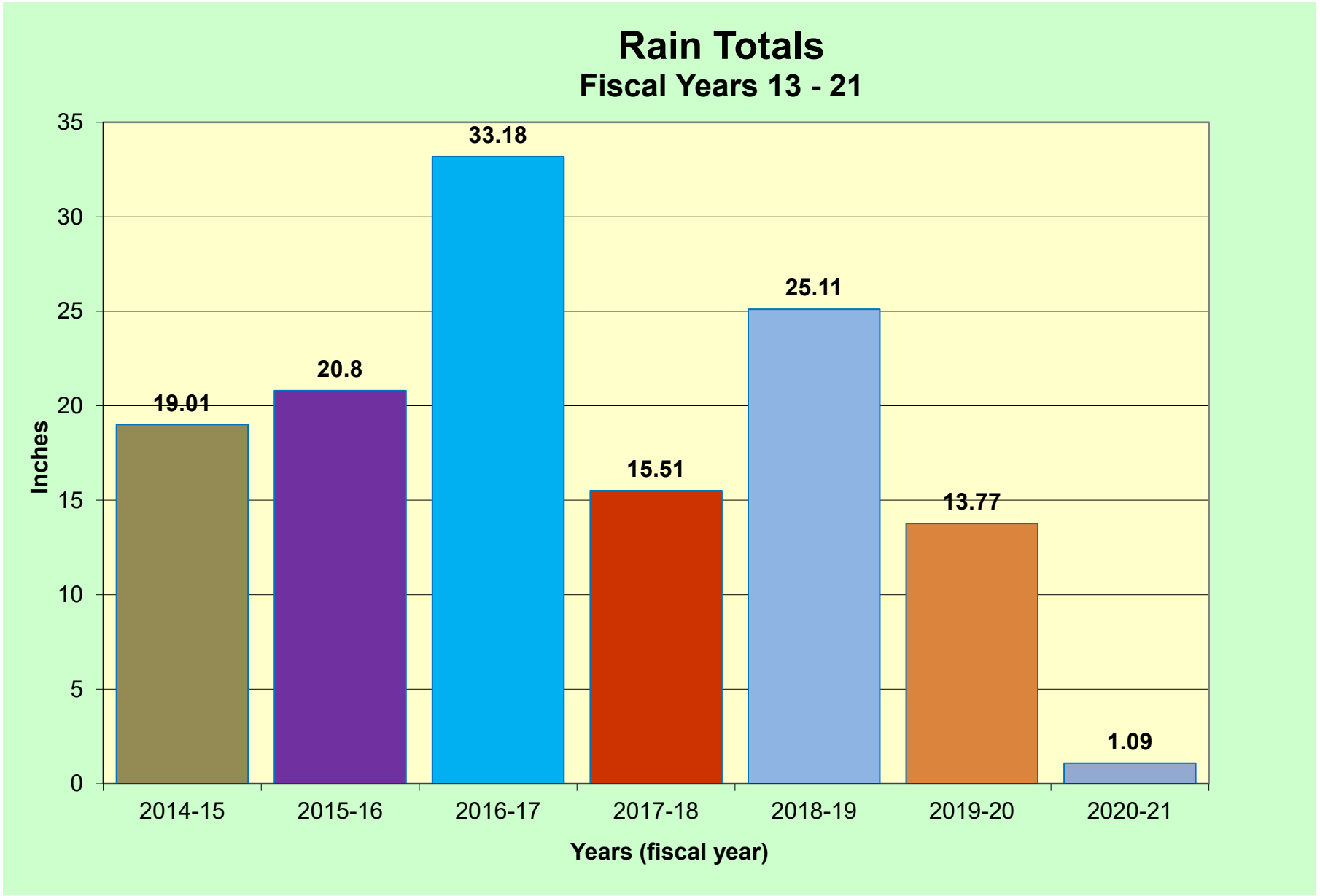
Nunes
Rainfall in Inches

	2020					2021						
	Jul	Aug	Sept	Oct	Nov	Dec	Jan	Feb	March	April	May	June
1	0	0.01	0	0	0							
2	0	0	0	0	0							
3	0	0.03	0	0	0							
4	0	0.03	0	0	0							
5	0	0.02	0	0.01	0							
6	0	0	0	0.02	0.04							
7	0	0	0	0	0							
8	0	0	0	0.01	0							
9	0	0	0.01	0.01	0							
10	0	0	0	0.01	0							
11	0	0	0.01	0.01	0							
12	0	0	0.02	0	0							
13	0	0	0.01	0	0.07							
14	0	0	0	0	0.01							
15	0	0	0	0	0							
16	0	0.08	0	0	0							
17	0	0	0.01	0	0.36							
18	0	0	0	0	0.1							
19	0	0	0	0	0.01							
20	0.01	0	0	0	0							
21	0	0.02	0	0	0							
22	0	0.01	0	0	0.03							
23	0.02	0	0.01	0	0.01							
24	0	0	0.01	0	0							
25	0	0.02	0	0	0							
26	0	0.01	0	0.01	0							
27	0	0.02	0	0	0							
28	0	0	0	0	0							
29	0	0.02	0	0	0							
30	0	0	0	0	0							
31	0	0		0								
Mon.Total	0.03	0.27	0.08	0.08	0.63							
Year Total	0.03	0.30	0.38	0.46	1.09							


Rainfall Total Comparison
Fiscal Years 20-21
16.00
14.00
12.00
10.00
8.00
6.00
4.00
2.00
0.00
Inches
Jul
Aug
Sept
Oct
Nov
Dec
Jan
Feb
March
April
May
June
Month
FY 20
FY 21

Coastside County Water District




Rain Totals
Fiscal Years 13 - 21
Inches
35
30
25
20
15
10
5
0
19.01
20.8
33.18
15.51
25.11
13.77
1.09
2014-15
2015-16
2016-17
2017-18
2018-19
2019-20
2020-21
Years (fiscal year)

San Francisco Public Utilities Commission
Hydrological Conditions Report
October 2020

J. Chester, C. Graham, N. Waelty, November 9, 2020

Hetch Hetchy Water and Power Staff remove debris from the Moccasin Creek Diversion Pipe in preparation for winter flows. This pipe diverts water from Moccasin Creek underneath Moccasin Reservoir, ensuring that unapproved local water does not mix with delivered water from Hetch Hetchy Reservoir. These metal sheets used to armor the invert of the pipe were damaged in the March 2018 storm and decreased the flow capacity.

System Storage

Current Tuolumne System and Local Bay Area storage conditions are summarized in Table 1.

Table 1
Current System Storage
as of November 1, 2020

	Current Storage		Maximum Storage		Available Capacity		Percentage of Maximum Storage
	acre-feet	millions of gallons	acre-feet	millions of gallons	acre-feet	millions of gallons	
Tuolumne System							
Hetch Hetchy Reservoir[1]	254,872		340,830		85,958		75%
Cherry Reservoir[2]	203,700		268,810		65,110		76%
Lake Eleanor[3]	10,456		21,495		11,039		49%
Water Bank	526,883		570,000		43,117		92%
Tuolumne Storage	995,911		1,201,135		205,224		83%
Local Bay Area Storage							
Calaveras Reservoir	57,929	18,876	96,824	31,550	38,895	12,674	60%
San Antonio Reservoir	44,903	14,632	50,496	16,454	5,592	1,822	89%
Crystal Springs Reservoir	51,325	16,724	58,377	19,022	7,052	2,298	88%
San Andreas Reservoir	15,494	5,049	18,996	6,190	3,503	1,141	82%
Pilarcitos Reservoir	1,866	608	2,995	976	1,128	368	62%
Total Local Storage	171,517	55,889	227,688	74,192	56,171	18,303	75%
Total System	1,167,428		1,428,823		261,395		82%

[1] Maximum Hetch Hetchy Reservoir storage with drum gates deactivated.
[2] Maximum Cherry Reservoir storage with flash-boards out.
[3] Maximum Lake Eleanor storage with flash-boards out.

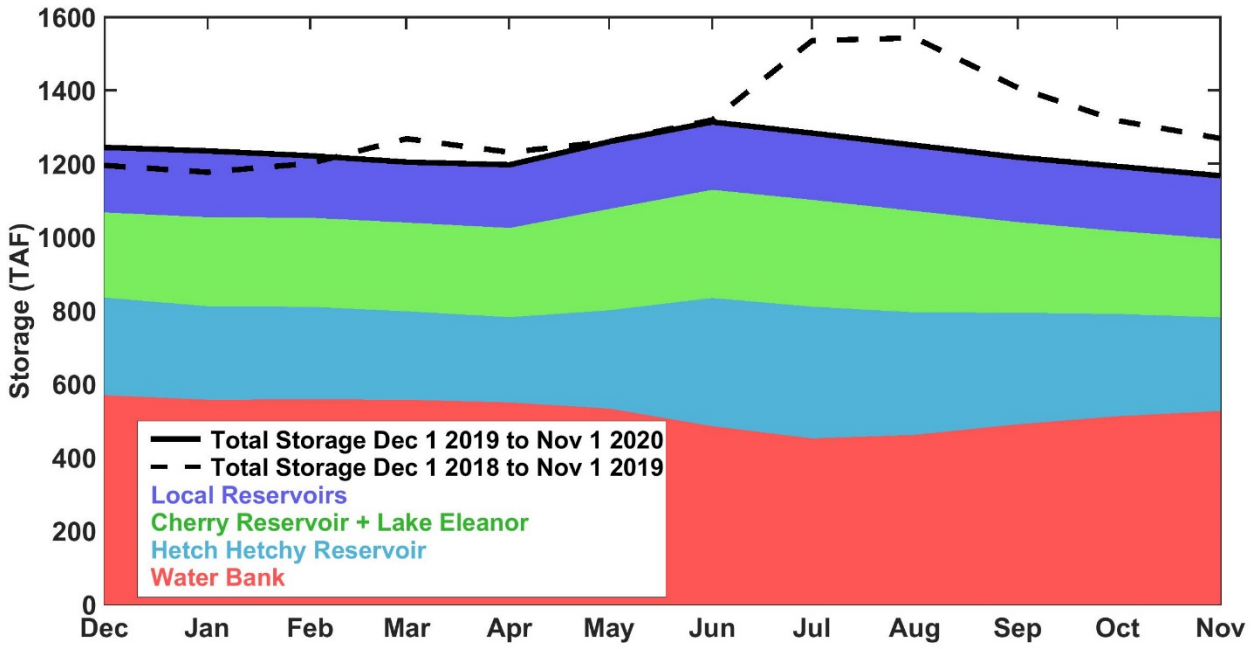


Figure 1: System storage for past 12 months in thousand acre-feet (TAF). Color bands show contributions to total system storage. Solid black line shows total system storage for the past 12 months. Dashed black line shows total system storage the previous 12 months.

Hetch Hetchy System Precipitation Index

Current Month: The October 2020 six-station precipitation index reported zero inches of precipitation for the month. The precipitation index is computed as the average of six Sierra precipitation stations and is an indicator of the overall basin wetness.

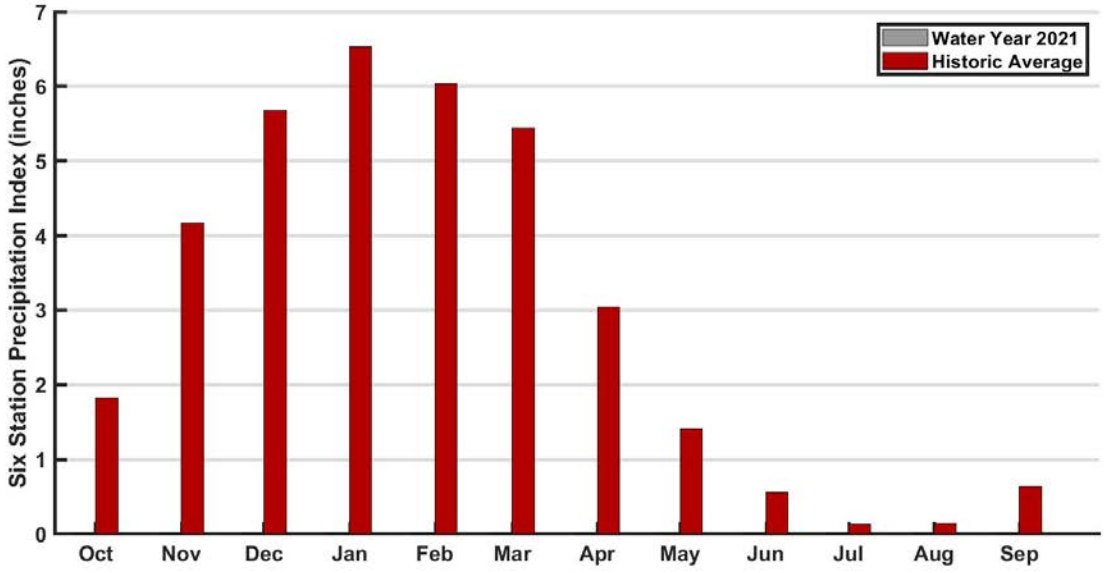


Figure 2: Monthly distribution of the six-station precipitation index relative to the monthly precipitation averages. The precipitation index is computed as the average of six Sierra precipitation stations and is an indicator of the overall basin wetness.

Cumulative Precipitation to Date: As of November 1, the six-station precipitation index for water year (WY) 2021 was zero inches, which is 0% of the average annual water year total. Hetch Hetchy received zero inches of precipitation in October for a total of zero inches for WY 2021, or 0% of average to-date. The cumulative Hetch Hetchy precipitation is shown in Figure 3 in red.

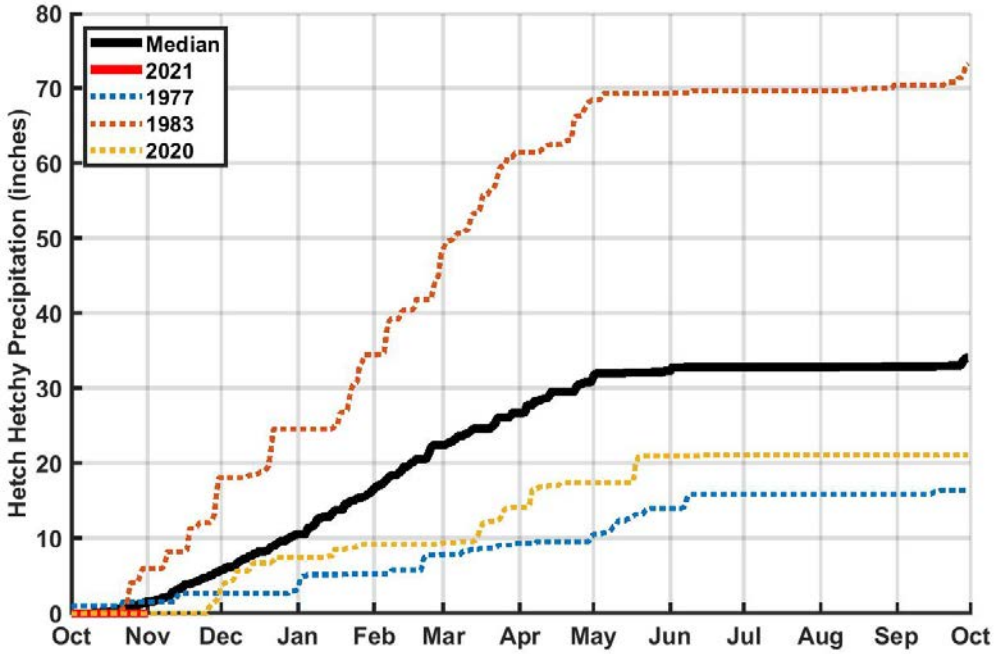


Figure 3: Water Year 2021 cumulative precipitation measured at Hetch Hetchy Weather Station. Median cumulative precipitation measured at Hetch Hetchy Weather Station and example wet and dry years are included with Water Year 2021 for comparison purposes.

Tuolumne Basin Unimpaired Inflow

Unimpaired inflow to SFPUC reservoirs and the Tuolumne River at La Grange for October 2020 and the year to date is summarized below in Table 2.

Table 2
Calculated Reservoir Inflows and Water Available to City

* All flows are in acre-feet	October 2020				October 1, 2020 through November 1, 2020			
	Observed Flow	Median[1]	Mean[1]	Percent of Mean	Observed Flow	Median[1]	Mean[1]	Percent of Mean
Inflow to Hetch Hetchy Reservoir	0	3,161	6,207	0%	0	3,161	6,207	0%
Inflow to Cherry Reservoir and Lake Eleanor	0	2,329	5,485	0%	0	2,329	5,537	0%
Tuolumne River at La Grange	6,182	10,099	17,672	35%	6,182	10,099	17,672	35%
Water Available to City	0	0	2,552	0%	0	0	2,552	0%

[1]Hydrologic Record: 1919-2015

Hetch Hetchy System Operations

Hetch Hetchy Reservoir power draft and stream releases during the month totaled 23,611 acre-feet. Hetch Hetchy Reservoir minimum instream release requirements for October were 35 cfs. Total precipitation and inflows for Calendar Year 2020 have resulted in a Water Year Type C (dry) for Hetch Hetchy Reservoir. Instream release requirements will remain at 35 cfs for the remainder of the calendar year.

Cherry Reservoir valve and power draft releases totaled 11,014 acre-feet for the month and were used to maintain seasonal target elevations. The required minimum instream release from Cherry Reservoir for October was 5 cfs and will remain at that flow through June 2021. Lake Eleanor required minimum instream release were 10 cfs for October. Lake Eleanor minimum stream releases decreased to 5 cfs on November 1. A total of 8,868 acre-feet of water was diverted from Lake Eleanor to Cherry Reservoir in October via the Cherry-Eleanor pump station.

Regional System Treatment Plant Production

The Harry Tracy Water Treatment Plant average production rate for October was 25 MGD. The Sunol Valley Water Treatment Plant average production for the month was 11 MGD.

Local System Water Delivery

The average October delivery rate was 214 MGD, which is a 5% decrease below the September delivery rate of 226 MGD.

Local Precipitation

The rainfall summary for October 2020 is presented in Table 3.

Table 3
Precipitation Totals at Three Local Area Reservoirs

Weather Station Location	October		October 1, 2020 through November 1, 2020	
	Total (inches)	Percent of Mean for the Month	Total (inches)	Percent of Mean for the Year-To-Date
Pilarcitos Reservoir	0.07	4 %	0.07	4%
Lower Crystal Springs Reservoir	0.00	0 %	0.00	0%
Calaveras Reservoir	0.00	0 %	0.00	0%

Water Supply and Planned Water Supply Management

The upcountry system as of November 1 is 83% full, as reservoirs have been managed through the summer and into the fall to maximize storage. SJPL1 is out of service for repairs through February 2021. SJPL deliveries remained at 200 MGD in October. Hetch Hetchy Reservoir storage is expected to continue to decrease as deliveries and stream releases exceed inflows. Cherry / Eleanor Pumps are currently off. Cherry Reservoir is slowly drafting as instream minimum releases and Holm Powerhouse powerdraft exceed inflows. The calculated unimpaired flow at La Grange and the allocation of flows between the Districts and the City are shown in Figure 4. As of November 1, there has been a total of 0 acre-feet available to the City in Water Year 2021.

Short and medium term forecasts remain dry for the upcountry region. As dry conditions persist, reservoir inflows remain very low. Continued reductions in upcountry storage are expected as deliveries exceed inflows.

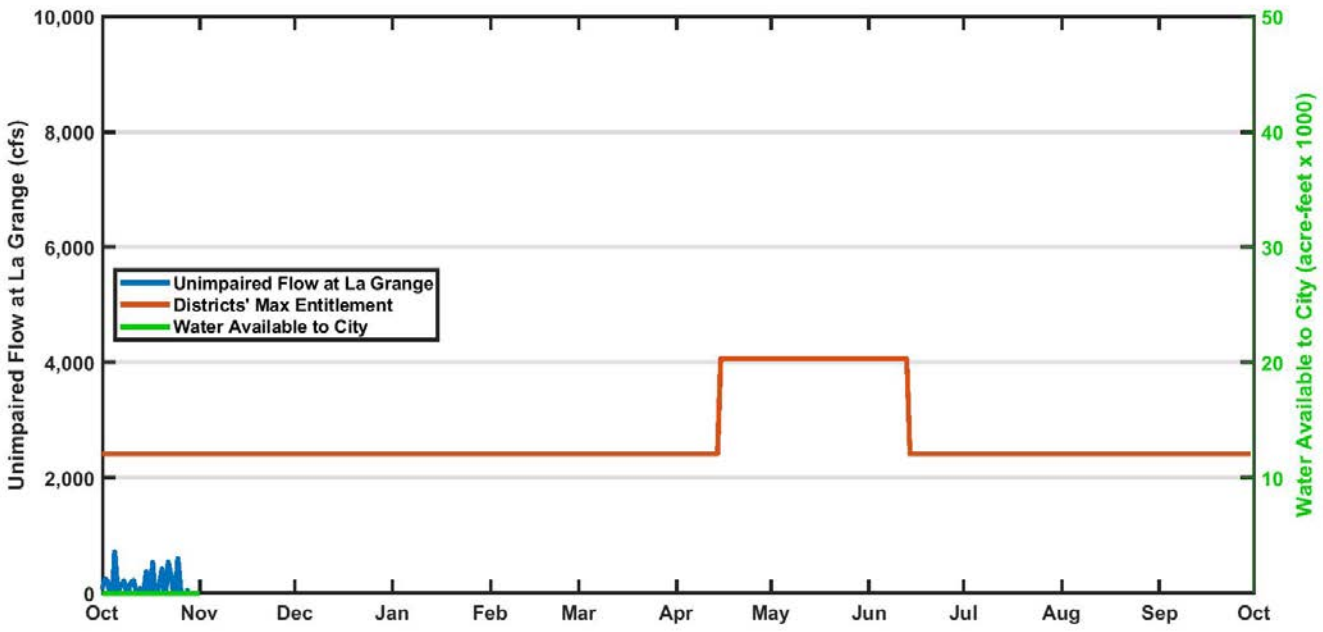


Figure 4: Calculated unimpaired flow at La Grange and the allocation of flows between the Districts and the City.

WATER SERVICE CONNECTION TRANSFER REPORT
TRANSFERS APPROVED FOR THE MONTH OF NOVEMBER 2020

DONATING APN	PROPERTY OWNER(S)	RECIPIENT APN	PROPERTY OWNER(S)	# OF CONNECTIONS	DATE
047-181-080	Steve C. & Kathy Zmay	047-282-160	K&S Development	one (1) 5/8"	November 9, 2020

STAFF REPORT

To: **Coastside County Water District Board of Directors**

From: **Mary Rogren, General Manager**

Agenda: **December 8, 2020**

Date: **December 4, 2020**

Subject: **Election of Coastside County Water District Board President and Vice-President**

Recommendation:

Consider election of officers.

Background:

Traditionally, the Coastside County Water District Board of Directors considers the election of officers for Board President and Vice-President annually, at the December Board meeting.

Fiscal Impact:

None.

STAFF REPORT

To: **Coastside County Water District Board of Directors**

From: **Mary Rogren, General Manager**

Agenda: **December 8, 2020**

Report Date: **December 4, 2020**

Subject: Approval of Coastside County Water District Response to Grand Jury Report Entitled "Ransomware: It Is Not Enough To Think You Are Protected"

Recommendation:

Approve Coastside County Water District's Response to the County of San Mateo Grand Jury Report Entitled "Ransomware: It Is Not Enough To Think You Are Protected" (see Exhibit A for draft response.)

Background:

On October 7, 2020, the 2019-2020 Grand Jury for the County of San Mateo filed a report "Ransomware: It is Not Enough to Think You are Protected" which contains findings and recommendations including best practices for County agencies to consider when developing a cybersecurity strategy (see Exhibit B for full Grand Jury report.)

Coastside County Water District ("District") along with 67 other County agencies are required to respond to the Grand Jury no later than January 5, 2021, and the response must be approved by the Board of Directors in a public meeting. The District must address the findings specifying that cyber security is important. In addition, the District will confirm in the comments that by November 30, 2020, the District has made a request for a confidential report from the District's IT consultants that addresses concerns included in the Grand Jury Report including systems security issues, backup and recovery, and prevention measures.

The District proposes that the attached draft response shown in Exhibit A be approved by the Board to be sent to the Grand Jury.

District staff takes cybersecurity issues very seriously and engaged the District's IT Consultants to prepare the confidential internal report referenced in the Grand Jury report.

EXHIBIT A - DRAFT

December __, 2020

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 8th Floor
Redwood City, CA 94063-1655

Subject: Coastside County Water District Response to Grand Jury Report Entitled "Ransomware: It Is Not Enough To Think You Are Protected"

Honorable Chou:

The Coastside County Water District (District) received the 2019-2020 Grand Jury report entitled "Ransomware: It Is Not Enough To Think You Are Protected." The District's Board of Directors reviewed the report and approved this response at the December 8 regular Board meeting. This letter responds to all of the Civil Grand Jury's findings and recommendations in the report.

Responses to Findings:

The District agrees with findings F1 and F3-F8. With regard to finding F2, the District agrees that local governments and schools across the country are involved in Ransomware attacks, however the District does not have sufficient information to know the percentage of Ransomware attacks that local governments and schools represent.

Responses to Recommendations:

R1: Each of the governmental entities in San Mateo County with an IT department or IT function (whether in-house, handled by another government unit or outsourced to a private enterprise) as listed in Appendix F, should by November 30, 2020, make a request for a report from their IT organization that addresses the concerns identified in the report, specifically:

1. System Security (Firewalls, Anti-malware/ Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, can you shut down your system quickly? What is being backed up, how it is being backed up, when are backups run, and where are the backups being stored? Have backups been tested? Can you fully restore a Server from a backup?)
3. Prevention (turning on email filtering, setting up message rules to warn users, providing employee training on phishing and providing a reporting system to flag suspect content)

Response 1: Recommendation R1 has been implemented. The District has an outside third party IT consultant and, prior to November 30, 2020, requested a report from the IT consultant that addresses system security, backup and recovery, and prevention.

R2: These confidential internal reports should be provided to the governing body by June 30, 2021. This report should describe what actions have already been taken and which will be given timely consideration for future enhancements to the existing cybersecurity plan.

Response 2: Recommendation R2 has not yet been implemented, but will be implemented by June 30, 2021.

R3: Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response 3: Recommendation R3 requires further analysis, and will be evaluated upon receipt of the report from the District's IT consultant. If the District chooses to request further guidance from the U.S. Department of Homeland Security or the County Controller's Office, it will do so by June 30, 2021.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool.

Response 4: Recommendation R4 requires further analysis, and will be evaluated upon receipt of the report from the District's IT consultant. If the District chooses to request its IT consultant to review the District's cybersecurity plan with the FCC's Cybersecurity Planning Guide and customizing the plan using FCC's Create Custom Cybersecurity Planning Guide tool, it will do so by June 30, 2021.

The District appreciates the effort that the Grand Jury put into the important cybersecurity issue and the opportunity to respond to the Grand Jury report. Please let us know if the District can provide additional information.

Very truly yours,

Chris Mickelsen
President, Board of Directors
Coastside County Water District

cc: Board of Directors
Mary Rogren, General Manager

EXHIBIT B

Superior Court of California, County of San Mateo
Hall of Justice and Records
400 County Center
Redwood City, CA 94063-1655

NEAL TANIGUCHI
COURT EXECUTIVE OFFICER
CLERK & JURY COMMISSIONER

(650) 261-5066
FAX (650) 261-5147
www.sanmateocourt.org

October 7, 2020

Governing Board
Coastside County Water District
766 Main Street
Half Moon Bay, CA 94019

Re: Grand Jury Report: "Ransomware: It Is Not Enough To Think You Are Protected"

Dear Governing Board:

The 2019-2020 Grand Jury filed a report on October 7, 2020 which contains findings and recommendations pertaining to your agency. Your agency must submit comments, within 90 days, to the Hon. Danny Y. Chou. Your agency's response is due no later than January 5, 2021. **Please note that the response should indicate that it was approved by your governing body at a public meeting.**

For all findings, your responding agency shall indicate one of the following:

1. The respondent agrees with the finding.
2. The respondent disagrees wholly or partially with the finding, in which case the response shall specify the portion of the finding that is disputed and shall include an explanation of the reasons therefore.

Additionally, as to each Grand Jury recommendation, your responding agency shall report one of the following actions:

1. The recommendation has been implemented, with a summary regarding the implemented action.
2. The recommendation has not yet been implemented, but will be implemented in the future, with a time frame for implementation.
3. The recommendation requires further analysis, with an explanation and the scope and parameters of an analysis or study, and a time frame for the matter to be prepared for discussion by the officer or director of the agency or department being investigated or reviewed, including the governing body of the public agency when applicable. This time frame shall not exceed six months from the date of publication of the Grand Jury report.
4. The recommendation will not be implemented because it is not warranted or reasonable, with an explanation therefore.

Please submit your responses in all of the following ways:

1. **Responses to be placed on file with the Clerk of the Court by the Court Executive Office.**

   - **Prepare original on your agency's letterhead, indicate the date of the public meeting that your governing body approved the response address and mail to Judge Chou.**

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655.

2. **Responses to be placed at the Grand Jury website.**

   - **Copy response and send by e-mail to: grandjury@sanmateocourt.org. (Insert agency name if it is not indicated at the top of your response.)**

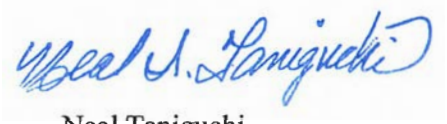
3. **Responses to be placed with the clerk of your agency.**

   - **File a copy of the response directly with the clerk of your agency. Do not send this copy to the Court.**

For up to 45 days after the end of the term, the foreperson and the foreperson's designees are available to clarify the recommendations of the report. To reach the foreperson, please call the Grand Jury Clerk at (650) 261-5066.

If you have any questions regarding these procedures, please do not hesitate to contact Paul Okada, Chief Deputy County Counsel, at (650) 363-4761.

Very truly yours,



Neal Taniguchi
Court Executive Officer

Enclosure

cc: Hon. Danny Y. Chou
Paul Okada

Ransomware:
It Is Not Enough To Think You Are Protected

ISSUE

City and county government computer systems are at risk of Ransomware attacks. Are adequate measures being taken by local government agencies to mitigate the risks and provide recovery options?

SUMMARY

Ransomware has already hit many governmental Information Technology (IT) systems in San Mateo County. In December 2019 the Grand Jury sent an online survey to all 68 public entities in San Mateo County,[1] received 37 survey responses (a 54% response rate), and interviewed several responders including one IT Manager (who had refused to respond to the survey for fear of being successfully attacked once again), for a total of 38 responses via survey and interview. More than 25% (10 of 38) of the public entities responding to the Grand Jury reported that they have been a victim of one or more Ransomware attacks. More concerning is the certainty that there will be more attempts to violate the integrity of our local governments' electronic infrastructure.

This report is intended to present "best practices" in developing a Cybersecurity strategy, then implementing and testing that plan. It addresses actions that can be taken (and have been taken, in some cases) in order to guard against Ransomware attacks, recover from an attack and the additional measures that can be taken to reduce the possibility of an attack. However, it is not an exposé with details of potential system weaknesses, in light of the need for Cybersecurity strategies and practices to be highly confidential. As such, this report walks the line between providing an informed discussion of potential concerns without providing a road map of how to breach public government IT systems.

The single largest exposure every organization has to cyber-thieves is phishing, the illegal practice of sending legitimate-looking emails to an organization's employees. These emails may contain malware or links that, when clicked, infect the computer with a virus that can spread to the entire information systems network.

Although many email software programs include some level of protection against Ransomware attacks, such protections require customization and activation, and it is not clear that local public entity IT departments are undertaking these necessary customization and activation steps. In addition, training for new employees and recurring training for existing employees is critical to dramatically reducing the probability of a Ransomware infection. In some agencies, it appears

[1] See Appendix F: Public Entities in San Mateo County (Cities, County, School Districts, Special Districts)

that only limited training is provided for new employees with little or no recurring training provided for current employees.[2]

Ransomware and other malware attacks are a test to an organization's backup and restoration procedures.[3] The Grand Jury found that none of the survey responders has actually performed a full restore as a test of their backup process. However, without adequate testing, backups do not provide sufficient protection.

Rigorous preparation for an attack is essential if fast and full recovery is desired and the payment of a ransom is to be avoided. There are several significant steps that local public entities should take to improve their defenses, their ability to detect incursions, and their responses to Ransomware attacks. These steps include:

- Using firewalls to protect internal environments from breaches;
- Using malware detection software to monitor incoming emails and network activity;
- Ensuring that users are educated and tested to learn what to watch for and avoid, especially in emails;
- Developing and fully testing a thorough backup and restore strategy to enable a complete recovery from an attack;
- Putting in place internal controls such as subnets, which require departmental authorization to access other department's data or programs.

In addition, cloud hosting should be considered for email and certain applications to reduce the success of Malware and Ransomware attacks on information systems infrastructure.

While all attacks are malicious in terms of time and potential data loss, in the case of Ransomware (or worse, Ransomware 2.0 that also infects backup data) the financial cost of paying the ransom in order to remove the infection and restore a data system can be significant. Alternatively, if the decision is to not pay the ransom but to attempt to recover from the infection manually, the direct and indirect costs could be considerably more.

This report is directed to the governing bodies of government entities in San Mateo County urging them to have their IT staff confidentially and urgently assess their respective Ransomware protection strategies and training and then move with all deliberate speed to address any shortcomings in their Cybersecurity programs.

GLOSSARY

CLOUD COMPUTING
Cloud computing is the delivery of on-demand computing services -- from applications to storage and processing power -- typically over the internet and on a pay-as-you-go basis. Rather than owning their own computing infrastructure or data centers, companies can rent access to

---

[2] Grand Jury interviews

[3] Epicor Corporation, *Protecting Yourself From Ransomware*, January 2020

anything from applications to storage from a cloud service provider.[4] Some examples of this are Yahoo Mail, services like Google Docs, and customer relationship management software.[5]

CYBERSECURITY
Cybersecurity refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.[6] Cybersecurity is a combination of secure systems (hardware and software) built into technology as well as human intervention, monitoring, training, awareness, and recovery.

ENCRYPTION
The process of locking out the contents of a file and the renaming of the file such that it cannot be opened and used in the intended application (e.g. Microsoft Excel). Typically, a 128 Bit (or larger) encryption key (a long series of letters and numbers) is used first to encrypt then later to un-encrypt a file.

MALWARE
Short for "malicious software," this software is designed specifically to damage or disrupt computer systems. Not all malware is Ransomware because some malware has no related attempt to extort money.

PHISHING
The illegal practice of sending email claiming to be from reputable companies to induce individuals to reveal personal information or click on website links or open attachments that then install malware.

RANSOMWARE
Ransomware can be simply described as an infection on a host machine that prevents access to data until a ransom is paid. The most common method of infection is to encrypt files making them totally unreadable by a user. The infection is usually delivered by a *Trojan Horse* (a term referring to the misleading of users of its true intent) installed when a user clicks on a malicious link or attachment in an email.

RANSOMWARE 2.0
This newer version of Ransomware no longer is just malware that encrypts data and asks for ransom, the attacker also threatens to release the data onto the internet and demands money in order not to do so. This newer Ransomware works in such a way that even backup copies of most important files will not be able to save an infected organization.[7] By planting the malware but delaying its activation, Ransomware 2.0 can infect backups thus defeating their value.

---

4 https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-from-public-and-private-cloud-to-software-as-a/

5 Pearson Education, Ubuntu Unleashed 2015 Edition: Covering 14.10 and 15.04, page 655

6 https://digitalguardian.com/blog/what-cyber-security

7 https://www.itproportal.com/news/welcome-to-the-era-of-ransomware-20/

BACKGROUND

Ransomware is a real and serious threat to every entity: government organizations, corporations, and individuals. The more dependence an organization has on the software and data in its network(s), the more important the concern should be. Loss of access to mission-critical data, systems, and software can severely impact an organization in both the short and long term.

According to an October 2019 report by the National League of Cities, since 2013, Ransomware attacks have been reported by at least 170 county, city or state government entities across the United States.[8] The actual number is likely to be much higher because it represents only those attacks that have been reported. Many infections go unreported when ransoms are paid,[9] when organizations are seeking to avoid embarrassment, or when the attacks were simply undetected or untraceable.[10] This has been true even in San Mateo County where local public governing entities have had Ransomware attacks that were not publicly reported.[11]

Not only do such data breaches embarrass and slow organizational productivity, they can be very expensive. For example, the MIT Technical Review (2019) asserts: "Ransomware may have cost the U.S. more than $7.5 billion in 2019... the victims were 113 governments and agencies, 764 health-care providers, and up to 1,233 individual schools affected by Ransomware attacks...most local governments do a poor job of practicing Cybersecurity."[12] The cost to the city of Atlanta to recover from its Ransomware breach was estimated at $17 million.[13] Similarly, a recent Baltimore Ransomware breach is estimated to have cost over $18 million.[14] In 2020, the UC San Francisco School of Medicine paid $1.14 million in ransom to recover its own data.[15] These are large cities and entities and although the ransom amounts they paid may not represent the expenses a San Mateo County public organization could incur, they provide examples of the severity of the potential threat and the enormous costs.

Specifically, the costs of a Ransomware attack could include some or all of the following:[16]

- Direct Costs:
    - Paying the ransom to obtain an encryption key and hoping that it works;
    - Expenditures for outside IT professionals and new systems providers to plan and implement improved breach security based on new Ransomware strategies;

---

[8] National League of Cities report, *Protecting Our Data: What Cities Should Know About Cybersecurity*. Forward by Clarence Anthony, CEO and Executive Director.

[9] https://healthitsecurity.com/news/as-ransomware-attacks-increase-dhs-alerts-to-Cybersecurity-insights

[10] Sheehan, Patrick, Ohio Emergency Management Agency, *Cascading Effects of Cyber Security on Ohio*, September 19, 2012

[11] Grand Jury survey responses

[12] MIT Technology Review, *Ransomware may have cost the US more than $7.5 billion in 2019*, January 2, 2020

[13] The Atlanta Journal- Constitution, Stephen Deere. *Confidential Report: Atlanta's cyber attack could cost taxpayers $17 million.* August 2018.

[14] Baltimore Sun, Ian Duncan, Baltimore *estimated cost of ransomware attack at $18.2 million as government begins to restore email accounts*. May 29, 2019.

[15] San Jose Mercury News, David Wu, "*UCSF pays $1.14 million ransom to recover data*", July 4, 2020

[16] https://www.sentinelone.com/blog/what-is-the-true-cost-of-a-ransomware-attack-6-factors-to-consider/

- Paying for enrollments in credit reporting bureaus to stop or correct identity thefts (from the release of previously confidential or secure personal information) for client/customers.
- Replacing hardware and/or software.

- Indirect Costs:
  - Operations efforts to restore systems and data;
  - Organizational downtime as well as employee overtime;
  - Reputation loss including negative public relations and loss of confidence by the organizations' constituents;
  - Liabilities for legal costs, including defense of lawsuits for breach of private and confidential information and poor handling of personal data.

According to the Coveware Report,[17] the median ransom payment in the first quarter of 2020 was $44,021. This was an increase of roughly 10% over the last quarter of 2019. Public sector entities represented 12% of attacks, about half of which were school systems. The average days of downtime was 15 representing an alarming number of days of inability to service constituents.[18] This underlines an urgent need to understand and evaluate current local governments' Cybersecurity strategies.

The discussion that follows is intended to encourage local public agencies and their IT staff to confidentially evaluate their respective Cybersecurity plans, software and prevention strategies. Since data and systems security are essential to the operation of every public entity in the County, the discussion will not present a specific road map for potential Ransomware-prevention actions but rather establish a "best practice model" that will enhance understanding of the elements essential for an adequate protection plan.

DISCUSSION

In December 2019, the Grand Jury developed an online survey that was sent to all 68 public entities in San Mateo County.[19] Responses were received from 37 of the entities (a 54% response rate). Additionally, follow-up interviews were conducted with three local public IT Managers, one of whom had refused to complete the online survey for fear of disclosing confidential information that could lead to a successful malware or Ransomware attack. These interviewees were questioned regarding the adequacy of Cybersecurity planning and execution. Following a general analysis of local government practices, this report concludes with a review of Cybersecurity best practices which local agencies should consider adopting.

Two Ransomware Attacks Derailed: Best Practices in Action

In order to better understand how to successfully defeat a Ransomware attack, the Grand Jury interviewed an IT Manager of a private enterprise that was attacked twice by Ransomware and was able to fully restore the environment and re-establish workflow within just a few hours.

---

17 https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report

18 https://www.msspalert.com/Cybersecurity-research/average-ransomware-payment-rises-again-research/

19 Appendix F

Given the usual secrecy involved in most malware incursions, the following description of this IT manager's actual experience is instructive since it offers an example of "best practices" that can guide others anticipating or facing a Ransomware threat.[20]

This organization suffered two serious breaches less than two months apart and successfully recovered both times. In the first breach, within 45 minutes of a user clicking on an email attachment, the Crypto virus had spread to 12 of the organization's 23 servers. The IT Manager was alerted to the problem both by the user whose PC was locked with the Ransomware demand on his screen and an auto alert from the network scanning software that reported unusual activity.

The IT Manager's first action was to rapidly shut down the entire server network. This of course stopped the spread of the virus, but also prevented users from performing their jobs. Fortunately, their backup strategy implementation worked well as they were able to fully recover within hours.

The major components of the protection strategy employed included:

- Separating the network into discrete departments or segments (creating subnets) which restricted individuals' access to only servers containing their department's software and network storage. This limited the spreading of the virus across various departments within the organization. The analogy is a modern ship with rooms and decks that can be completely closed off from each other in the event of a fire or explosion.
- Taking snapshots (copies) of their Storage Area Network (SAN) twice a day.
- Completing full nightly backups of their SQL databases and incremental backups of the databases at five-minute intervals.
- Performing server backups with a commercial external backup appliance and/or service. See Appendix D for examples of companies in this market.[21]
- Regularly testing the restore process to ensure the successful recovery of critical server hardware. Without testing, there is no assurance that the Cybersecurity plan will work. Moreover, even if it works once, that is no assurance it will work again, without periodic re-testing.
- Conducting weekly backups of critical personnel's full PC hard drives.
- Use the "3-2-1 strategy"[22]: do three backups into two different media including one offsite.

Having all of these Cybersecurity plan components was a good start but it took much more to affect a recovery. First a commercial Virus Removal Software Tool was used which did not work (in this case). Therefore, the IT team used the snapshot copies to replace corrupted data on infected server units followed by the application of the incremental backups of the database to complete the restore.

---

[20] Grand Jury Interview

[21] These services include onsite and offsite backup and recovery services which are usually located outside the immediate locale.

[22] Management Wire, *The 3-2-1 Backup Rule and Effective Cybersecurity Strategy,* January 7, 2020.

This detailed example represents a well thought out and highly prepared plan, executed with precision. The first breach resulted in 4½ hours of downtime as 12 servers were infected. The second breach resulted in 6 ½ hours of downtime to recover 19 affected servers. The IT team was able to recover the servers and their data both times, become fully operational within hours, and the organization did not pay any ransom demands.

Grand Jury Cybersecurity Survey and Follow-up Interviews

Survey question:[23] "*Has your Organization had a Ransomware attack? Specifically, has there been an instance or multiple instances when an attack has locked up a computer or computers and presented a demand for ransom to unlock the infection?*"

Nine survey responders and one non-survey responder interviewee, a total of 10 of 38 (37 responders to the online survey and one non-survey responder) affirmed an attack had occurred or had possibly occurred in their organization, a 26% "hit" rate. The circumstances of their attacks were reviewed.[24] The non-survey interviewee was the IT manager from a public entity in the County who was unwilling to complete the survey because they did not want to reveal that their organization had been subject to "one or more" Ransomware attacks. Nor were they willing to disclose how successful the Ransomware attack(s) were for fear that they would open themselves up to more attacks.

Survey Question:[25]
"*Is your Information Systems Budget adequate to secure your network properly from malicious attack?*"

Thirty-two of the 37 survey respondents, or 86%, answered Yes to this question. This high percentage of "Yes" responses either indicates a high level of confidence in their defense setup, a reluctance to complain about their IT budget, or as two of our follow-up interviewees revealed[26], a lack of understanding of the complexity of a well-written, well-executed Cybersecurity Plan.[27] Suggesting the latter, The National League of Cities conducted a similar survey of 165 city governments nationwide and asked the same question, ("*Is your budget adequate enough to secure your network properly?*"): 67% replied "No". [28]

Investigation Results Regarding Backup/Restore/Maintenance

The Grand Jury survey and follow-up interviews revealed that, while many local agencies have backup plans,[29] only a portion of those same agencies had successfully recovered lost files from backups and none of the survey responders had ever done a full restore of a server.[30] When an

---

[23] Appendix A – Question #1

[24] Grand Jury Interview

[25] Appendix A – Question #2

[26] Grand Jury Interviews

[27] Federal Communications Commission, *Cyber Security Planning Guide*, October 2012.

[28] National League of Cities report, *Protecting Our Data: What Cities Should Know About Cybersecurity*, page 8

[29] Appendix A – Question #3

[30] Appendix A – Question #4

attack occurs with inadequate backup processes in place, there is no way to recover. Moreover, a proactive and well-thought-out business continuity plan is something that all system and data administrators must embrace.

What is a good backup strategy? Certain applications provide the ability within the applications themselves to set up different types of backups and schedule them to be performed automatically. A good example of this is SQL.[31] Using a SQL-based approach, both nightly full database backups can be scheduled as well as intermittent transaction log backups (which capture activity during small time increments), so that a recovery could be completed with virtually no loss of data. These backups should then be stored according to the 3-2-1 backup rule[32] whereby three copies or versions are taken, stored on two different media, one of which is offsite. Operating systems and third-party vendors offer a multitude of backup solutions for servers. Snapshots or image backups[33] provide the most complete backup and the fastest restore option.[34]

Raj Samani, Chief Technology Officer for Europe at Intel Security captures the importance of a complete backup strategy, "Most Ransomware attacks can be avoided through good cyber hygiene and effective, regular data backups that are continually tested to ensure they can be restored if needed."[35]

As this discussion shows, the technology to prevent and if necessary, correct, the impact of a malware attack is available. Local government agencies must be pro-active and vigilant in using such to protect their data and their businesses.

Investigation Results Regarding Employee Training

Education is the best defense. "Preventing infection is far easier than correcting the situation as most of the infections are acquired either from a socially engineered email (one that appears reputable or from a familiar source), or from visiting an infected website, so controlling risk on your side is the easiest method."[36]

Answers to Survey Question #5 provide strong evidence for the need for the governing boards to review with their IT managers their defenses against cyberthreats: "*Do you provide training to employees regarding malware?*" 12 responded with a non-qualified "Yes". Nine responded "No" (24%) and 16 responded with a qualified "Yes" (42%) and described their training as needing improvements.[37] As one survey responder commented, "The answer is yes, but a lot more needs to be done."

---

31 Structured Query Language (SQL) is a programming language

32 Management Wire, *The 3-2-1 Backup Rule and Effective Cybersecurity Strategy,* January 7, 2020.

33 Image backup consists of block by block storing of the contents of a hard drive

34 https:\\www.ltnow.com/file-backup-vs-image-backup-which-is-best/

35 Zerto, Raj Samani, *Ransomware – Mitigating the Threat of Cyber Attacks, 2019*

36 Epicor, *Protecting Yourself from Ransomware,* January 2020

37 Grand Jury Survey responses

Cybersecurity training is a well-established industry – providing a focused set of classes and materials designed to reduce users' clicks on harmful links and attachments. Security training, awareness, and assessment should be a routine part of the Cybersecurity strategy in government. Deploying such a program covers the education, training and testing of employees to recognize, delete and report attempted attacks. Studies show these programs reduce but do not eliminate user error.

Government Technology magazine captured it best in their cover story entitled "In the quest to guard against cyberthreats, can we solve the people problem? The Weakest Link."[38] The article concluded that even with the best training programs and defenses, the human element may never be completely overcome.[39] This is precisely why recurring training and user testing is encouraged by best practices.

Handling Incoming Emails – Phishing Defenses

In a worldwide survey of Managed IT Service Providers (MSP's) in 2019, "67% of Ransomware attacks originated from a phishing or spam email…the easiest method of delivery and man does it pay off."[40] The greatest threats take advantage of users "within" the network, i.e., users who click on malicious links or open email attachments that contain viruses or make other mistakes that allow hackers to gain access to the entity's system or network. Trend Micro estimates that the vast majority of all attacks occur when a user clicks on something they should not.[41]

There are different ways to help the user community recognize and protect against a phishing attack. Most network environments utilize spam filters to automatically filter incoming messages. Spam filters are used to detect unsolicited, unwanted, and virus-infested email and stop it from getting into email inboxes.[42] "Additionally, malware detection software can also be highly successful in reducing the risk of Ransomware but the anti-malware definitions (a database of known infectious code) need to be constantly updated…which takes effort and time but represents the single most effective defensive strategy."[43]

Message rules can be used to flag external emails and thereby decrease the probability that a user clicks on bad content. An administrator can set up message rules on a users' client or the email server. An example of a message rule might be if the sending organization includes *@smithco.com* in the sender's address, the message is automatically moved the incoming message into a personal folder called "Smith Company." A better example would be a rule that flags all external emails (not from the host's domain) and warns about the threats of clicking on attachments or weblinks. An example of this visual potential threat message rule is displayed in Appendix C.

---

38 Government Technology Magazine, Adam Stone, *The Weakest Link*, Oct/Nov 2018

39 Ibid

40 VadeSecure – Predictive Email Defense, *Ransomware Attacks: Why Email is still the #1 Delivery Method"*, January 16, 2020

41 https://blog.trendmicro.com/online-phishing-how-to-stay-out-of-the-hackers-nets/

42 https://www.mailchannels.com/what-is-spam-filtering/

43 Epicor, *Protecting Yourself from Ransomware"*, January 2020

Message rules can be very powerful to alert users of potential threats or to be careful about what they might click on and endanger their system. Some of the vendors listed in Appendix B also can "report" a suspected phishing attempt to an IT administrator. The Grand Jury's review revealed that some of the Information Technology Services departments for local public entities have installed message rules on their email servers to notify users of external emails.[44] This is a "best practice" which all local governmental agencies should consider.

Phishing emails are easy to create, as they do not take a high level of skill to provide the illusion of legitimacy by mimicking web-site brands or using logos from Google images. They can also easily spoof (fake) an email address to look like a trusted source.[45] It can often be very difficult to catch these risky emails, as the spoofed emails are cleverly disguised. A YouTube video created by Cisco Systems illustrates the sophisticated approach a phishing email may take – "Anatomy of an Attack".[46] It shows an attacker constructing a realistic identity deception email and can be viewed at https://www.youtube.com/watch?v=4gR562GW7TI After you watch this video please note, had an email filter caught this message and flagged it as external and warned about clicking on links, the deception may have been caught.

What Does Excellent Cyber Defense Look Like?

Survey Question[47]: *"What defenses do you currently employ to block malware? Please be specific. (Firewall brand/model, Software filters/spam blocker, etc.)"*

Five survey responders did not divulge the infrastructure of their environment. 17 responders provided abbreviated details indicating they do have Cybersecurity protections in place. The remaining 15 responses were explicit about their organizations' hardware and software defense strategies. Below is a survey response that illustrates a well-protected environment using some of the best practices of Cybersecurity:

"At the first layer, we use a PAN 220 Firewall with all subscriptions enabled, (URL Filtering, Antivirus/Vulnerability, Wildfire, etc.), block all international countries both in and outbound. Once traffic is passed for email, it passes through a Barracuda spam filter, filtering and scanning phishing and virus emails, checks with External Reputation servers for known virus and spamming servers, then passes to an on-premise exchange server. The exchange servers have another layer installed, Symantec Antivirus, giving a third layer of scanning. All servers and workstations have the latest version of the antivirus installed controlled by a centralized server. Window patches are applied on a monthly basis to all servers and workstations, and servers are retired once Microsoft ends support for an operating system." [48]

The survey respondent's best practices:

- Filtering incoming email for viruses, malware, and phishing attempts;
- Utilizing protection software from multiple vendors;
- Utilizing multiple layers of defense;

---

44 Grand Jury interviews

45 Ibid

46 Cisco Systems, *Ransomware - Anatomy of an Attack,* https://www.youtube.com/watch?v=4gR562GW7TI

47 Appendix A - Question #6

48 Grand Jury Survey response

- Keeping systems up-to date.

Breaches and attacks that manage to extract data (Ransomware 2.0) expose additional risks to sensitive information. Security professionals point out additional options for securing organizational data:[49]

- Use Subnets[50] to section out servers with separate security permissions and limited access;
- Disable and block unused services, protocols and ports;
- Perform Backup & Recovery (focus on full testing of recovery);
- Strengthen the password policy (long, complex, with expiration dates);
- Employ 2-factor authentication (password then keycode) for external user access.[51]
- Install Anti-malware / Antivirus software on all machines and keep current (update at least monthly);
- Update at least monthly, patches for operating systems, firewalls, spam filters, malware, and other key applications;
- Perform monitoring and auditing of failed logins, password changes, resource usage, and services stopping.

Local public entities can get assistance from The Federal Communications Commission's (FCC) Cyber Security Planning Guide that includes a customized Cyber Security Planning Tool to craft and execute a customizable Cybersecurity plan.[52] As their introduction explains, "data security is crucial … customer and client information, payment information, personal files, bank account details … all of this information is often impossible to replace if lost and dangerous in the hands of criminals… losing (your data) to hackers or malware infection can have far graver consequences."[53] Public entities should take advantage of this Guide in reviewing the current status of their own data system security.

When answering questions of respondents via email it was found that some already use cloud hosting for email.[54] During the interviews it was further uncovered that a school IT manager is considering additional cloud hosting of one or more of their applications. Cloud providers are able to provide layers of protection for a customer's network and software, as well as creating a segregation between their network and their customers. A cloud provider will patch and maintain current software versions, leverage security and malware and have a dedicated security team (24x7x365) that is responsible for staying on top of the security risks.[55]

---

49 Government Technology Magazine, Adam Stone, *The Weakest Link*, Oct/Nov 2018

50 https://searchnetworking.techtarget.com/tutorial/Protocols-Lesson-6-IP-subnetting-The-basic-concepts

51 The County's Office of the Assessor-County Clerk-Recorder and Elections has already instituted 2-factor authentication. 2018-2019 Grand Jury Report – Security of Election Announcements.

52 Federal Communications Commission, *Cyber Security Planning Guide* https://transition.fcc.gov/cyber/cyberplanner.pdf and FCC *Cyber Security Planner* (customizable) https://www.fcc.gov/cyberplanner

53 Ibid, page PDS-1

54 eMails received from public domain accounts

55 Government Technology Magazine, Adam Stone, *The Weakest Link*, Oct/Nov 2018

Conclusions

Grand Jury survey results and in-depth interviews determined that some local government agencies have Cybersecurity strategies in place. For them, this report is asking those IT departments to re-challenge the sufficiency of their employee training, the regular (full) testing of their defense strategies and the adequacy/age of their Cybersecurity strategy including consideration of cloud hosting. For the rest, this is a good time to complete a review and see what additional measures can be taken to beef up their IT security using the information provided in this report as a guide. The biggest trap is believing that a malware attack, or in the worst case a Ransomware attack, is unlikely to happen to organizations and that the Cybersecurity strategies already in place are sufficient to successfully recover.

As learned from the best practices example of the IT manager who thwarted two attacks successfully, a comprehensive Cybersecurity plan includes user prevention steps, spam and malware software, back-ups and full recovery testing. These suggestions as well as those from the professional literature on Cybersecurity include the following list of best practices:

- Anti-Malware definitions need to be constantly updated to retain their effectiveness.
- Software updates need to be kept current.
- To identify external emails, message rules can be used to flag external emails and thereby decrease the probability that a user clicks on bad content.
- To thwart phishing attempts, footers can be added to incoming emails to warn about opening attachments and clicking on links (see Appendix C).
- Security training, awareness and assessment need to be routine along with testing all employees to recognize, delete and report attempted attacks (See Appendix B).
- Establishing a thorough and comprehensive backup process for all Servers using the 3-2-1 rule and establishing a separate backup process for key users' critical folders (e.g., administration, accounting, human resources) to be able to restore/recover from a secure onsite and/or offsite backup.
- Snapshots and/or image backups provide the most complete backup and the fastest recovery option.
- Consider cloud-hosting of email and other applications to provide added security, backup & restore capabilities and filtering benefits to close the largest and easiest route for Ransomware to penetrate entity systems.

FINDINGS

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

F3. The direct and indirect costs of Ransomware can be significant.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

RECOMMENDATIONS

The Grand Jury recommends that each governing body undertake its own confidential effort to protect against Ransomware attacks. Specifically:

R1. Each of the governmental entities in San Mateo County with an IT department or IT function (whether in-house, handled by another government unit or outsourced to a private enterprise) as listed in Appendix F, should by November 30, 2020, make a request for a report from their IT organization that addresses the concerns identified in the report, specifically:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, can you shut down your system quickly? What is being backed up, how it is being backed up, when are backups run, and where are the backups being stored? Have backups been tested? Can you fully restore a Server from a backup?)
3. Prevention (turning on email filtering, setting up message rules to warn users, providing employee training on phishing and providing a reporting system to flag suspect content)

R2. These confidential internal reports should be provided to the governing body by June 30, 2021. This report should describe what actions have already been taken and which will be given timely consideration for future enhancements to the existing cybersecurity plan.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security[56] and/or a cyber hygiene assessment from the County Controller's Office.[57]

---

[56] https://www.us-cert.gov/resources/assessments

[57] 2018-2019 San Mateo Grand Jury Report – Security of Election Announcements

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

METHODOLOGY

Documents

- Attack incident reports were requested from IT Departments who experienced attack(s). No incident reports were received.

Site Tours

- No site tours were performed as a part of this report.

Interviews

Reports issued by the Civil Grand Jury do not identify individuals interviewed. Penal Code Section 929 requires that reports of the Grand Jury not contain the name of any person or facts leading to the identity of any person who provides information to the Civil Grand Jury.

- Three Information Systems Managers of three different public entity IT organizations.
- Two non-public professional IT Managers. Both of these Managers' IT infrastructure environments had been infected with Ransomware attacks. One paid the ransom and the other did not.
- A professional Ransomware expert who often consults with companies who have been attacked or desire assistance preventing attacks. He also teaches classes on preparing for and preventing Ransomware attacks.
- Numerous security industry professionals at the RSA Conference held at Moscone Center in San Francisco between February 24th and 28th 2020.

BIBLIOGRAPHY

Anslinger, Joe. *"File Backup vs. Image Backup – Which is Best?"* Lieberman Technology. June 11, 2013. https://www.ltnow.com/file-backup-vs-image-backup-which-is-best/

Cisco Systems. *Ransomware - Anatomy of an Attack.* https://www.youtube.com/watch?v=4gR562GW7TI

Coveware, *"Ransomware Payments Increase In Evolving Distribution of Enterprise Ransomware Variants."* April 29, 2020. https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report

Davis, Jessica. *"As Ransomware Attacks Increase, DHS Alerts to Cybersecurity Insights."* Health IT Security, September 9, 2019. https://healthitsecurity.com/news/as-ransomware-attacks-increase-dhs-alerts-to-cybersecurity-insights

Deere, Stephen. *"Confidential Report: Atlanta's Cyber Attack Could Cost Taxpayers $17 Million."* The Atlanta Journal- Constitution. August 2018.

Department of Homeland Security (DHS): Cybersecurity and Infrastructure Security Agency (CISA). *"Assessments: Cyber Resilience Review (CRR)"* https://www.us-cert.gov/resources/assessments

Duncan, Ian. *"Baltimore Estimated Cost of Ransomware Attack at $18.2 Million as Government Begins to Restore Email Accounts."* Baltimore Sun, May 29, 2019.

Epicor Corporation. *Protecting Yourself From Ransomware*. January 2020.

Fadilpasic, Sead. *"Welcome to the era of Ransomware 2.0"* ITProPortal. February 12, 2020. https://www.itproportal.com/news/welcome-to-the-era-of-ransomware-20/

Federal Communications Commission. *Cyber Security Planning Guide.* https://www.fcc.gov/cyber/cyberplanner.pdf

Gutman, Yotam. *"What is the True Cost of a Ransomware Attack."* SentinelOne. January 8, 2020. https://www.sentinelone.com/blog/what-is-the-true-cost-of-a-ransomware-attack-6-factors-to-consider/

Iloh, Raphael. *"The 3-2-1 Backup Rule and Effective Cybersecurity Strategy."* Management Wire. January 7, 2020. https://www.managementwire.com/the-3-2-1-backup-rule-and-effective-cybersecurity-strategy/

Jendre, Adrien." *Ransomware Attacks: Why Email Is Still the #1 Delivery Method."* Vade Security. January 16, 2020. https://www.vadesecure.com/en/ransomware-attacks-why-email-is-still-the-1-delivery-method/

Kass, DH. *"Average Ransomware Payment Rises Again: Research."* MSSP Alert. April 30, 2020. https://www.msspalert.com/cybersecurity-research/average-ransomware-payment-rises-again-research/

Kraft Technology Group. *"When Was The Last Time You Tested Your Business Backups?"* https://www.kraftgrp.com/when-was-the-last-time-you-tested-your-business-backups/

MailChannels. *"What is Spam Filtering?"* https://www.mailchannels.com/what-is-spam-filtering/

MIT Technology Review, *"Ransomware May Have Cost the US More Than $7.5Billion in 2019."* January 2, 2020. https://www.technologyreview.com/2020/01/02/131035/ransomware-may-have-cost-the-us-more-than-75-billion-in-2019/

National League of Cities Report. *"Protecting Our Data: What Cities Should Know About Cybersecurity."* Forward by Clarence Anthony, CEO and Executive Director.

Pearson Education. *Ubuntu Unleashed.* 2015 Edition. Page 655.

Ranger, Steve. *"What is cloud computing? Everything you need to know about the cloud explained."* ZD Net, December 13, 2018. https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-from-public-and-private-cloud-to-software-as-a/

Samani, Raj. *"Ransomware – Mitigating the Threat of Cyber Security Attacks."* Zerto. 2019. https://www.zerto.com/wp-content/uploads/2019/09/ransomware-mitigating-the-threat-of-cyber-security-attacks.pdf

San Mateo Grand Jury Report. *Security of Election Announcements*. 2018-2019.

Search Networking, *"Protocols, Lesson 6: IP subnetting - The basic concepts."* October 2004. https://searchnetworking.techtarget.com/tutorial/Protocols-Lesson-6-IP-subnetting-The-basic-concepts

Sheehan, Patrick. *"Cascading Effects of Cyber Security on Ohio."* Ohio Emergency Management Agency. September 19, 2012.

Stone, Adam. *The Weakest Link.* Government Technology Magazine, October/November 2018.

Trend Micro. *"Online Phishing: How To Stay Out Of The Hackers' Nets"* November 20, 2019. https://blog.trendmicro.com/online-phishing-how-to-stay-out-of-the-hackers-nets/

Wu, David. *"UCSF pays $1.14 Million Ransom to Recover Data."* San Jose Mercury News. July 4, 2020.

APPENDIX A – SURVEY QUESTIONS

1. Has your Organization had a Ransomware attack? Specifically, has there been an instance or multiple instances when an attack has locked up a computer or computers and presented a demand for ransom to unlock the infection?

If you answered Yes or Possibly to Question 1, please provide a detailed description of the attack. What actions were taken once the attack was realized?

2. Is your Information Systems Budget adequate to secure your network properly from malicious attack?

3. Please provide an explanation of your Systems Backup processes? How often are backups run, where do you store the Backups?

4. Have you ever had to Restore from Backups? Please describe in detail why you did the Restore and describe the process used.

5. Do you provide training to employees regarding Malware?

6. What defenses do you currently employ to block malware? Please be specific. (Firewall brand/model, Software filters/spam blocker, etc.)

APPENDIX B – EMPLOYEE TRAINING OPTIONS

Phishing is the primary method of entry in cyber-attacks worldwide. Over the past few years, some security industry companies have come up with excellent testing, training, monitoring, measuring and reporting solution to help with employee training. The primary goal of an employee training program is to change user's behavior when viewing emails that might contain threats.

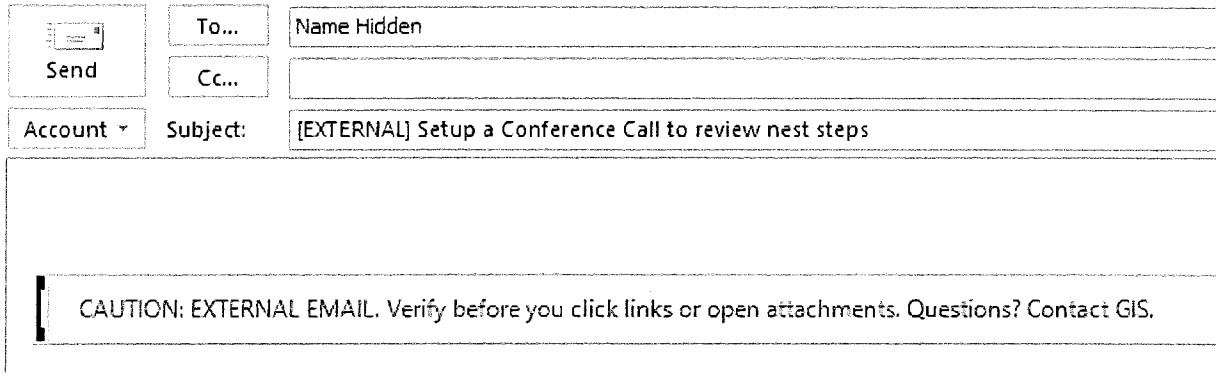
The typical components of these solutions include:

- Customized phishing attacks designed to test employees in spotting attack attempts
- Provide users a simple to use reporting tool to flag suspected attacks
- An incidence response platform for controlling the spread of an attack
- Reporting dashboards tracking user click-throughs
- Employee training programs

Here are some website links for the companies offering training solutions.
www.knowbe4.com
www.lucysecurity.com
www.metacompliance.com
www.mediapro.com
www.cofense.com
www.elevatesecurity.com
www.securitymentor.com

www.habitu8.io

APPENDIX C – EMAIL MESSAGE RULE - EXTERNAL



APPENDIX D – BACKUP & RECOVERY APPLIANCES & SERVICES

There are a large number of companies that provide Backup and Recovery solutions. Solutions Review has prepared a buyer's guide for the leading vendors. Click on the following link or copy and paste this URL into a browser to get your own copy of this guide.

https://solutionsreview.com/backup-disaster-recovery/get-a-free-backup-and-disaster-recovery-buyers-guide/

Specifically, some of the vendors in this report do not provide appliances, only virtual server support. Here is a partial list of appliance and solution vendors:

www.unitrends.com
www.barracuda.com
www.carbonite.com
www.commvault.com
www.dellemc.com
www.axcient.com
www.cohesity.com
www.datto.com
www.infrascale.com

APPENDIX E – PHISHING DEFENSE VENDORS

Some companies that provide solutions that improve email defenses are:

https://www.opswat.com/products/metadefender/email-gateway-security
https://www.agari.com/products/phishing-defense/
https://www.inky.com/anti-phishing-software
https://www.mimecast.com/products/email-security-with-targeted-threat-protection/

APPENDIX F: PUBLIC ENTITIES IN SAN MATEO COUNTY (68)

City/Town Governments (20)

Town of Atherton
City of Belmont
City of Brisbane
City of Burlingame
City of Colma
City of Daly City
City of East Palo Alto
City of Foster City
City of Half Moon Bay
City of Hillsborough
City of Menlo Park
City of Millbrae
City of Pacifica
Town of Portola Valley
City of Redwood City
City of San Bruno
City of San Carlos
City of San Mateo
City of South San Francisco
Town of Woodside

County Government (1)

County of San Mateo, Information Services Department

School Districts (25)

Bayshore Elementary School District
Belmont Redwood Shores School District
Brisbane School District
Burlingame School District
Cabrillo Unified School District
Hillsborough City School District
Jefferson Elementary School District
Jefferson Union High School District
La Honda Pescadero School District
Las Lomitas Elementary School District
Menlo Park City School District
Millbrae School District
Pacifica School District
Portola Valley School District
Ravenswood City School District
Redwood City School District
San Bruno Park School District
San Carlos School District

San Mateo Foster City School District
San Mateo Union High School District
Sequoia Union High School District
San Mateo County Community College School District
San Mateo County Office of Education
South San Francsico Unified School District
Woodside School District

Independent Special Districts (22)
Bayshore Sanitary District
Broadmoor Police Protection District
Coastside County Water District
Coastside Fire Protection District
Colma Fire Protection District
East Palo Alto Sanitary District
Granada Community Services District
Highlands Recreation District
Ladera Recreation District
Menlo Park Fire Protection District
Mid Peninsula Regional Open Space District
Mid-Peninsula Water District
Montara Water and Sanitary District
North Coast County Water District
Peninsula Health Care District
San Mateo County Harbor District
San Mateo County Mosquito and Vector Control District
San Mateo County Resource Conservation District
Sequoia Healthcare
West Bay Sanitary District
Westborough Water District
Woodside Fire Protection District

Not Included: County-governed special districts and subsidiary special districts governed by their respective city councils.

Issued: October 7, 2020

MONTHLY REPORT

To: **Mary Rogren, General Manager**

From: **James Derbin, Superintendent of Operations**

Agenda: **December 8, 2020**

Report Date: **December 3, 2020**

Monthly Highlights

- Denniston Water Treatment Plant started on 11/30/20 @ 300gpm
- Pilarcitos wells running at 275gpm
- Pilarcitos Reservoir ~450gpm
- Replaced Hydrants at:
    - 141 Kelly Avenue
    - 491 Kelly Avenue
    - 171 Escalona Avenue
    - 251 Sonora Avenue

Sources of Supply

- **November Sources:**
    - Crystal Spring, Denniston Reservoir/Wells, Pilarcitos Reservoir/Wells

Projects

- Denniston Generators installed, factory startup/testing partially complete. Issue with ATS cabinets. Cummins is resolving at their cost.
- Emergency pump for Pilarcitos dam will arrive in December
- Staff has requested a proposal from Brown and Caldwell and HDR for engineering design of a DN prestressed replacement tank for HMB #3.
- Valve truck VIN Number issued from Ford, Whachs equipment at Scelzi waiting for chassis to install equipment
- HDR – Nunes Upgrades - Bi-weekly progress meetings with staff ongoing. 90% design delivered in November. Staff providing review comments and expect 100% design by end of December, out to bid January, award middle of February.
- EKI – 90% on Pilarcitos crossing replacement. Waiting for Biological Resources Evaluation from WRA before staff can start the CDP process.

STAFF REPORT

To: **Board of Directors**

From: **Cathleen Brennan, Water Resources Analyst**

Agenda: **December 8, 2020**

Report: December 3, 2020

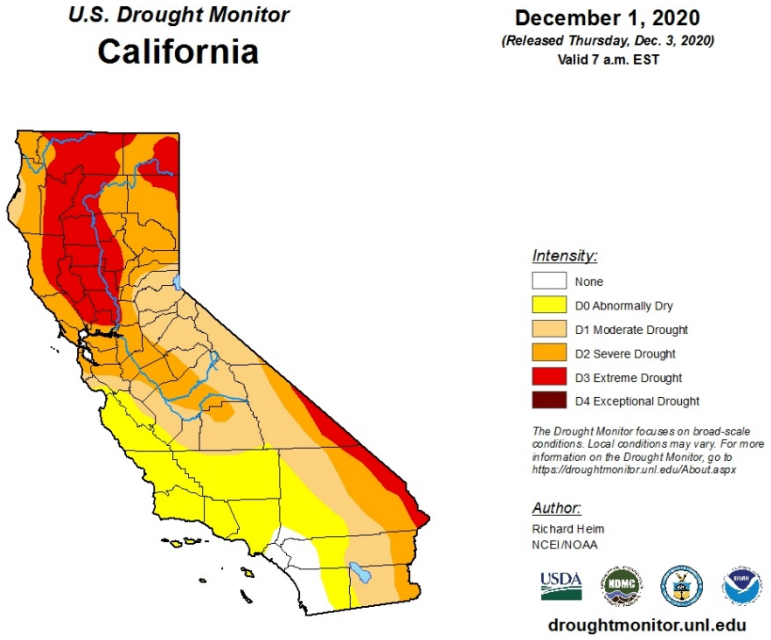
Subject: Water Resources Informational Report

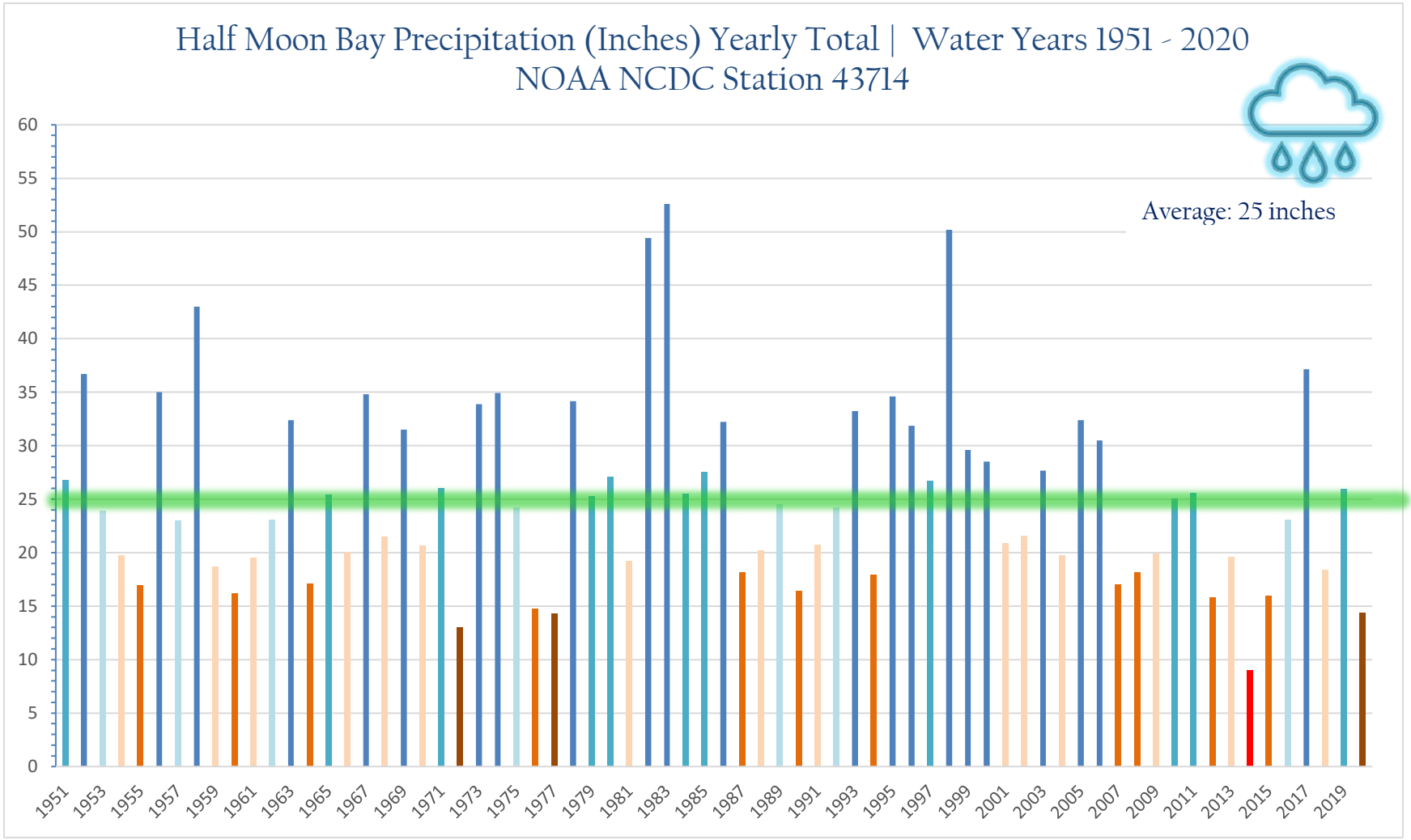
Water Year 2020 Summary and Current Water Year 2021 Conditions

Half Moon Bay had less than average precipitation for Water Year 2020 (October 1, 2019 – September 30, 2020) at approximately 14 inches. The SFPUC[i] reported less than average precipitation totals for both the regional watersheds and the Hetch Hetchy watershed for Water Year 2020.

Summary Table for Water Year 2020 by Watershed		
Watershed	Percent of Average	Total (inches)
Hetch Hetchy	62	22.08
Pilarcitos Reservoir	64	24.1
Crystal Springs Reservoir (lower)	57	15.13
Calaveras Reservoir	57	13.37
Half Moon Bay	57	14.40

Water Year 2021 has started out dry for California with La Niña[ii] conditions in the east central equatorial Pacific Ocean.





[i] SFPUC, Hydrological Conditions Report September 2020, 10/11/2020

[ii] National Oceanic and Atmospheric Administration, https://oceanservice.noaa.gov/facts/ninonina.html, 02/10/2020