

City of Guadalupe
Notes to Basic Financial Statements
For the year ended June 30, 2019

8. EMPLOYEE RETIREMENT PLANS, Continued

E. Actuarial Assumptions

The total pension liabilities in the June 30, 2017 actuarial valuations were determined using the following actuarial assumptions:

Valuation Date	June 30, 2017
Measurement Date	June 30, 2018
Actuarial Cost Method	Entry-Age Normal in accordance with the requirements of GASB 68
Actuarial Assumptions:	
Discount Rate	7.15%
Inflation	2.75%
Projected Salary Increase	Varies by entry age and service
Mortality(1)	Derived using CalPERS' membership data for all funds
Post Retirement Benefit Increase	Contract COLA up to 2.75% until purchasing power protection allowance floor on purchasing power applies, 2.75% thereafter

(1) The underlying mortality assumptions and all other actuarial assumptions used in the June 30, 2017 valuation were based on the results of a January 2014 actuarial experience study for the period 1997 to 2011. Further details of the Experience Study can found on the CalPERS website.

F. Discount Rate

The discount rate used to measure the total pension liability was 7.15% for the Plan. To determine whether the municipal bond rate should be used in the calculation of a discount rate for the Plan, CalPERS stress tested plans that would most likely result in a discount rate that would be different from the actuarially assumed discount rate. Based on the testing, none of the tested plans run out of assets. Therefore, the current 7.15 percent discount rate is adequate and the use of the municipal bond rate calculation is not necessary. The long-term expected discount rate of 7.15 percent will be applied to all plans in the Public Employees Retirement Fund (PERF). The stress test results are presented in a detailed report that can be obtained from the CalPERS website.

The long-term expected rate of return on pension plan investments was determined using a building-block method in which best-estimate ranges of expected future real rates of return (expected returns, net of pension plan investment expense and inflation) are developed for each major asset class.

In determining the long-term expected rate of return, CalPERS took into account both short-term and long-term market return expectations as well as the expected pension fund cash flows. Using historical returns of all the funds' asset classes, expected compound returns were calculated over the short-term (first 10 years) and the long-term (11-60 years) using a building-block approach. Using the expected nominal returns for both short-term and long-term, the present value of benefits was calculated for each fund. The expected rate of return was set by calculating the single equivalent expected return that arrived at the same present value of benefits for cash flows as the one calculated using both short-term and long-term returns. The expected rate of return was then set equivalent to the single equivalent rate calculated above and rounded down to the nearest one quarter of one percent.

City of Guadalupe
Notes to Basic Financial Statements
For the year ended June 30, 2019

8. EMPLOYEE RETIREMENT PLANS, Continued

F. Discount Rate, Continued

The table below reflects the long-term expected real rate of return by asset class. The rate of return was calculated using the capital market assumptions applied to determine the discount rate and asset allocation. These rates of return are net of administrative expenses.

Asset Class(1)	Assumed asset allocation	Real return years 1 - 10(2)	Real return years 11+(3)
Global equity	50.00%	4.80%	5.98%
Fixed income	28.00%	1.00%	2.62%
Inflation assets	—	0.77%	1.81%
Private equity	8.00%	6.30%	7.23%
Real assets	13.00%	3.75%	4.93%
Liquidity	1.00%	—	-0.92%
Total	100.00%		

(1) In the Sytem's CAFR, Fixed income is included in Global debt securities;

Liquidity is included in Short-term investments;

Inflation assets are included in both Global equity securities and Global debt securities

(2) An expected inflation of 2.00% used for this period.

(3) An expected inflation of 2.92% used for this period.

Sensitivity of the Proportionate Share of the Net Pension Liability to Changes in the Discount Rate – The following presents the City's proportionate share of the net pension liability for the Plan, calculated using the discount rate for the Plan, as well as what the City's proportionate share of the net pension liability would be if it were calculated using a discount rate that is 1-percentage point lower or 1-percentage point higher than the current rate:

1% Decrease	6.15%
Net Pension Liability	\$ 5,002,476
Current Discount Rate	7.15%
Net Pension Liability	\$ 3,050,995
1% Increase	8.15%
Net Pension Liability	\$ 1,445,435

G. Payable to the Pension Plan

At June 30, 2019 the City reported a payable of \$0 for outstanding amount of contributions to the pension plan required for the year ended June 30, 2019.

City of Guadalupe
Notes to Basic Financial Statements
For the year ended June 30, 2019

9. OTHER POST EMPLOYMENT BENEFITS

A. Plan Description

The City's other post-employment benefits (OPEB) plan, an agent multiple-employer defined benefit plan, is for retiree health benefits and is administrated by the California Public Employees Retirement System (PERS) Health Benefit Program. The City entered the PERS medical insurance program in 1990 under the Public Employees Medical and Hospital Care Act (PEMHCA). The required employer contribution was \$133-\$136 per month for each retiree, spouse or surviving spouse, and dependent. The City provides post-employment health care insurance to all employees who retire from the City on or after attaining age 50 with at least 5 years of PERS credited service. For employees first covered under PERS on or after January 1, 2013, the eligibility requirements are attaining age 52 and 5 years of PERS credited service. Benefits are paid for the lifetime of the retiree, spouse or surviving spouse, and dependents up to the age of 65. The City's OPEB Plan does not issue a publicly available financial report.

B. Employees Covered

The following current and former employees were covered by the benefit terms under the OPEB plan as of the July 1, 2018 actuarial valuation:

Active Employees	28
Inactive employees or beneficiaries currently receiving benefits	3
	31

C. Contributions

The City currently finances benefits on a pay-as-you-go basis, and sets its maximum monthly contribution rates for health insurance on behalf of active employees according to the PEMHCA statutory minimum. The minimum was \$133 per month for calendar year 2018 and \$136 per month for calendar year 2019. This amount is indexed to the rate of medical inflation and increased each year accordingly. The City also pays a 0.32% of premiums as an administrative fee on behalf of employees and retirees. For the measurement period July 1, 2018 to June 30, 2019, the City contributed \$4,842 in benefit payments for retirees.

City of Guadalupe
Notes to Basic Financial Statements
For the year ended June 30, 2019

9. OTHER POST EMPLOYMENT BENEFITS, Continued

D. Total OPEB Liability

The City's total OPEB liability was measured as of June 30, 2019, and was determined by an actuarial valuation as of July 1, 2018. Standard actuarial update procedures were used to project/discard from the valuation to measurement dates. The total OPEB liability was determined using the following actuarial assumptions, applied to all periods included in the measurement, unless otherwise specified:

Discount Rate	3.13%
Salary increases	3.00%
Healthcare cost trend rate	5.90% for 2019, decreasing 0.10% each year to an ultimate rate of 5.00% for 2028 and later years

Pre-retirement mortality rates were based on the RP-2014 Employee Mortality Table for Males or Females, as appropriate, without projection.

Post-retirement mortality rates were based on the RP-2014 Health Annuitant Mortality Table for Males or Females, as appropriate, without projection.

Actuarial assumptions used in the July 1, 2018 valuation were based on a review of plan experience during the period July 1, 2016 to June 30, 2018.

The discount rate used to measure the total OPEB liability was 3.13%, which reflects the municipal bond 20-year high grade index rate, and assumes the net fiduciary position of the plan remains at \$0.

E. Changes in the Total OPEB Liability

	Increase (Decrease)
	Total OPEB Liability
Balance at June 30, 2018	
(Measurement date 06/30/2018)	\$ 251,163
Changes in the year:	
Service cost	22,620
Interest	11,639
Changes of benefit terms	-
Difference between expected and actual experience	72,513
Changes of assumptions	31,372
Benefit payments	(4,842)
Net changes	133,302
Balance at June 30, 2019	
(Measurement date 06/30/2019)	\$ 384,465

City of Guadalupe
Notes to Basic Financial Statements
For the year ended June 30, 2019

9. OTHER POST EMPLOYMENT BENEFITS, Continued

F. Sensitivity of the Total OPEB Liability to Changes in the Discount Rate

The following presents the net OPEB liability of the City, as well as what the City's net OPEB liability would be if it were calculated using a discount rate that is 1-percentage-point lower (2.13 percent) or 1-percentage point higher (4.13 percent) than the current discount rate:

	1% Decrease 2.13%	Discount Rate 3.13%	1% Increase 4.13%
Total OPEB Liability (Asset)	\$ 460,601	\$ 384,465	\$ 324,527

G. Sensitivity of the Total OPEB Liability to Changes in the Healthcare Cost Trend Rate

The following presents the total OPEB liability of the City, as well as what the City's total OPEB liability would be if it were calculated using a healthcare cost trend rate that is 1-percentage-point lower (4.00 percent) or 1-percentage point higher (6.00 percent) than the current healthcare cost trend rate:

	1% Decrease (4.90% decreasing to 4.00%)	Trend Rate (5.90% decreasing to 5.00%)	1% Increase (6.90% decreasing to 6.00%)
Total OPEB Liability (Asset)	\$ 314,787	\$ 384,465	\$ 475,775

H. OPEB Expense and Deferred Outflows and Inflows of Resources

At June 30, 2019, the City's deferred outflows of resources and deferred inflows of resources to OPEB from the following sources are as follows:

	Deferred Outflows of Resources	Deferred Inflows of Resources
Difference between expected and actual experience	\$ 64,365	\$ -
Changes in assumptions or other inputs	27,847	-
Differences between projected and actual return on investments	-	-
	<u>\$ 92,212</u>	<u>\$ -</u>

Amounts reported as deferred outflows and deferred inflows of resources will be recognized in OPEB expense as follows:

Fiscal year ending June 30,	Pension Expense
2020	\$ 11,673
2021	11,673
2022	11,673
2023	11,673
2024	11,673
2025-2027	33,847

For the fiscal year ended June 30, 2019, the City recognized OPEB expense of \$45,932.

10. CONTINGENCIES AND COMMITMENTS

A. *Litigation*

The City is presently involved in certain matters of litigation that have arisen in the normal course of conducting City business. City management believes, based upon consultation with the City Attorney, that these cases, in the aggregate, are not expected to result in a material adverse financial impact on the City. Additionally, City management believes that the City's insurance programs are sufficient to cover any potential losses should an unfavorable outcome materialize.

B. *Grant Commitments*

The City had received state and federal funds for specific purposes that are subject to review and audit by the grantor agencies. Although such audits could generate expenditure disallowances under terms of the grants, it is believed that any required reimbursements will not be material.

11. SUCCESSOR AGENCY TRUST FOR ASSETS OF THE FORMER REDEVELOPMENT AGENCY

On December 29, 2011, the California Supreme Court upheld Assembly Bill 1X 26 (the "Bill") that provides for the dissolution of all redevelopment agencies in the State of California. This action impacted the reporting entity of the City of Guadalupe that previously had reported the City's Redevelopment Agency within the reporting entity as a blended component unit.

The Bill provided that upon dissolution of a redevelopment agency, either the City or another unit of local government will agree to serve as the "successor agency" to hold the assets until they are distributed to other units of state and local government. On January 9, 2012, the City Council elected to become the Successor Agency for the former Redevelopment agency in accordance with the Bill as part of City Resolution No. 2 (2012).

After enactment of the law, which occurred on June 28, 2011, redevelopment agencies in the State of California were prohibited from entering into new projects, obligations or commitments. Subject to the control of a newly established oversight board, remaining assets could only be used to pay enforceable obligations in existence at the date of dissolution (including the completion of any unfinished projects that were subject to legally enforceable contractual commitments).

In future fiscal years, successor agencies will only be allocated revenue in the amount that is necessary to pay the estimated annual installment payments on enforceable obligations of the former redevelopment agency until all enforceable obligations of the prior redevelopment agency have been paid in full and all assets have been liquidated.

The Bill directs the State Controller of the State of California to review the propriety of any transfers of assets between redevelopment agencies and other public bodies that occurred after January 1, 2011. If the public body that received such transfers is not contractually committed to a third party for the expenditure of encumbrance of those assets, the State Controller is required to order the available assets to be transferred to the public body designated as the successor agency of the Bill.

City of Guadalupe
Notes to Basic Financial Statements
For the year ended June 30, 2019

**11. SUCCESSOR AGENCY TRUST FOR ASSETS OF THE FORMER REDVELOPMENT AGENCY,
Continued**

Management believes, in consultation with legal counsel, that the obligations of the former redevelopment agency due to the City are valid enforceable obligations payable by the successor agency trust under the requirements of the Bill. The City's position on this issue is not a position of settled law and there is a considerable legal uncertainty regarding this issue. It is reasonably possible that a legal determination may be made at a later date by an appropriate judicial authority that would resolve this issue unfavorably to the City.

In accordance with the timeline set forth in the Bill (as modified by the California Supreme Court on December 29, 2011) all redevelopment agencies in the State of California were dissolved and ceased to operate as a legal entity as of February 1, 2012. After the date of dissolution, the assets and activities of the dissolved redevelopment agency were transferred to and are reported in a fiduciary fund (private-purpose trust fund, the Trust Fund) in the financial statements of the City.

A. Cash and Investments

The City maintained investments with the State of California Local Agency Investment Fund (LAIF) for all City activities, including the Trust Fund. The Trust had \$991,979 in cash and investments as of June 30, 2019, that was held in LAIF. The City manages the Trust Fund's cash and investments in a consistent manner with the rest of its cash and investment pool. Refer to Note 2 for additional information regarding LAIF.

B. Cash with Fiscal Agent

The Trust Fund had \$300,798 in cash and investments as of June 30, 2019, held by fiscal agents pledged for the payment or security of certain bonds. The California Government code provides that these monies, in the absence of specific statutory provisions governing the issuance of bonds, certificates, or leases, may be invested in accordance with the ordinance, resolutions, or indentures specifying the types of investments its fiscal agents may make. These ordinances, resolutions, and indentures are generally more restrictive than the Trust's general investment policy. In no instance have additional types of investments, not permitted by the Trust's general investment policy, been authorized.

C. Property Held for Resale

At June 30, 2019, the carrying value of property held for resale was as follows:

West side of Obispo Street	\$	105,507
Next door to Royal Theatre		75,308
Royal Theatre		41,667
Total	\$	222,482

City of Guadalupe
Notes to Basic Financial Statements
For the year ended June 30, 2019

11. SUCCESSOR AGENCY TRUST FOR ASSETS OF THE FORMER REDVELOPMENT AGENCY,
Continued

D. Capital Assets

For the year ended June 30, 2019, capital assets activity was as follows:

	Balance June 30, 2018	Transfers/ Additions	Retirements	Balance June 30, 2018
Capital assets being depreciated				
Infrastructure	\$ 201,197	\$ -	\$ -	\$ 201,197
Structures and improvements	83,333	-	-	83,333
Less accumulated depreciation	(121,170)	(9,900)	-	(131,070)
Net capital assets	<u>\$ 163,360</u>	<u>\$ (9,900)</u>	<u>\$ -</u>	<u>\$ 153,460</u>

E. Long-Term Liabilities

For the year ended June 30, 2019, long-term liabilities activity was as follows:

	Balance June 30, 2018	Additions	Deductions	Balance June 30, 2019	Due within One Year
Note payable	\$ 9,861	\$ 720	\$ (4,859)	\$ 5,722	\$ 4,215
2017 Tax allocation bonds	4,900,000	-	(260,000)	4,640,000	215,000
Discount on 2017 bonds	(98,965)	-	5,498	(93,467)	-
Total	<u>\$ 4,810,896</u>	<u>\$ 720</u>	<u>\$ (259,361)</u>	<u>\$ 4,552,255</u>	<u>\$ 219,215</u>

Note Payable

The Trust Fund had a note payable to a private party related to the purchase of property currently held for resale. Principal and interest payments on the note payable are due on the 16th of each month and the note matures in 2021. Interest accrues at 9.0% per annum. At June 30, 2019, the principal balance outstanding was \$5,722.

At June 30, 2019, the aggregate maturities of the note payable were as follows:

For the Year Ending June 30,	Principal	Interest	Total
2020	\$ 4,215	\$ 515	\$ 4,730
2021	1,507	136	1,643
Total	<u>\$ 5,722</u>	<u>\$ 651</u>	<u>\$ 6,373</u>

City of Guadalupe
Notes to Basic Financial Statements
For the year ended June 30, 2019

11. SUCCESSOR AGENCY TRUST FOR ASSETS OF THE FORMER REDVELOPMENT AGENCY,
Continued

E. Long-Term Liabilities, Continued

Tax Allocation Bonds

On April 3, 2003, the former redevelopment agency issued \$6,455,000 of tax allocation bonds for a refunding of Series 1997 Tax Allocation Bonds. The bonds were scheduled to mature through August 1, 2035, with interest rates from 2.0 to 5.125%.

On November 1, 2017, the Successor Agency to the Guadalupe Community Redevelopment Agency issued \$4,900,000 of tax allocation bonds (Bonds) to refund the 2003 series bonds. The refunding was undertaken to reduce total future debt service payments. The refunding resulted in \$1,326,400 gross debt service (principal and interest) savings over 18 years, an economic gain of \$147,832, and an accounting deferred loss on refunding of \$92,886.

The scheduled payment of principal of and interest on the Bonds when due is guaranteed under an insurance policy issued concurrently with the Bonds. The Bonds mature through August 1, 2035, with interest rates from 1.5% to 3.5%. Principal on the bonds is due annually on August 1 of each year, commencing August 1, 2018, and interest on the Bonds is due semiannually on February 1 and August 1 of each year, commencing February 1, 2018. At June 30, 2019, the total principal and interest remaining to be paid on the bonds was \$6,065,034. The outstanding principal balance net of bond discounts was \$4,546,533.

For the year ended June 30, 2019, the aggregate maturities of the tax allocation bonds were as follows:

For the Year Ending June 30,	Principal	Interest	Total
2020	215,000	140,681	355,681
2021	220,000	136,331	356,331
2022	225,000	131,600	356,600
2023	230,000	126,194	356,194
2024	240,000	120,019	360,019
2025-2029	1,295,000	488,547	1,783,547
2030-2034	1,530,000	257,600	1,787,600
2035-2036	685,000	24,062	709,062
Subtotal	4,640,000	\$ 1,425,034	\$ 6,065,034
Bond Discount	(93,467)		
	<u>\$ 4,546,533</u>		

City of Guadalupe
Notes to Basic Financial Statements
For the year ended June 30, 2019

11. SUCCESSOR AGENCY TRUST FOR ASSETS OF THE FORMER REDVELOPMENT AGENCY,
Continued

E. Long-Term Liabilities, Continued

Pollution Remediation

The Trust owns property designated by the Santa Barbara County Public Health Department as a LUFT (Leaking Underground Fuel Tank) site (#52010). The property cleanup project has been accepted into the State Water Resources Cleanup of Underground Storage Tanks Fund (USTCF), which approved a total Letter of Commitment (LOC) in the amount of \$1.5 Million. These funds are available for reimbursement of most of the costs associated with assessment and cleanup of the contamination under the site, associated with a former gasoline storage tank leak.

Between the fiscal years 2008/2009 through June 30, 2019, the former Agency expended a total of \$890,184 toward the cleanup costs. Cleanup costs incurred and paid for the 2018/19 fiscal year, but which the City had not yet been reimbursed for by the State as of June 30, 2019, totaled \$175,052. These costs are anticipated to take as long as until November 2019 to be reviewed for payment. Some of these costs (approximately \$25,378) were contested by the State and re-petitioned. Re-petitioned costs can take several years to be reviewed and decided on.

Tasks in 2018/19 included: 1) providing electronic technical assistance services (ETAC) required by the State for submitting reimbursement request #12; 2) evaluation, preparation and submittal of a Project Execution Plan (PEP) update and Budget Change Order Request for future site corrective action activities anticipated, as required by the State; 3) final system construction, final permitting, project management, system startup, and initial system operations and maintenance (O&M) activities related to approved remedial actions [soil vapor extraction (SVE)]; 4) providing ETAC services required for submitting reimbursement request #13; 5) on-going remediation system repairs, reporting, permitting, project management, system restart, and system operations and maintenance (O&M) activities related to approved remedial actions (SVE)]; 6) assistance with waste management, profiling and removal activities; and, 7) ETAC services required for submitting reimbursement request #14.

In January 2017, the LOC directed that soil vapor extraction (SVE) activities be employed at the site for a period of approximately 12 months. Between January 10, 2017 and June 30, 2018, DMI-EMK initiated these SVE activities, coordinating the field activities and obtaining the associated permits required before field activities can be implemented. While field work was anticipated to commence by September 2017 and finish around September 2018, due to difficulties with the utility companies (gas and electric), obtaining final permit approvals, and significant electrical issues at the site, the system is currently anticipated to run through March or April of 2020.

DMI-EMK estimates that, once closure is granted by the County, it will take approximately 6 more months before a final closure letter can be obtained for the site. As such, it is anticipated that the soonest a final closure letter can be obtained for this site is approximately November-December 2020.

Estimated future costs beyond June 30, 2019 are anticipated to be approximately \$300,000 to \$400,000 through obtaining site closure - assuming the site is found to meet the low-threat closure criteria after 12 months of active remediation. Based on the above, the total current estimated costs for cleanup activities is approximately \$1,200,000-\$1,300,000, well below the \$1.5 Million budget allotted this site by the State.

City of Guadalupe
Notes to Basic Financial Statements
For the year ended June 30, 2019

11. SUCCESSOR AGENCY TRUST FOR ASSETS OF THE FORMER REDVELOPMENT AGENCY, Continued

F. Prior Period Adjustment

The City recorded a prior period adjustment to correct an error in accounting for interest payable and interest expense in the fiscal year ended June 30, 2018 in the Successor Agency Trust Fund.

Net position as previously reported at June 30, 2018:	\$ (3,724,373)
Overstatement of interest payable:	81,693
Net position as restated at June 30, 2018:	<u>\$ (3,642,680)</u>

12. OPERATING LEASES

The City leases equipment under operating leases with lease terms in excess of one year. The agreements contain a termination clause providing for cancellation after a specified number of days written notice to lessors but it is unlikely that the City will cancel the agreements prior to the expiration date. Rent expense under operating leases was \$11,334 for the year ended June 30, 2019.

At June 30, 2019, future minimum lease payments under these operating leases were as follows:

<u>For the Year</u> <u>Ending June 30,</u>	<u>Payment</u>
2020	\$ 12,006
2021	12,006
2022	7,084
2023	6,100
2024	<u>6,100</u>
Total	<u>\$ 43,296</u>

13. DEFICIT FUND BALANCES/NET POSITION

Major Funds

A deficit net position of \$9,273 exists for the Solid Waste Fund. Over the years, the difference was due to the City not always increasing customer rates to cover increases by the waste hauler, discrepancies between the waste hauler's customer data base and the City's customer data base and prior year loans to cover negative balances in the Solid Waste Fund.

City of Guadalupe
Notes to Basic Financial Statements
For the year ended June 30, 2019

14. GOING CONCERN

The City continues to have more expenditures than revenues in its General Fund. Transfers from other funds based on cost allocation analysis is creating a positive net change in fund balance. In order to continue operations, in prior years the General Fund borrowed from other funds. These borrowings still need to be repaid. There are doubts about the General Fund's ability to continue to repay these interfund loans in their entirety if economic activity declines. Below is how management intends to address those issues:

The City is experiencing an increase in business licenses and building permits from the Pasadera residential development. New business activity results in a positive economic boost to the General Fund.

The General Fund's priority is to eliminate future borrowing from other funds, payoff current inter-fund loans and be economically self-sufficient. Inter-fund loan payment schedules will be reviewed annually and, if possible, revised in an effort to decrease balances at a faster rate.

The 2019-20 month-end cash balances have been positive. Staff will submit a monthly cash balance report to Council to ensure pooled cash does not result in usage of other funds' cash by the General Fund. If a negative balance exists in the General Fund, the Council and staff will review and apply available methods to reverse the deficit within one month.

15. SUBSEQUENT EVENTS

On March 19th, 2020, the governor of California (State) issued an Executive Order (Order) effective immediately for all individuals living in the State to stay home or at their place of residence. The State identified sixteen critical infrastructure sectors that were exempt from the Order. Among the sectors deemed essential were government facilities, and water and wastewater systems.

This subsequent event had a ripple-effect through state-wide and local economies where nonessential businesses suspended operations. The employees of these businesses were furloughed or laid-off. Revenues such as gas taxes, sales taxes and building permits are expected to be dramatically less than prior years. City Staff will continue to monitor revenues closely and is working with FEMA to obtain reimbursement for costs related to the pandemic.

This page intentionally left blank.

**REQUIRED
SUPPLEMENTARY INFORMATION**

City of Guadalupe
Required Supplementary Information
For the year ended June 30, 2019

1. BUDGETS AND BUDGETARY ACCOUNTING

A. Budgetary Control and Budgetary Accounting

Annual budgets are adopted on a basis consistent with accounting principles generally accepted in the United States of America for all governmental funds. After adoption of the final budget, transfers of appropriations within a General Fund department, or within other funds, can be made by the City Administrator. Budget modifications between funds and increases or decreases to a fund's overall budget, must be approved by the City Council. No amendments were made during the fiscal year.

Budgetary control is enhanced by integrating the budget into the general ledger accounts. Encumbrance accounting is employed (e.g., purchase orders) to avoid expenditures over budget. Encumbrances outstanding at fiscal year-end are automatically re-budgeted in the following fiscal year.

The following are the budget comparison schedules for all major Governmental Funds.

City of Guadalupe
Budgetary Comparison Schedule - General Fund
For the year ended June 30, 2019

	Budgeted Amounts		Actual Amounts	Variance with Final Budget Positive (Negative)
	Original	Final		
REVENUES:				
Taxes	\$ 2,091,000	\$ 2,091,000	\$ 2,349,261	\$ 258,261
Licenses and permits	783,520	783,520	736,416	(47,104)
Fines and penalties	21,800	21,800	25,101	3,301
Revenues from other agencies	382,122	382,122	343,729	(38,393)
Charges for current services	101,650	101,650	87,086	(14,564)
Interest	109,700	109,700	123,127	13,427
Other revenues	152,979	152,979	209,903	56,924
Total revenues	3,642,771	3,642,771	3,874,623	231,852
EXPENDITURES:				
Current:				
General Government	1,198,835	1,110,293	1,026,400	83,893
Public Safety	2,348,287	2,348,287	2,275,212	73,075
Leisure, cultural and social services	154,239	148,739	165,310	(16,571)
Community development	411,898	386,898	393,225	(6,327)
Capital outlay	37,200	37,200	68,238	(31,038)
Debt service:				
Principal	51,830	51,830	50,057	1,773
Interest and fiscal charges	16,128	16,128	16,612	(484)
Total expenditures	4,218,417	4,099,375	3,995,054	104,321
REVENUES OVER (UNDER) EXPENDITURES	(575,646)	(456,604)	(120,431)	336,173
OTHER FINANCING SOURCES (USES):				
Transfers in	451,000	461,600	366,360	(95,240)
Transfers out	-	(62,732)	(62,732)	-
Total other financing sources (uses)	451,000	398,868	303,628	(95,240)
Net change in fund balances	(124,646)	(57,736)	183,197	240,933
FUND BALANCES:				
Beginning of year	(167,872)	(167,872)	(167,872)	-
End of year	\$ (292,518)	\$ (225,608)	\$ 15,325	\$ 240,933

City of Guadalupe
Budgetary Comparison Schedule - Measure A Fund
For the year ended June 30, 2019

	Budgeted Amounts		Actual Amounts	Variance with Final Budget Positive (Negative)
	Original	Final		
REVENUES:				
Taxes	\$ 457,000	\$ 457,500	\$ 508,780	\$ 51,280
Interest	6,500	6,500	19,951	13,451
Total revenues	463,500	464,000	528,731	64,731
EXPENDITURES:				
Current:				
Transportation	786,307	786,307	845,416	(59,109)
Total expenditures	786,307	786,307	845,416	(59,109)
REVENUES OVER (UNDER) EXPENDITURES	(322,807)	(322,307)	(316,685)	5,622
OTHER FINANCING SOURCES (USES):				
Transfers out	(76,400)	(54,069)	-	54,069
Total other financing sources (uses)	(76,400)	(54,069)	-	54,069
Net change in fund balances	(399,207)	(376,376)	(316,685)	59,691
FUND BALANCES:				
Beginning of year	1,210,262	1,210,262	1,210,262	-
End of year	\$ 811,055	\$ 833,886	\$ 893,577	\$ 59,691

City of Guadalupe
Budgetary Comparison Schedule - Park Development Fund
For the year ended June 30, 2019

	Budgeted Amounts		Actual Amounts	Variance with Final Budget Positive (Negative)
	Original	Final		
REVENUES:				
Charges for current services	\$ 500	\$ 500	\$ 703,622	\$ 703,122
Interest	15	15	156	141
Total revenues	515	515	703,778	703,263
REVENUES OVER (UNDER) EXPENDITURES	515	515	703,778	703,263
Net change in fund balances	515	515	703,778	703,263
FUND BALANCES:				
Beginning of year	2,657	2,657	2,657	-
End of year	\$ 3,172	\$ 3,172	\$ 706,435	\$ 703,263

City of Guadalupe
Required Supplementary Information
For the year ended June 30, 2019

2. DEFINED BENEFIT PENSION PLANS

A. Schedule of the City's Proportionate Share of the Net Pension Liability - Last 10 Years*

Fiscal year	2019	2018	2017	2016	2015
Measurement date	6/30/2018	6/30/2017	6/30/2016	6/30/2015	6/30/2014
Proportion of the net pension liability	3.16600%	0.03091%	0.02989%	0.02666%	0.0312%
Proportionate share of the net pension liability	\$3,050,995	\$3,065,323	\$2,586,229	\$1,830,129	\$1,939,137
Covered payroll	\$2,153,332	\$1,925,534	\$1,572,208	\$1,479,094	\$1,548,925
Proportionate Share of the net pension liability as percentage of covered payroll	141.69%	159.19%	164.50%	123.73%	125.19%
Plan fiduciary net position as a percentage of the total pension liability	73.31%	73.31%	74.06%	78.40%	79.82%

* Historical information is required only for measurement period for which GASB 68 is applicable

B. Schedule of Plan Contributions - Last 10 Years*

Fiscal Year	2019	2018	2017	2016	2015
Contractually required contribution (actuarially determined)	\$ 363,003	\$ 329,839	\$ 305,064	\$ 251,172	\$ 211,025
Contribution in relation to the actuarially determined contributions	(363,003)	(329,839)	(305,064)	(251,172)	(211,025)
Contribution deficiency (excess)	\$ -	\$ -	\$ -	\$ -	\$ -
Covered payroll	\$2,025,580	\$2,153,332	\$1,925,534	\$1,572,208	\$1,479,094
Contributions as a percentage of covered payroll	17.92%	15.32%	15.84%	15.98%	14.27%

* Historical information is required only for measurement periods for which GASB 68 is applicable

City of Guadalupe
Required Supplementary Information
For the year ended June 30, 2019

3. OTHER POST EMPLOYMENT BENEFITS (OPEB)

Schedule of Changes in Total OPEB Liability and Related Ratios

<i>Measurement Period</i>	2019	2018¹
Total OPEB Liability		
Service Cost	\$ 22,620	\$ 22,060
Interest	11,639	11,646
Changes of benefit terms	-	-
Difference between expected and actual experience	72,513	-
Changes of assumptions	31,372	-
Benefit payments	(4,842)	(206,667)
Net change in total OPEB liability	133,302	(172,961)
Total OPEB liability - beginning (a)	251,163	424,124
Total OPEB liability - ending (b)	<u>\$ 384,465</u>	<u>\$ 251,163</u>
Covered-employee payroll	\$ 2,525,683	\$ 2,267,277
Total OPEB liability as a percentage of covered-employee payroll	15.2%	11.1%

¹Amount includes implicit subsidy associated with benefits paid for this year.

This page intentionally left blank.

SUPPLEMENTARY INFORMATION

City of Guadalupe
Combining Balance Sheet
Other Governmental Funds
June 30, 2019

	Special Revenue				
	Local Transportation	Library	Public Facilities	Guadalupe Lighting and Assessment	Public Safety
ASSETS					
Cash and investments	\$ 150,374	\$ 10,110	\$ 11,449	\$ 302,311	\$ 95,968
Accounts receivable	15,270	74	67	1,267	29,181
Prepaid items	-	4,000	-	-	-
Interfund loans receivable	-	-	-	320,000	-
Loans receivable	-	-	-	-	-
Total assets	\$ 165,644	\$ 14,184	\$ 11,516	\$ 623,578	\$ 125,149
LIABILITIES AND FUND BALANCES					
Liabilities:					
Accounts payable	-	-	-	5,611	-
Cash overdraft	-	-	-	-	-
Accrued wages and benefits	-	-	-	-	1,929
Interfund loans payable	-	68,333	-	-	-
Total liabilities	-	68,333	-	5,611	1,929
Deferred inflows of resources:					
Unavailable revenue	-	-	-	-	9,695
Total deferred inflows of resources	-	-	-	-	9,695
Fund Balances:					
Nonspendable:					
Prepaid items	-	4,000	-	-	-
Restricted for:					
Street maintenance	165,644	-	-	-	-
Other capital projects	-	-	-	-	-
Community development	-	-	-	-	-
Public safety	-	-	-	-	113,525
Utility infrastructure	-	-	11,516	-	-
Debt service	-	-	-	-	-
Lighting and landscape	-	-	-	617,967	-
Assigned to:					
Capital projects	-	-	-	-	-
Unassigned	-	(58,149)	-	-	-
Total fund balances	165,644	(54,149)	11,516	617,967	113,525
Total liabilities and fund balances	\$ 165,644	\$ 14,184	\$ 11,516	\$ 623,578	\$ 125,149

Special Revenue			Capital Projects			Total Other
Community Development	Transportation Grant	Gas Tax	City Hall	Traffic Mitigation	Sewer Bond Debt Service	Governmental Funds
\$ 83,239	\$ -	\$ 139,711	\$ 13,899	\$ 71,382	\$ 29,297	907,740
578	-	779	81	366	247	47,910
-	-	-	-	-	-	4,000
-	-	-	-	-	-	320,000
13,173	-	-	-	-	-	13,173
\$ 96,990	\$ -	\$ 140,490	\$ 13,980	\$ 71,748	\$ 29,544	\$ 1,292,823
18,322	53,197	7,835	-	-	-	84,965
-	18,780	-	-	-	-	18,780
-	-	-	-	-	-	1,929
-	-	-	-	-	-	68,333
18,322	71,977	7,835	-	-	-	174,007
-	-	-	-	-	-	9,695
-	-	-	-	-	-	9,695
-	-	-	-	-	-	4,000
-	-	132,655	-	-	-	298,299
-	-	-	13,980	-	-	13,980
78,668	-	-	-	-	-	78,668
-	-	-	-	-	-	113,525
-	-	-	-	-	-	11,516
-	-	-	-	-	29,544	29,544
-	-	-	-	-	-	617,967
-	-	-	-	71,748	-	71,748
-	(71,977)	-	-	-	-	(130,126)
78,668	(71,977)	132,655	13,980	71,748	29,544	1,109,121
\$ 96,990	\$ -	\$ 140,490	\$ 13,980	\$ 71,748	\$ 29,544	\$ 1,292,823

City of Guadalupe
Combining Statement of Revenues, Expenditures and Changes in Fund Balances
Other Governmental Funds
For the year ended June 30, 2019

	Special Revenue				
	Local Transportation	Library	Public Facilities	Guadalupe Lighting and Assessment	Public Safety
REVENUES:					
Taxes	\$ -	\$ -	\$ -	\$ 215,504	\$ -
Licenses and permits	-	7,799	-	-	-
Revenues from other agencies	143,130	-	-	-	190,226
Charges for current services	-	-	5,547	-	-
Interest	4,087	231	192	10,697	2,841
Other revenues	-	4,000	-	-	8,408
Total revenues	147,217	12,030	5,739	226,201	201,475
EXPENDITURES:					
Current:					
Public Safety	-	-	-	-	233,435
Transportation	185,675	-	-	-	-
Leisure, cultural and social services	-	7,408	-	-	-
Community development	-	-	-	71,721	-
Capital outlay	-	-	-	-	11,555
Debt service:					
Principal	-	-	-	-	-
Interest and fiscal charges	-	-	-	-	-
Total expenditures	185,675	7,408	-	71,721	244,990
REVENUES OVER (UNDER) EXPENDITURES	(38,458)	4,622	5,739	154,480	(43,515)
OTHER FINANCING SOURCES (USES):					
Transfers in	-	-	-	-	-
Transfers out	-	-	-	(14,988)	-
Total other financing sources (uses)	-	-	-	(14,988)	-
Net change in fund balances	(38,458)	4,622	5,739	139,492	(43,515)
FUND BALANCES:					
Beginning of year	204,102	(58,771)	5,777	478,475	157,040
End of year	\$ 165,644	\$ (54,149)	\$ 11,516	\$ 617,967	\$ 113,525

Special Revenue			Capital Projects			Total Other
Community Development	Transportation Grant	Gas Tax	City Hall	Traffic Mitigation	Sewer Bond Debt Service	Governmental Funds
\$ -	\$ -	\$ 148,079	\$ -	\$ -	\$ 18,364	\$ 381,947
-	-	-	3,121	20,783	-	31,703
-	18,149	106,261	-	-	-	457,766
-	-	-	-	-	-	5,547
3,051	-	1,647	294	1,201	754	24,995
-	-	-	-	-	-	12,408
<u>3,051</u>	<u>18,149</u>	<u>255,987</u>	<u>3,415</u>	<u>21,984</u>	<u>19,118</u>	<u>914,366</u>
-	-	-	-	-	-	233,435
-	90,126	262,291	-	-	-	538,092
94,184	-	-	-	-	-	101,592
-	-	-	-	-	-	71,721
-	-	-	-	-	-	11,555
-	-	20,808	-	-	16,000	36,808
-	-	-	-	-	800	800
<u>94,184</u>	<u>90,126</u>	<u>283,099</u>	<u>-</u>	<u>-</u>	<u>16,800</u>	<u>994,003</u>
<u>(91,133)</u>	<u>(71,977)</u>	<u>(27,112)</u>	<u>3,415</u>	<u>21,984</u>	<u>2,318</u>	<u>(79,637)</u>
-	-	62,732	-	-	-	62,732
(492)	-	-	-	-	-	(15,480)
<u>(492)</u>	<u>-</u>	<u>62,732</u>	<u>-</u>	<u>-</u>	<u>-</u>	<u>47,252</u>
<u>(91,625)</u>	<u>(71,977)</u>	<u>35,620</u>	<u>3,415</u>	<u>21,984</u>	<u>2,318</u>	<u>(32,385)</u>
170,293	-	97,035	10,565	49,764	27,226	1,141,506
<u>\$ 78,668</u>	<u>\$ (71,977)</u>	<u>\$ 132,655</u>	<u>\$ 13,980</u>	<u>\$ 71,748</u>	<u>\$ 29,544</u>	<u>\$ 1,109,121</u>

City of Guadalupe
Budgetary Comparison Schedule - Capital Facilities Fund
For the year ended June 30, 2019

	Budgeted Amounts		Actual Amounts	Variance with Final Budget Positive (Negative)
	Original	Final		
REVENUES:				
Licenses and permits	\$ 281,250	\$ 281,250	\$ 804,342	\$ 523,092
Interest	2,400	2,400	16,936	14,536
Total revenues	283,650	283,650	821,278	537,628
REVENUES OVER (UNDER) EXPENDITURES	283,650	283,650	821,278	537,628
Net change in fund balances	283,650	283,650	821,278	537,628
FUND BALANCES:				
Beginning of year	312,520	312,520	312,520	
End of year	\$ 596,170	\$ 596,170	\$ 1,133,798	\$ 537,628

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS BASED ON AN AUDIT OF FINANCIAL STATEMENTS PERFORMED IN ACCORDANCE WITH GOVERNMENT AUDITING STANDARDS

To the Honorable Mayor and Members of the City Council
of the City of Guadalupe
Guadalupe, California

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, the financial statements of the governmental activities, the business-type activities, each major fund, and the aggregate remaining fund information of the City of Guadalupe, California (City), as of and for the year ended June 30, 2019, and the related notes to the financial statements, which collectively comprise the City's basic financial statements and have issued our report thereon dated April 28, 2020.

Internal Control over Financial Reporting

In planning and performing our audit of the financial statements, we considered the City's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the City's internal control. Accordingly, we do not express an opinion on the effectiveness of the City's internal control.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. However, as described in the accompanying schedule of findings and responses, we identified certain deficiencies in internal control that we consider to be material weaknesses and significant deficiencies.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A *material weakness* is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. We consider the deficiency described as item 2019-001 in the accompanying schedule of findings and responses to be a material weakness.

A *significant deficiency* is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the deficiencies described as items 2019-002 to 2019-005 in the accompanying schedule of findings and responses to be significant deficiencies.

To the Honorable Mayor and Members of the City Council
of the City of Guadalupe
Guadalupe, California
Page 2

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the City's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

City's Response to Findings

The City's response to the findings identified in our audit is described in the accompanying schedule of findings and questioned costs. The City's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.



Badawi & Associates, CPAs
Berkeley, California
April 28, 2020

City of Guadalupe
Schedule of Findings and Responses
For the year ended June 30, 2019

FINDINGS - FINANCIAL STATEMENTS AUDIT

2019-001 - Insufficient Fund Balance in the General Fund and the Ability of the City to Continue As a Going Concern (Material Weakness)

Criteria:

General purpose local governments, regardless of size, at a minimum should maintain a fund balance in the general fund of either 1) no less than 5 to 15 percent of regular general fund operating revenues, or 2) no less than 1 to 2 months of regular general fund operating expenditures.

Condition:

The General Fund did not maintain a sufficient or adequate fund balance level to ensure continuity of operations as of June 30, 2019. The General Fund finished the year with a balance of \$15,325 compared to a negative fund balance of \$(167,872) in the prior fiscal year. This balance represents 0.4% of operating revenues and 1 day of operating expenditures. The fund balance in spendable form is \$549. As of June 30, 2019 the General Fund owed internally to the Lighting and Assessment Fund and the Water Fund the amounts of \$320,000 and \$491,998, respectively. These interfund loans were made so that the General Fund could sustain its basic operations.

The aforementioned conditions have raised doubt about the City's ability to continue as a going concern, as described further in Note 14.

Cause:

The City has either overspent its budget in the past or the budget was not balanced which led to overspending and the insufficient fund balance situation.

Effect:

Insufficient fund balances and decrease in revenues in the past have created a budget shortfall that requires continued cost cutting measures to reach a budget that will increase the fund balance to an acceptable level as well as provide the necessary revenues and financing for continued operations of the City. In addition, an insufficient General Fund balance puts the City in a vulnerable position in times of economic stress.

Recommendation:

We recommend the City continue to analyze all potential cost cutting measures and revenue sources, and review options to adhere to a budget plan for the General Fund and other funds to increase the fund balance, as well as provide continued financing for City operations.

Management Response:

The City has a positive fund balance currently as of March 2020. The City's goal is to maintain a positive fund balance and the preservation of future reserves. The City adopted Financial Policies with its 2019-2021 Budget that target the establishment of reserve funds at optimum levels. However, the City of Guadalupe declared a local state of Emergency in March 2020 due to the COVID19 pandemic. Although the pandemic brings much uncertainty, the City expects sales tax revenue to be negatively impacted, along with business licenses, property tax and local streets and roads funding. City staff will

City of Guadalupe
Schedule of Findings and Responses
For the year ended June 30, 2019

monitor the financial situation and impact of the pandemic on a monthly basis for the remainder of fiscal year 2020 and into fiscal year 2021. Amid the pandemic, building Permit and related construction fee revenues have aid the City's cash flow as the Pasadera development continues construction. The City is also working with FEMA to obtain reimbursement for COVID19 related expenses. The City is looking to sustain recurring revenue streams for the future including a new sales tax measure in 2020 and continuation of increase of water and wastewater rates. In addition, Users Tax, Franchise Fees and Property taxes are expected to rise over time as a positive long-term outcome of the new Pasadera development.

2019-002 - Recordkeeping of Capital Assets (Significant Deficiency)

Criteria:

A good internal control system over capital assets requires that the City maintain detailed records of all its capital assets to be able to support amounts reported on the financial statements and to ensure the safeguarding of assets and timely payment on long-term debt.

Condition:

We noted during the audit that the City did not maintain adequate records for capital assets to enable it to exercise control over that activity. Instead, the City is relying on a loosely maintained spreadsheets that were originally developed by the previous audit firm used by the City. The spreadsheets contained multiple depreciation errors, assets that weren't accounted for, and unclear fund assignments.

Cause:

The City did not keep accurate and complete records of its capital assets.

Effect:

Capital assets may be misstated and/or not properly or timely accounted for.

Recommendation:

We recommend that the City implement a tracking system and to conduct an inventory of its capital assets.

Management Response:

The City approved a new financial accounting software system to be implemented starting in fiscal year 2020. As part of this system, a fixed asset module will be included, which will integrate seamlessly into the general ledger module. The goal will be to include all assets of the City by cost, category, governmental unit and other detailed identification. Tracking of acquisitions and disposals of assets will become more efficient and accurate.

2019-003 - Control Over Expenditures and Accounts Payable (Significant Deficiency)

Criteria:

A good internal control system over expenditures and accounts payable requires that certain tasks such as creating new vendors, correctly coding, inputting invoices, and processing checks be segregated and

City of Guadalupe
Schedule of Findings and Responses
For the year ended June 30, 2019

not performed by the same individual. In addition, changes to the master file should be reviewed and reconciled by a qualified individual independent from the accounts payable process.

Condition:

During our audit we noted that the Accounts Payable Clerk is responsible for setting up new vendors in the system. There is no independent review of changes made to the vendor master files. In addition, we noted that the reviewer of the accounts payable does not keep track of the sequence numbers of the checks reviewed. We also noted in our testing procedures, some invoices were missing, and some did not have explicit approval signatures. Lastly, expenditures were sometimes coded to incorrect accounts, funds, and fiscal year. Some of these mistakes were caught and fixed later, but not all.

Cause:

Duties in the accounts payable system are not properly segregated to ensure that good checks and balances are in place.

Effect:

Errors in accounts payable may not be detected timely. In addition, unauthorized payments to vendors or payments to unauthorized vendors may not be detected timely.

Recommendation:

We recommend that the City improve and strengthen its procedures for review and reconciliation to ensure that changes to the vendor master files are properly reviewed and reconciled by an independent person and there is adequate segregation of duties in place.

Management Response:

Accounts Payable Clerk sets up new vendor and the Finance Director reviews the entry and signs off. Only department heads and management code invoices. Business Manager checks the entry of invoices before processing checks. Accounts Payable Clerk also keeps track of all voided checks and sequence of check numbers. City Staff is hopeful that the new accounting software will accommodate workflow and authorization parameters to improve our controls and segregation of duties.

2019-004 - Control Over Payroll and Related Liabilities (Significant Deficiency)

Criteria:

A good internal control system over payroll requires that certain tasks such as creating new employees, inputting pay rates, and processing payroll be segregated and not performed by the same individual. In addition, payroll should be reviewed and reconciled by a qualified individual independent from the payroll process.

Condition:

During our audit we noted that there was one person who was responsible for setting up new employees, making and updating all changes in the payroll system as well as processing payroll. Additionally, we noted that after November 2018 there was no review of the bi-weekly payroll.

City of Guadalupe
Schedule of Findings and Responses
For the year ended June 30, 2019

Cause:

Duties in the payroll system are not properly segregated to ensure that good checks and balances are in place.

Effect:

Payroll amounts may be misstated due to errors not detected during the review process. In addition, incorrect or unauthorized pay rates may be used and not detected timely.

Recommendation:

We recommend that the City improve and strengthen its procedures for review and reconciliation to ensure that payroll is properly reviewed and reconciled by an independent person and there is adequate segregation of duties in place.

Management Response:

Finance Director currently reviews the processing of payroll and the payroll bank account reconciliation. City Staff is hopeful that the new accounting software will accommodate workflow and authorization parameters to improve our controls and segregation of duties.

2019-005 - Control Over Journal Entries and Financial Reporting (Significant Deficiency)

Criteria:

A good internal control system over financial reporting requires that certain tasks such as creating journal entries and reviewing journal entries be segregated and not performed by the same individual.

Condition:

During our audit we noted that there was mainly one person who was responsible for creating journal entries with no independent review of those entries by an independent person. We also noted multiple journal entry errors that were both corrected and uncorrected.

Cause:

Duties in the financial reporting system are not properly segregated to ensure good checks and balances are in place.

Effect:

Journal entries amounts may be misstated due to errors not detected during the review process. In addition, unauthorized entries may be posted and not detected timely.

Recommendation:

We recommend that the City improve and strengthen its procedures for review and reconciliation to ensure that journal entries are properly reviewed and reconciled by an independent person and there is adequate segregation of duties in place.

Management Response:

Finance Director proposes journal entries and Business Manager reviews and enters the journal entries. The City will review and set up controls to ensure approval controls of journal entries takes place for

City of Guadalupe
Schedule of Findings and Responses
For the year ended June 30, 2019

all changes to the accounting records. City Staff is hopeful that the new accounting software will accommodate workflow and authorization parameters to improve our controls and segregation of duties.



**REPORT TO THE CITY COUNCIL OF THE CITY OF GUADALUPE
Agenda of May 26, 2020**

Prepared by:
Todd Bodem, City Administrator

SUBJECT: City's response to a Santa Barbara Grand Jury Report entitled "Cyber-Attacks Threaten Santa Barbara County"

RECOMMENDATION:

1. That the City Council review staff's recommendations for the City's response to the Santa Barbara County Grand Jury Report entitled "Cyber-Attacks Threaten Santa Barbara County" and make any changes the Council believes are necessary; and
2. That the City Council adopt Resolution No. 2020-39 approving the attached final response (with any changes made by the Council) to the Santa Barbara County Grand Jury Report entitled "Cyber-Attacks Threaten Santa Barbara County" with the signatures of each member of the City Council to Judge Michael J. Carrozzo and the Santa Barbara Grand Jury.

EXECUTIVE SUMMARY:

The Santa Barbara County Civil Grand Jury issued a report that requires a response from the City of Guadalupe. The report is titled "Cyber-Attacks Threaten Santa Barbara County," which was issued on March 18, 2020. This report is concerns nine (9) jurisdictions within Santa Barbara County including the City of Guadalupe.

Staff has prepared draft responses for the City Council's review and consideration. If the Council believes any changes are required to these draft responses, staff will make these corrections pursuant to Council's direction. Thereafter, Council should adopt a resolution to approve the final report.

BACKGROUND:

On March 18, 2020, the City received a report from the Santa Barbara County Grand Jury entitled "Cyber-Attacks Threaten Santa Barbara County." This Grand Jury report is concerned with eight (8) incorporated cities including Guadalupe and the County of Santa Barbara for a total of nine (9) jurisdictions.

This report ("Cyber-Attacks Threaten Santa Barbara") has eight (8) findings and twelve (12) recommendations. The City is required to respond to all of the finding and recommendations in this report.

California Penal Code section 933(c) provides that: "[n]o later than 90 days after the grand jury submits a final report on the operations of any public agency subject to its reviewing authority, the governing body of the public agency shall comment to the presiding judge of the superior court on the findings and recommendations pertaining to matters under the control of the governing body,..." Accordingly, the City has until June 18, 2020, to respond to the report entitled "Cyber-Attacks Threaten Santa Barbara County."

DISCUSSION:

"Cyber-Security Attacks Threaten Santa Barbara County" The 2019-20 Santa Barbara County Grand Jury determined that cyber-attacks and related threats are an ongoing reality and that all public entities within Santa Barbara County need to take prompt and aggressive steps to prevent significant disruption from these attacks. The Grand Jury noted that when cyber-attacks are successful, the costs to respond and recover can be extremely costly for any agency. The Grand Jury also noted that while some local public entities are taking steps to protect themselves from these risks, many are not adequately prepared. The City of Guadalupe recognizes the need to take proactive steps both by policy and during the budgeting process to upgrade its systems to prevent future cyber-attacks.

In total, the Grand Jury report sets forth eight (8) findings and twelve (12) recommendations. The City of Guadalupe is required to respond to Finding Nos. 1, 2, 3, 4, 5, 6, 7, and 8 and recommendations 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b,7, 8.

The City's response includes agreement with all of the Grand Jury's findings, and with respect to the recommendations, the City has actually been actively aware of cyber-security threats and already taken action to implement most of the recommendations by the Grand Jury.

FISCAL IMPACT:

Cost of new computers (cost TBD), cost of change in IT consultant, other alternatives to mitigate risks and time spent on establishment of policies.

CONCLUSION:

Staff recommends that the City Council adopt Resolution No. 2020-39 (Attachment 3) and after it reviews the draft responses prepared by staff to the Grand Jury report and make any changes it determines to be necessary, if any.

ATTACHMENTS:

1. Grand Jury Report entitled "Cyber-Attacks Threaten Santa Barbara County" dated March 18, 2020

2. City's draft response to Grand Jury Report entitled "Cyber-Attacks Threaten Santa Barbara County."
3. Resolution No. 2020-39 "A Resolution of the City Council of the City of Guadalupe adopting a response to the Santa Barbara County Grand Jury Report entitled "Cyber-Attacks Threaten Santa Barbara County."

COUNTY COURTHOUSE
1100 ANACAPA STREET
SANTA BARBARA, CA 93101



(805) 568-2291
SBCGRANDJURY@SBCGJ.ORG
HTTP://WWW.SBCGJ.ORG

**GRAND JURY
SANTA BARBARA COUNTY**

March 2020

Mr. Todd Bodem
Guadalupe City Administrator
918 Obispo Street
Guadalupe, CA 93434

Dear Mr. Bodem,

On behalf of the 2019-20 Santa Barbara County Grand Jury, the report titled:
Cyber-Attacks Threaten Santa Barbara County
is enclosed for your review and response.

The Grand Jury, County Counsel and Presiding Judge have approved this report. *California Penal Code 933.05* requires the following:

- You are receiving this report two working days prior to its release to the public, and you shall not disclose this report prior to its public release.
- You must respond to each relevant Finding and Recommendation in this report where listed and required.
- You must submit your response to the Grand Jury and Presiding Judge.
- If you are an elected county official or agency head, the response time is no later than 60 days from the date of receipt of this report.
- If you are the governing body subject to the reviewing authority of the Grand Jury, the response time is no later than 90 days of receipt of this report.

Responses to the Findings shall be either:

- Agree
- Disagree wholly
- Disagree partially with an explanation

Responses to Recommendations shall be one of the following:

- Has been implemented, with a brief summary of implementation actions taken.
- Will be implemented, with an implementation schedule.
- Requires further analysis, with timeframe that shall not exceed six months from the publication of the report.
- Will not be implemented, with an explanation.

Your response will be posted of the Santa Barbara County Grand Jury website www.sbcgj.org.

Please provide a digital copy of your response to:
Santa Barbara County Grand Jury
sbcgrandjury@sbcgj.org

DocuSigned by:
Todd Bodem
EF07F3E1AE43472...

Also, a copy of your response must be sent to:
The Honorable Judge Michael J. Carozzo
1100 Anacapa Street
Santa Barbara, CA, 93101

This report will be released to the public not less than two working days following the date of delivery. Again, this report is confidential until public release. If you have any questions, please contact me at the address below.

Respectfully yours,

Pamela Olsen

Pamela Olsen
Foreperson
2019-20 Santa Barbara County Grand Jury
Santa Barbara Courthouse
1100 Anacapa Street
Santa Barbara, CA 93101

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

SUMMARY

Nationwide, a cyber-attack occurs at least every 39 seconds. Globally, the cost of cyber-attacks is expected to be \$6 trillion by 2021¹. The 2019-20 Santa Barbara County Grand Jury through its research learned the County of Santa Barbara, the eight incorporated cities, and the special districts within the County, as a whole, are woefully ill-prepared for a cyber-attack. Such an attack could cripple their services and data systems. The cost to repair and recover these systems could be millions of dollars!² Cyber security attacks include corruption or theft of data, denial of service, or complete destruction of critical data. Also, attacks could include subverting critical operations, such as water systems, electrical grids, and communication systems, and thus threaten public safety.

Cyber-attacks are more widespread and dangerous than is generally recognized, even by people who should know. The attacks are certain to get worse. There is a never-ending evolutionary race between attack and defense. In this digital world, local government entities, even small ones, are not immune and their risks will grow as automated attack methods increase.

INTRODUCTION

According to a recent survey of national business leaders, cyber security risks are the top concern among businesses of all sizes, ahead of medical cost inflation, employee benefit costs, the ability to attract and retain talent, and legal liability.³ Fewer than half of all Chief Information Security Officers and senior executives are confident their organizations are fully prepared to deal with cyber-attacks, according to a study conducted by a well-known cyber security consultancy.⁴

Whether the cyber-attack is motivated by money, revenge, mischief or geo-politics, the costs to respond and recover can be astronomical. These attacks can be in the form of:

- **Data theft**, the unauthorized taking or interception of computer-based information.
- **Ransomware**, a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

¹ Herjavec Group: The 2019 Official Annual Cybercrime Report. <https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report> (Last visited 02/03/2020)

² "Texas Ransomware attack to cost \$12 million and more", *Cybersecurity Insiders*, <https://www.cybersecurity-insiders.com/texas-ransomware-attack-to-cost-12-million-and-more/> (Last visited 02/03/2020)

³ "2018 Travelers Risk Index: Cyber [Infographic]", *Travelers*, 2018 <https://www.travelers.com/resources/risk-index/2018-cyber-infographic> (Last visited 03/12/2020)

⁴ "Cyber Tops All Other Risk Concerns for Businesses of All Sizes", *Insurance Journal*, October 1, 2019 <https://www.insurancejournal.com/news/national/2019/10/01/541645.htm> (Last visited 02/03/2020)

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

- **Sabotage**, deliberate attacks intended to disable or modify computers or networks for the purpose of disrupting operations or transactions, accessing or destroying files or otherwise compromising an organization.

The Jury reviewed many news reports of cyber-attacks on public entities, a few of which are summarized below:

A ransomware attack in March 2018 paralyzed Atlanta's 424 software programs, of which 30% were mission critical. Atlanta refused to pay the ransom of \$51,000 and it ultimately cost the city \$21 million to recover their systems.⁵

In May 2019, Baltimore refused to pay a \$76,000 ransom demand resulting in weeks of downtime and system upgrade costs of \$18 million. Subsequently, the city purchased insurance policies totaling \$20 million, with an annual premium of \$835,103.⁶

As recently as July 2019, Los Angeles city computers were breached, resulting in the theft of the personal information of approximately 20,000 applicants to the police department. The information stolen did not directly impact the city, but could be used to compromise the privacy of the individuals, and allow the criminals to open credit cards, take out loans, intercept tax refunds, and otherwise disrupt an individual's credit.⁷

In August 2019, \$4.2 million was stolen from the Oklahoma Law Enforcement Retirement System after an employee's account was compromised.⁸

In October 2019, it was reported there were more than 140 ransomware demands in the last 10 months across the United States. These attacks were made on county, city, or state government systems, including health care systems and police departments.⁹

While sabotage of governmental computer systems and networks has not yet been reported as widespread, there have been instances which demonstrate it is a valid concern. In 2013, a New York

⁵ Lee Matthews, "City Of Atlanta Computers Hit By Ransomware Attack", *Forbes*, March 23, 2018 <https://www.forbes.com/sites/leemathews/2018/03/23/city-of-atlanta-computers-hit-by-ransomware-attack/#3a8316812ee4> (Last visited 02/03/2020)

⁶ Sarah Cole, "Baltimore Doubles Up on Cyber-Insurance Following Ransomware Attack", *Infosecurity Group*, October 18, 2019 <https://www.infosecurity-magazine.com/news/baltimore-buys-cyber-insurance/> (Last visited 02/03/2020)

⁷ Cindy Chang, David Zahniser, "City computers breached, data potentially stolen from 20,000 LAPD applicants," *Los Angeles Times*, July 29, 2019 <https://www.latimes.com/california/story/2019-07-29/lapd-applicants-data-breach> (Last visited 02/03/2020)

⁸ Nolan Clay, "Hackers get \$4.2 million from Oklahoma pension fund for retired troopers, state agents", *The Oklahoman*, September 6, 2019 <http://oklahoman.com/article/5640503/hackers-get-42-million-from-pension-fund-for-retired-troopers-state-agents> (Last visited 02/03/2020)

⁹ Allen Kim, "In the last 10 months, 140 local governments, police stations and hospitals have been held hostage by ransomware attacks", *CNN.com*, October 8, 2019 <https://www.cnn.com/2019/10/08/business/ransomware-attacks-trnd/index.html> (Last visited 02/03/2020)

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

dam's control system was hacked by a foreign group.¹⁰ In January 2020, the Federal Depository Library Program's website was hijacked, and a pro-Iranian message was displayed.¹¹

In January 2020 in Santa Barbara County, the Carpinteria Unified School District was attacked by ransomware, temporarily shutting down the district's networked computers and creating \$90,000 in damage.¹²

Cyber security is a critical element of today's world of computerized life. Types of attacks that can occur include:

- **Phishing** is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.
- **Harvesting employee credentials, also known as password harvesting**, takes many forms, including phishing, and is used to steal user credentials. Credential-harvesting attacks often start with targeted phishing emails that request the victim to click on a link and log into their own account to change password or payment information. The link then directs the user to a spoofed¹³ site, allowing the hacker to harvest the valid credentials entered by the victim, and then use those to log into the victim's actual account.
- **Backdoor** is a method of bypassing authentication in a piece of software or a computer system allowing access without being detected.
- **Social engineering** is manipulating people to give up confidential information. The type of information sought includes passwords, bank information and other personal information. It can also help someone gain access to your computer to secretly install malicious software, allowing them access to and control of your confidential information.
- **Programming bug** is a programming error in the computer code that results in faulty results or information. It can also allow for unwanted access to a computer system or network.
- **Outdated software** is software that is no longer fully supported by the vendor which can make it easier to attack through known flaws and weaknesses in the system.

¹⁰ Joseph Burger, "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case", *The New York Times*, March 25, 2016 <https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html> (Last visited 02/03/2020)

¹¹ Mihir Zaveri, "Government Website Is Hacked With Pro-Iran Messages", *The New York Times*, January 6, 2020 <https://www.nytimes.com/2020/01/06/us/iran-hack-federal-depository-library.html> (Last visited 02/03/2020)

¹² Debra Herrick, "CUSD Hit By Malware...", *Coastal View News* (January 23, 2020)

¹³ Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. <https://www.forcepoint.com/cyber-edu/spoofing> (Last visited 02/17/2020)

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

- *Unpatched software* is software that has not been updated to the latest version provided by the vendor. Similar to outdated software, it can be easier to attack.
- *System misconfiguration* is when settings within a computer program are not configured properly and could allow unauthorized access or unintended consequences.
- *Inside attack* is an attack by someone with authorized access to a computer system or network that uses the access in ways not approved or granted by the organization. This can sometimes occur when a terminated employee's system access has not been revoked on a timely basis.
- *Physical attack* involves gaining access to computer systems and networks through physical means. This includes unauthorized access to facilities and buildings but can also include accessing the systems and networks by using an unattended computer terminal.

Every public entity within Santa Barbara County needs to be familiar with these dangers and threats and the steps that need to be taken to prevent them.

METHODOLOGY

The Grand Jury interviewed two well-known experts on cybersecurity, a Certified Information Systems Security Professional and a highly credentialed Independent Information Security Analyst. The Jury attended an all-day Cybersecurity Summit at UC Santa Barbara, which included seminars and interaction with speakers and attendees. The Jury also reviewed a large number of studies, news reports and professional articles related to cyber security.

The Jury interviewed individuals who have extensive experience in cyber security. Their experiences include:

- Oversight of information technology security for private enterprise and government organizations
- Presidency of information security management service organizations
- Service on cyber security task forces
- Work in national information security

To get an overview of the general status of cyber security awareness within the County, the Grand Jury sent surveys to many governmental entities within the County, including the incorporated cities, special districts and the County itself. The surveys were emailed to administrators and Information Technology (IT) department heads. The surveys covered a variety of cyber security issues, including the nature of their systems and how they are administered, whether there is a written cyber security plan and if it has been tested, whether cyber security audits are performed and when the last audit was, and whether they have cyber insurance and what kind.

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

OBSERVATIONS

The responses to the Grand Jury's survey showed most entities were deficient in one or more critical areas. Many of those surveyed reported that they had no cyber security plan, had never performed a security audit and carried no cyber insurance.

Clearly, many public entities within Santa Barbara County are not fully prepared to withstand a cyber-attack.

Important Concepts and Best Practices:

As a result of its investigation, the Grand Jury found the following important concepts and best practices should be implemented as soon as possible to lower an organization's risks from cyber threats and damage:

- ***Identify someone to be in charge.*** Organizations should appoint a designated individual with the proper expertise who is granted authority to be accountable and responsible for all cyber security, including managed service providers.¹⁴
- ***Identify the nature of the organization's data and the electronic systems employed and understand the security risks.*** Organizations should understand what type of data they maintain and use in the execution of their mission and the electronic systems employed that do, or could, allow access to the data. How is the data handled and protected to prevent unauthorized use? Who has access to that data and under what circumstances? What are risks related to unauthorized access or, in the worst case, destruction of the organization's data?
- ***Establish a written cyber security plan.*** A cyber security plan adds a layer of protection to an organization's important resources. Protecting important data and related systems is important, not only for the organization, but also its customers. Cybercrime is escalating and having a strong defense and recovery plan helps protect the organization's reputation. A well written plan should not only detail the preventative steps the organization needs to take to prevent an attack, but also provide a recovery plan in case the data is attacked, corrupted or otherwise compromised.
- ***Protect data from internal and external threats.*** Data can be attacked or compromised from many sources, whether intentional or by accident. Protecting an organization's data and systems from an external threat and intentional attack is not enough—they also must be protected from unauthorized internal access, accidental corruption or destruction. An organization's plan needs to identify and

¹⁴ Edward Gately, "ESET: MSPs Not Proactive Enough with Cybersecurity", *ChannelFutures.com*, February 7, 2020 <https://www.channelfutures.com/channel-research/eset-mtps-not-proactive-enough-with-cybersecurity/>. (Last visited 02/10/2020)

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

address all possible threats and should require periodic changing of all passwords and making sure sensitive systems are contained in a secure environment with controlled access.

- ***Have strong firewalls, appropriate authorization and access controls, and effective antivirus software.*** Strong firewalls prevent unauthorized outside access to an organization's systems and data. If an attacker cannot get into the system, it is harder for them to disrupt operations or damage or steal data. Having an appropriate authorization and access control system helps, among other things, assure that employees and authorized contractors can access only the systems and data they require to properly execute their duties and helps prevent unauthorized activities, theft, corruption or destruction of data. Antivirus software helps prevent software viruses, worms, "Trojan Horses," spyware or malware from being downloaded to an organization's electronic systems, as well as increasing protection from phishing attacks.
- ***Install and update software regularly.*** Using the correct software and keeping it updated frequently is a strong step to help prevent attacks. Software providers are continually updating and improving their products to not only make it more effective but to address flaws that are discovered that could be used to attack an organization's systems or data. Old and out-of-date software is much more vulnerable than current software. Software should not only be updated on internal equipment but also on all portable devices that have access to the organization's systems.
- ***Maintain cyber security awareness and training for all employees.*** A system is only as strong as the people who are using it. While there are many ways to attack a system electronically, one of the easiest ways to get access to a system is to trick someone to open the door for you. This "social engineering" is cheap, effective and quicker than trying to break into a system through other means. Employees and contractors with access to the system should be made aware of the dangers of social engineering and phishing scams, and be trained how to prevent access through these means. This awareness and training should focus not only on electronic devices provided by the organization but also personal and portable electronic devices that have access to the organization's system via Wi-Fi, email or the internet.
- ***Create a recovery plan.*** While planning and prevention is a vital component to strong cyber security, the reality is that things can go wrong, attackers can succeed, and things break. Therefore, it is very important that an organization have a detailed and documented recovery plan. This plan, among other things, should include periodic backups, and safe offsite storage of backup data and system software.
- ***Regularly update and test the plan.*** Just like practice fire drills are an important component of assuring the safety of employees, practicing the steps of an organization's cyber security plan, especially the recovery components of the plan, is vitally important. Practice runs not only help to confirm if the plan works and what improvements could be made, they also prepare the organization for a fast response in the case of an actual attack.

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

- *Consider working with other organizations to improve cyber security practices cost effectively.* Working as a consortium provides an approach allowing even those with smaller budgets to participate and contribute to a successful security program.¹⁵

CONCLUSIONS

The 2019-20 Santa Barbara County Grand Jury determined that cyber-attacks and related threats are an ongoing reality and that all public entities within Santa Barbara County need to take prompt and aggressive steps to prevent significant disruption from these attacks. When cyber-attacks are successful, the costs to respond and recover can be in the millions of dollars. While some local public entities are taking steps to protect themselves from these risks, many are not adequately prepared.

FINDINGS AND RECOMMENDATIONS

Finding 1

Ensuring critical cyber security tasks and activities are properly executed on a timely basis requires a designated individual to be accountable and responsible.

Recommendation 1

That each public entity within Santa Barbara County designate an individual to be accountable and responsible to oversee cyber security.

Finding 2

Most public entities within Santa Barbara County have an inadequate understanding of what communication and electronic systems they use and what data they maintain, and do not fully understand the risks, security issues and costs associated with the destruction of systems or loss of data.

Recommendation 2

That each public entity within Santa Barbara County complete a full inventory of their data, electronic and communication systems and determine the related security risks.

Finding 3

Some public entities within Santa Barbara County do not have a written cyber security plan.

Recommendation 3

That each public entity within Santa Barbara County establish a written cyber security plan.

¹⁵ Wany Zhao and Gregory White, "A collaborative information sharing framework for community cyber security," published in Homeland Security (HST), 2012 IEEE Conference on Technologies for Homeland Security (HST), November 13-15, 2012

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

Finding 4

Nationally, cyber-attacks on governmental organizations have been successful for many years and are occurring with more frequency and sophistication.

Recommendation 4

That each public entity within Santa Barbara County take substantial steps to protect data from internal and external attacks or threats.

Finding 5

Cyber-attackers use a number of methods to install malicious software on systems including access through backdoors, staff or employee carelessness, and known bugs in software.

Recommendation 5a

That each public entity within Santa Barbara County install and maintain current antivirus software to detect malware and other threats.

Recommendation 5b

That each public entity within Santa Barbara County install and update all operating software regularly.

Recommendation 5c

That each public entity within Santa Barbara County periodically train employees and then test their cyber security awareness.

Recommendation 5d

That each public entity within Santa Barbara County periodically ensure electronic system-related contractors have been trained for cyber security awareness.

Finding 6

If data is lost or compromised for any reason, including cyber-attack, mechanical failure or error, the most cost effective and expedient way to recover is to have current data backups and a plan to reinstall it.

Recommendation 6a

That each public entity within Santa Barbara County create and implement a full backup and recovery plan.

Recommendation 6b

That each public entity within Santa Barbara County regularly update and test their backup and recovery plan.

Finding 7

Some public entities within Santa Barbara County do not have any, or adequate, cyber insurance.

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

Recommendation 7

That each public entity within Santa Barbara County secure adequate cyber insurance.

Finding 8

A cost-effective method to address cyber risks and concerns is to form an information sharing and learning consortium.

Recommendation 8

That each public entity within Santa Barbara County that is unable to allocate adequate funds for cyber security develop a cybersecurity working group to establish best practices and share costs for education, expertise, and insurance.

REQUEST FOR RESPONSE

Pursuant to *California Penal Code Sections 933 and 933.05*, the Santa Barbara County Grand Jury requests each entity or individual named below to respond to the enumerated findings and recommendations with the specified statutory time limit:

Responses to Findings shall be either:

- Agree
- Disagree wholly
- Disagree partially with an explanation

Responses to Recommendations shall be one of the following:

- Has been implemented, with brief summary of implementation actions taken
- Will be implemented, with an implementation schedule
- Requires further analysis, with analysis completion date of no more than six months after the issuance of the report
- Will not be implemented, with an explanation of why

Santa Barbara County Board of Supervisors – 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8

Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8

City of Buellton – 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8

Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

City of Carpinteria – 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8

Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8

City of Goleta – 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8

Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8

City of Guadalupe – 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8

Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8

City of Lompoc – 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8

Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8

City of Santa Barbara – 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8

Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8

City of Santa Maria – 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8

Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8

City of Solvang – 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8

Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8



May 21, 2020

The Honorable Judge Michael J. Carrozzo
Presiding Judge, Santa Barbara Superior Court
1100 Anacapa Street
Santa Barbara, CA 93101

Re: Grand Jury Report titled "Cyber-Attacks Threaten Santa Barbara County"

Dear Judge Carrozzo:

This letter is the response of the Guadalupe City Council and the City's Mayor to the Santa Barbara Grand Jury report titled "Cyber-Attacks Threaten Santa Barbara County." This response is submitted in compliance with Penal Code Sections 933 and 933.05. A copy of this response is being sent concurrently to the Grand Jury.

The Grand Jury report sets forth eight (8) findings and twelve (12) recommendations. The City Council of the City of Guadalupe is required to respond to all eight (8) findings and all twelve (12) recommendations.

Finding 1

Ensuring critical cyber security tasks and activities are properly executed on a timely basis requires a designated individual to be accountable and responsible.

- Response: Agree.

Recommendation 1

That each public entity within Santa Barbara County designate an individual to be accountable and responsible to oversee cyber security.

- Response: Has been implemented. The City Administrator has been designated the primary individual to be accountable and responsible to oversee cyber security.

Finding 2

Most public entities within Santa Barbara County have an inadequate understanding of what communication and electronic systems they use and what data they maintain, and do not fully

understand the risks, security issues and costs associated with the destruction of systems or loss of data.

- Response: Agree.

Recommendation 2

That each public entity within Santa Barbara County complete a full inventory of their data, electronic and communication systems and determine the related security risks.

- Response: Has been implemented. City of Guadalupe stores City data on shared drives stored on in-house servers. Files and folders are organized and secured to limit access to only appropriate and approved City staff. Email is controlled through an in-house Microsoft Exchange Email Server using standard security practices based on Microsoft guidelines for government entities. All email is scanned for malware and spam before being delivered. Line-of-business applications are all stored on in-house servers so the City can better control access to sensitive data. The City has recently prepared an inventory of its equipment and communication systems. In addition, the City is evaluating other alternatives to mitigate security risk, which may include moving records from a physical server to a cloud-based system, cybersecurity scan of its network, further isolating and protecting backups, updating to Microsoft Office 365, and rotating out outdated equipment.

Finding 3

Some public entities within Santa Barbara County do not have a written cyber security plan.

- Response: Agree.

Recommendation 3

That each public entity within Santa Barbara County establish a written cyber security plan.

- Response: Will be implemented. The City's Information Technology (IT) service provider has been directed to help the City develop a written cyber security plan over the next 90 days.

Finding 4

Nationally, cyber-attacks on governmental organizations have been successful for many years and are occurring with more frequency and sophistication.

- Response: Agree.

Recommendation 4

That each public entity within Santa Barbara County take substantial steps to protect data from internal and external attacks or threats.

- Response: Has been implemented. A hardened firewall, updated regularly, is in place to

protect all City IT infrastructure from external attacks. To help remedy internal attacks, all City staff are limited to access only the data needed to perform their job functions. Auditing in place on servers allows for tracking of suspicious behavior. Enterprise-grade anti-virus is installed to protect data from any malicious activity. The City will receive a cybersecurity scan of its network to identify any weaknesses. The City will have its employees change their passwords often and will include multifactor authentication. In addition, the City is evaluating other alternatives to mitigate security risk, which may include moving records from a physical server to a cloud-based system, cybersecurity scan of its network, further isolating and protecting backups, updating to Microsoft Office 365, and rotating out outdated equipment.

Finding 5

Cyber-attackers use a number of methods to install malicious software on systems including access through backdoors, staff or employee carelessness, and known bugs in software.

- Response: Agree.

Recommendation 5a

That each public entity within Santa Barbara County install and maintain current antivirus software to detect malware and other threats.

- Response: Has been implemented. Enterprise-grade anti-virus is installed on all appropriate devices to protect data from any malicious activity (malware and other threats).

Recommendation 5b

That each public entity within Santa Barbara County install and update all operating software regularly.

- Response: Will be implemented. The City is already in the process of upgrading all servers. The City's plan is to complete upgrades of all old workstations and laptops throughout the coming year fiscal year 20-21. The City's accounting system is in the process of being upgraded and should be completed within one year. All systems owned by the City receive weekly security updates to the current operating systems, as well as line of business applications where appropriate.

Recommendation 5c

That each public entity within Santa Barbara County periodically train employees and then test their cyber security awareness.

- Response: Will be implemented pending available funds for service. The City will be developing a cyber-security awareness training plan for its employees within the next 6 months. Testing cyber-security awareness for the City's employees is best completed using services purchased from a 3rd party. The City currently has no funds available for this purpose. The City will seek attempt to obtain funding for this purpose by applying

for grants and/or trying to increase revenue. The City will instruct its employees about cyber security awareness by advising all City employees about the Grand Jury's report and the City's response and direct all employees to read the Grand Jury's report in order to increase cyber-security awareness.

Recommendation 5d

That each public entity within Santa Barbara County periodically ensure electronic system-related contractors have been trained for cyber security awareness.

- Response: Has been implemented.

Finding 6

If data is lost or compromised for any reason, including cyber-attack, mechanical failure or error, the most cost effective and expedient way to recover is to have current data backups and a plan to reinstall it.

- Response: Agree.

Recommendation 6a

That each public entity within Santa Barbara County create and implement a full backup and recovery plan.

- Response: Has been implemented. Enterprise-grade backup and disaster recovery software is installed on all servers. All City data is stored on the servers. The City's IT service provider continually updates the recovery plan as changes take place. However, the City is evaluating the alternative of having offsite cloud backups.

Recommendation 6b

That each public entity within Santa Barbara County regularly update and test their backup and recovery plan.

- Response: Has been implemented. The City's IT service provider tests the integrity of backups, as well as the recovery process, every 3 months. The back and recovery plan is updated as changes are made.

Finding 7

Some public entities within Santa Barbara County do not have any, or adequate, cyber insurance.

- Response: Agree.

Recommendation 7

That each public entity within Santa Barbara County secure adequate cyber insurance.

- Response: Has been implemented. The city has cyber insurance through the California

Joint Powers Insurance Authority.

Finding 8

A cost-effective method to address cyber risks and concerns is to form an information sharing and learning consortium.

- Response: Agree.

Recommendation 8

That each public entity within Santa Barbara County that is unable to allocate adequate funds for cyber security develop a cybersecurity working group to establish best practices and share costs for education, expertise, and insurance.

Response: Has been implemented. The City is already actively addressing cyber risks and concerns; however, the City is willing to participate in such cybersecurity working group and share costs provided that the City has available funds for such purposes.

Sincerely,

Ariston D. Julian, Mayor

Gina Rubalcaba, Mayor pro tem

Tony Ramirez, Council member

Eugene Costa Jr., Council member

Liliana Cardenas, Council member

RESOLUTION NO. 2020-39

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF GUADALUPE ADOPTING A RESPONSE TO THE SANTA BARBARA COUNTY GRAND JURY REPORT ENTITLED "CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY"

WHEREAS, the Santa Barbara County Grand Jury released a report on March 18, 2020 titled "Cyber-Attacks Threaten Santa Barbara County" with eight (8) findings and twelve (12) recommendation; and

WHEREAS, the City Council of the City of Guadalupe is required to response to eight (8) of these findings (nos. 1, 2, 3, 4, 5, 6, 7, and 8) and recommendations 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, and 8; and

WHEREAS, the City Council has 90 days to respond to this report, each finding, and the recommendations; and

WHEREAS, City staff prepared responses on behalf of the City Council and submitted them to the City Council for adoption at the City Council's meeting on May 26, 2020.

NOW, THEREFORE, BE IT RESOLVED by the City Council of the City of Guadalupe as follows:

SECTION 1: Staff's responses are approved and adopted by the City Council as the official response of the City Council to the above-mentioned Santa Barbara Grand Jury.

SECTION 2: The City Council authorizes staff to submit (Exhibit 1) final response with the signatures of each member of the City Council to Judge Michael J. Carrozzo and the Santa Barbara Grand Jury.

PASSED AND ADOPTED at a regular meeting of the City Council of the City of Guadalupe on the 26th day of May 2020 by the following vote.

Motion:

AYES:

NOES:

ABSENT:

ABSTAIN:

I, **Joice Earleen Raguz, City Clerk of the City of Guadalupe** DO HEREBY CERTIFY that the foregoing Resolution, being Resolution No. 2020-39, has been duly signed by the Mayor and attested by the City Clerk, all at a regular meeting of the City Council, held May 26, 2020, and that same was approved and adopted.

ATTEST:

Joice Earleen Raguz, City Clerk

Ariston Julian, Mayor

APPROVED AS TO FORM:

Philip F. Sinco, City Attorney



(Exhibit 1)

May 21, 2020

The Honorable Judge Michael J. Carrozzo
Presiding Judge, Santa Barbara Superior Court
1100 Anacapa Street
Santa Barbara, CA 93101

Re: Grand Jury Report titled "Cyber-Attacks Threaten Santa Barbara County"

Dear Judge Carrozzo:

This letter is the response of the Guadalupe City Council and the City's Mayor to the Santa Barbara Grand Jury report titled "Cyber-Attacks Threaten Santa Barbara County." This response is submitted in compliance with Penal Code Sections 933 and 933.05. A copy of this response is being sent concurrently to the Grand Jury.

The Grand Jury report sets forth eight (8) findings and twelve (12) recommendations. The City Council of the City of Guadalupe is required to respond to all eight (8) findings and all twelve (12) recommendations.

Finding 1

Ensuring critical cyber security tasks and activities are properly executed on a timely basis requires a designated individual to be accountable and responsible.

- Response: Agree.

Recommendation 1

That each public entity within Santa Barbara County designate an individual to be accountable and responsible to oversee cyber security.

- Response: Has been implemented. The City Administrator has been designated the primary individual to be accountable and responsible to oversee cyber security.

Finding 2

Most public entities within Santa Barbara County have an inadequate understanding of what communication and electronic systems they use and what data they maintain, and do not fully

understand the risks, security issues and costs associated with the destruction of systems or loss of data.

- Response: Agree.

Recommendation 2

That each public entity within Santa Barbara County complete a full inventory of their data, electronic and communication systems and determine the related security risks.

- Response: Has been implemented. City of Guadalupe stores City data on shared drives stored on in-house servers. Files and folders are organized and secured to limit access to only appropriate and approved City staff. Email is controlled through an in-house Microsoft Exchange Email Server using standard security practices based on Microsoft guidelines for government entities. All email is scanned for malware and spam before being delivered. Line-of-business applications are all stored on in-house servers so the City can better control access to sensitive data. The City has recently prepared an inventory of its equipment and communication systems. In addition, the City is evaluating other alternatives to mitigate security risk, which may include moving records from a physical server to a cloud-based system, cybersecurity scan of its network, further isolating and protecting backups, updating to Microsoft Office 365, and rotating out outdated equipment.

Finding 3

Some public entities within Santa Barbara County do not have a written cyber security plan.

- Response: Agree.

Recommendation 3

That each public entity within Santa Barbara County establish a written cyber security plan.

- Response: Will be implemented. The City's Information Technology (IT) service provider has been directed to help the City develop a written cyber security plan over the next 90 days.

Finding 4

Nationally, cyber-attacks on governmental organizations have been successful for many years and are occurring with more frequency and sophistication.

- Response: Agree.

Recommendation 4

That each public entity within Santa Barbara County take substantial steps to protect data from internal and external attacks or threats.

- Response: Has been implemented. A hardened firewall, updated regularly, is in place to

protect all City IT infrastructure from external attacks. To help remedy internal attacks, all City staff are limited to access only the data needed to perform their job functions. Auditing in place on servers allows for tracking of suspicious behavior. Enterprise-grade anti-virus is installed to protect data from any malicious activity. The City will receive a cybersecurity scan of its network to identify any weaknesses. The City will have its employees change their passwords often and will include multifactor authentication. In addition, the City is evaluating other alternatives to mitigate security risk, which may include moving records from a physical server to a cloud-based system, cybersecurity scan of its network, further isolating and protecting backups, updating to Microsoft Office 365, and rotating out outdated equipment.

Finding 5

Cyber-attackers use a number of methods to install malicious software on systems including access through backdoors, staff or employee carelessness, and known bugs in software.

- Response: Agree.

Recommendation 5a

That each public entity within Santa Barbara County install and maintain current antivirus software to detect malware and other threats.

- Response: Has been implemented. Enterprise-grade anti-virus is installed on all appropriate devices to protect data from any malicious activity (malware and other threats).

Recommendation 5b

That each public entity within Santa Barbara County install and update all operating software regularly.

- Response: Will be implemented. The City is already in the process of upgrading all servers. The City's plan is to complete upgrades of all old workstations and laptops throughout the coming year fiscal year 20-21. The City's accounting system is in the process of being upgraded and should be completed within one year. All systems owned by the City receive weekly security updates to the current operating systems, as well as line of business applications where appropriate.

Recommendation 5c

That each public entity within Santa Barbara County periodically train employees and then test their cyber security awareness.

- Response: Will be implemented pending available funds for service. The City will be developing a cyber-security awareness training plan for its employees within the next 6 months. Testing cyber-security awareness for the City's employees is best completed using services purchased from a 3rd party. The City currently has no funds available for this purpose. The City will seek attempt to obtain funding for this purpose by applying

for grants and/or trying to increase revenue. The City will instruct its employees about cyber security awareness by advising all City employees about the Grand Jury's report and the City's response and direct all employees to read the Grand Jury's report in order to increase cyber-security awareness.

Recommendation 5d

That each public entity within Santa Barbara County periodically ensure electronic system-related contractors have been trained for cyber security awareness.

- Response: Has been implemented.

Finding 6

If data is lost or compromised for any reason, including cyber-attack, mechanical failure or error, the most cost effective and expedient way to recover is to have current data backups and a plan to reinstall it.

- Response: Agree.

Recommendation 6a

That each public entity within Santa Barbara County create and implement a full backup and recovery plan.

- Response: Has been implemented. Enterprise-grade backup and disaster recovery software is installed on all servers. All City data is stored on the servers. The City's IT service provider continually updates the recovery plan as changes take place. However, the City is evaluating the alternative of having offsite cloud backups.

Recommendation 6b

That each public entity within Santa Barbara County regularly update and test their backup and recovery plan.

- Response: Has been implemented. The City's IT service provider tests the integrity of backups, as well as the recovery process, every 3 months. The back and recovery plan is updated as changes are made.

Finding 7

Some public entities within Santa Barbara County do not have any, or adequate, cyber insurance.

- Response: Agree.

Recommendation 7

That each public entity within Santa Barbara County secure adequate cyber insurance.

- Response: Has been implemented. The city has cyber insurance through the California

Joint Powers Insurance Authority.

Finding 8

A cost-effective method to address cyber risks and concerns is to form an information sharing and learning consortium.

- Response: Agree.

Recommendation 8

That each public entity within Santa Barbara County that is unable to allocate adequate funds for cyber security develop a cybersecurity working group to establish best practices and share costs for education, expertise, and insurance.

Response: Has been implemented. The City is already actively addressing cyber risks and concerns; however, the City is willing to participate in such acyber security working group and share costs provided that the City has available funds for such purposes.

Sincerely,

Ariston D. Julian, Mayor

Gina Rubalcaba, Mayor pro tem

Tony Ramirez, Council member

Eugene Costa Jr., Council member

Liliana Cardenas, Council member