



# City of Camarillo

601 Carmen Drive • P.O. Box 248 • Camarillo, CA 93011-0248

Office of the City Manager  
(805) 388-5307  
FAX (805) 388-5318



RECEIVED

AUG 04 2020

Ventura County  
Grand Jury

July 24, 2020

Anida Margolis, Foreperson  
2019-2020 Ventura County Grand Jury  
County of Ventura  
800 South Victoria Avenue  
Ventura, CA 93009

## Re: Cybersecurity Strategies for Cities in Ventura County

Dear Foreperson Margolis:

Attached you will find the Camarillo City Council's written response signed by Mayor Tony Trembley, as requested by the Grand Jury, to the Conclusions and Recommendations in the subject report.

If additional information is needed, please feel free to contact me at (805) 388-5307.

Sincerely,

Greg Ramirez  
City Manager

cc: City Clerk  
Interim Director of Administrative Services



# City of Camarillo

601 Carmen Drive • P.O. Box 248 • Camarillo, CA 93011-0248

Administrative Services Department  
(805) 383-5633  
Fax (805) 388-5318

## Response to Grand Jury Report Form

**Report Title:** Cybersecurity Strategies for Cities in Ventura County

**Report Date:** July 22, 2020

**Response By:** City Council of the City of Camarillo

Pursuant to California Penal Code Sections 933.05 (c) and (d), the City Council of the City of Camarillo provided a response to the "Cybersecurity Strategies for Cities in Ventura County" Grand Jury Report.

### BACKGROUND

On May 21, 2020, the Ventura County Grand Jury provided the City Council and City Manager with a report of its investigation entitled, "Cybersecurity Strategies for Cities in Ventura County".

### FORMAT OF RESPONSE

The City's detailed response to the Grand Jury Report is set forth in the following pages. The response is ordered in the same manner as the report itself – Facts, Conclusions, and Recommendations.

### RESPONSE TO FINDINGS

There were no Findings in the final report.

### RESPONSE TO CONCLUSIONS

**C-01** "While the Grand Jury recognizes each city is taking steps to implement cybersecurity and to defend against cyberattacks, it concludes there is no perfect solution to cybersecurity or defense against cyberattacks. (FA-01, FA-02, FA-03, FA-04, FA-05, FA-06, FA-07)"

**City Response:** We agree with conclusion C-01.

**C-02** "The Grand Jury concluded eight Cities are currently using suboptimal web addresses for their websites. (FA-08, FA-09)"

**City Response:** We mostly agree with conclusion C-02. This conclusion does not necessarily make the website more secure but can assist in validating our web address to the public. We already use HTTPS to secure our websites and payment portals. We will consider adding the .gov domain as an option as part of our upcoming website redesign.

**C-03** "The Grand Jury concluded generally Cities are not utilizing free federal and discounted federally aligned resources available to Cities to bolster their cybersecurity defenses. (FA-10, FA-11, FA-12, FA-13, FA-14, FA-15, FA-16, FA-17, FA-18, FA-19, FA-20)"

**City Response:** We agree with conclusion C-03. Since receiving the Grand Jury's Final report, we have begun the process of engaging CISA and MISAC to take advantage of their free resources. We have regularly attended MISAC conferences including the conference held in 2019.

**C-04** "The Grand Jury concluded cybersecurity staffing could be improved with more effective recruiting and staff retention practices. (FA-21, FA-22, FA-23)"

**City Response:** We mostly agree with conclusion C-04. We currently employ five full-time IS staff positions with two focused on network infrastructure and security. We conduct annual salary surveys to ensure wages and benefits are competitive and have had no problems with retention of staff. When opportunities arise, we will consider recruiting interns from County higher education internship programs.

**C-05** "The Grand Jury concluded Cities should manage cyber risks associated with vendors by requiring they provide annual documentation regarding cybersecurity insurance and cybersecurity practices. (FA-24, FA-25, FA-30, FA-31)"

**City Response:** We agree with conclusion C-05. We already require cybersecurity insurance from our information technology vendors.

**C-06** "The Grand Jury concluded some Cities do not clearly identify expenditures regarding information technology or cybersecurity in their budgets. (FA-26, FA-27)"

**City Response:** We agree with conclusion C-06. We currently identify information technology and cybersecurity expenditures within our annual budget.

**C-07.** "The Grand Jury concluded all Cities would benefit from comprehensive cyber incident response, recovery, and business continuity plans. (FA-28, FA-29)"

**City Response:** We agree with conclusion C-07. We regularly update and maintain a disaster response plan which addresses cyber incident response, recovery, and business continuity plans.

**C-08.** "The Grand Jury concluded some Cities are not following the recommended best practices for teleworking published by California Cyber Security Integration Center. (FA-03, FA-04)"

**City Response:** We agree with conclusion C-08. Before the COVID-19 virus outbreak, we had no teleworking staff. To maintain business continuity during the outbreak, we began implementing teleworking with select staff while following the best practices as recommended by the California Cyber Security Integration Center.

**R-01.** "The Grand Jury recommends Cities establish secure web addresses through the use of HTTPS or other such protocols. (C-02)"

**City Response:** We agree with recommendation R-01. This recommendation has already been implemented. We use the HTTPS protocol across all City webpages, payment portals, and web addresses.

**R-02.** "The Grand Jury recommends Cities establish trustworthy web addresses by following the California Department of Technology domain name taxonomy guidance. (C-02)"

**City Response:** As stated above, we mostly agree with recommendation R-02. This conclusion does not necessarily make the website more secure but can assist in validating our web address to the public. We already use HTTPS to secure our websites and payment portals. We will consider adding the .gov domain as an option as part of our upcoming website redesign.

**R-03.** "The Grand Jury recommends Cities utilize free federal and federally aligned cybersecurity services as set forth in Appendix 02 to supplement internal staff and/or replace vendor services whenever possible. (C-03)"

**City Response:** We agree with conclusion R-03. We already utilize several of the listed resources and are exploring additional services not currently used.

**R-04.** "The Grand Jury recommends Cities' IT staff subscribe to CISA updates online. (C-03)"

**City Response:** We agree with recommendation R-04. This recommendation has already been implemented. We currently receive the CISA technology updates and alerts.

**R-05.** "The Grand Jury recommends Cities take advantage of discounted services and cooperative purchasing programs whenever possible. (C-03)"

**City Response:** We agree with recommendation R-05. We already take advantage of cooperative purchasing programs whenever possible, per our City Purchasing Policy. We will continue to find ways to take advantage of available discounted services.

**R-06.** “The Grand Jury recommends Cities develop personnel cost-saving opportunities and create a cybersecurity talent pool by recruiting interns or graduating students using: (C-04)

- The Scholarships for Service program described in Appendix 02
- Local educational institutions (high school, community college, private college and state university)”

**City Response:** We agree with recommendation R-06. We will explore opportunities offered through the Scholarships for Service program and consider recruiting interns from County higher education internship programs when opportunities arise.

**R-07.** “The Grand Jury recommends Cities maintain good vendor management by: (C-03, C-05)

- Obtaining CISA assistance to conduct risk management assessments on all third-party vendors that have access to any confidential data or that interact with City networks and systems
- Requiring all vendors provide cybersecurity documentation. As part of their ongoing third-party due diligence, Cities should evaluate vendors for compliance and risk on an annual basis.
- Requiring IT vendors obtain cybersecurity insurance.”

**City Response:** We agree with recommendation R-07. This recommendation has already been implemented. The City will explore CISA assistance in risk management of their vendors and begin reviewing on an annual basis. We currently require cybersecurity insurance from our IT vendors.

**R-08.** “The Grand Jury recommends Cities clearly identify expenses for their Information Services (Technology) Departments in their approved budgets. (C-06)”

**City Response:** We agree with recommendation R-08. This recommendation has already been implemented. We currently identify all Information Services expenditures separately in our budget.

**R-09.** “The Grand Jury recommends Cities develop and test cyber incident response, recovery and business continuity plans. (C-07)”

**City Response:** We agree with recommendation R-09. This recommendation has already been implemented. We regularly update and maintain a disaster response plan which addresses cyber incident response, recovery, and business continuity plans.

**R-10.** "The Grand Jury recommends Cities implement the best practices for teleworking as published by the California Security Integration Center. (C-08)"

**City Response:** We agree with recommendation R-10. This recommendation has already been implemented. To maintain business continuity during the recent COVID-19 outbreak, we began implementing teleworking with select staff while following the best practices as recommended by the California Cyber Security Integration Center.


**R-11.** "The Grand Jury recommends Cities develop a plan for implementation of R-01 through R-10 prior to December 31, 2020."

**City Response:** We agree with recommendation R-11. We will begin working on a written plan to comply with the December 31, 2020 date. The City has made cybersecurity an increased focus in recent years. All city staff are required to attend annual cybersecurity training. IS staff regularly send out updates and alerts on the latest phishing and ransomware attacks. IS staff attend annual information technology conferences, various webinars and attend vendor demos on the latest trends and applications in cybersecurity.

**SUMMARY**

The City of Camarillo wishes to thank the Grand Jury for its time.

Date: July 22, 2020

Signed:   
Tony Trembley, Mayor  
City of Camarillo

Number of pages attached 0