



"Citrus Capital of the World"

City of Santa Paula

970 Ventura Street • Santa Paula, California • Mailing Address: P.O. Box 569 • 93061 • Phone: (805) 525-4478 • Fax: (805) 525-6278

August 15, 2020

The Honorable Kent M. Kellegrew
Presiding Judge of the Superior Court
County of Ventura
800 South Victoria Avenue
Ventura, CA 93009

Re: City's Response to Grand Jury Report Entitled "Cybersecurity Strategies
for Cities in Ventura County"

Dear Judge Kellegrew:

On April 17, 2020, the Ventura County Grand Jury issued its report entitled "Cybersecurity Strategies for Cities in Ventura County" (the "Report"). In the Report, the Grand Jury assessed the degree to which Cities in the County were prepared to defend against data breaches and ransomware and recommended the implementation of several measures to bolster cybersecurity and decrease cybersecurity expenditures.

At the conclusion of the Report, the Grand Jury requested a response from the City to Conclusions C-01 through C-08 and Recommendations R-01 through R-11. We provide the following responses to these Conclusions and Recommendations in accordance with Penal Code §933.05.

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 of cyberattacks.

The City agrees with Conclusion C-01.

C-02. The Grand Jury concluded eight Cities are currently using suboptimal web addresses for their websites.

The City agrees in part and disagrees in part with Conclusion C-02. It is true that identity thieves can easily generate emails and websites in the dot com or dot org domains that can look and seem like a legitimate web pages. However, trust in links and emails coming from dot.gov domains, or at least the assumption that there are more stringent

verification requirements involved in obtaining a dot.gov domain, is likely misplaced as such domains are not difficult to obtain. Regardless, email recipients should always be wary of unsolicited emails and attachments (even from people you know) and keep software and virus protections and employee training on the subject up to date.

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

The City agrees that the City has not utilized free federal and discounted federally aligned resourced in an effort to bolster its cybersecurity defenses. As noted below, the City intends to evaluate those resources as a mechanism towards furthering its cybersecurity defenses.

C-04. The Grand Jury concluded cybersecurity staffing could be improved with more effective recruiting and staff retention practices.

The City agrees with this conclusion, although it notes that it is difficult to train interns who are often available only at times when classes are not in session. The City does offer internship opportunities in IT, cybersecurity and other fields. The City also agrees that an increase in the salary range for IT professionals would make staff positions more competitive with the private sector. In the interim, however, salary ranges are not likely to increase due to the economic slowdown resulting from the COVID-19 pandemic.

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.

The City agrees with this conclusion. As noted in the Grand Jury's report, the City does have cyber liability insurance through the California Joint Powers Insurance Authority. The City intends to evaluate the need to contractually require vendors that provide information technology-related services (either via the Internet or by otherwise accessing, furnishing, processing, or storing data electronically) to maintain cyber-liability insurance coverage.

C-06. The Grand Jury concluded some Cities do not clearly identify expenditures regarding information technology or cybersecurity in their budgets.

The City agrees that its adopted 2020/21 Annual Budget does not clearly identify amounts spent on cybersecurity. The City notes that while such amounts are not clearly delineated, virtually every line item in the Information Technology Department's budget encompasses amounts earmarked for cybersecurity and cyber defense. While next year's budget will include a line item for cybersecurity software, the City will not specifically identify programs involving cybersecurity in the annual budget for security reasons.

C-07. The Grand Jury concluded all Cities would benefit from comprehensive cyber incident response, recovery and business continuity plans.

The City agrees with this conclusion and is, in fact, currently working on such plans and policies.

C-08. The Grand Jury concluded some Cities are not following the recommended best practices for teleworking published by California Cyber Security Integration Center.

The City agrees with this conclusion and does follow the best practices for teleworking. Among others, the City's IT staff continuously educates all City employees regarding phishing, malware, ransomware and other cyber threats via telephone and email, the City's software system is continuously updated and analyzed to detect malware and other virus threats, and employees are required to change their passwords and password complexity on a regular basis.

Recommendations:

R-01. The Grand Jury recommends Cities establish secure web addresses through the use of HTTPS or other such protocols.

Recommendation R-01 has been implemented. The City currently uses HTTPS on its webpage.

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

Recommendation R-02 requires further analysis as the City has not seen any compelling evidence to suggest that a dot gov domain carries added protections. However, the City will review and discuss the potential advantages and pitfalls of changing its domain name to a dot.gov domain.

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.

Recommendation R-03 requires further analysis. The City intends to evaluate the resources and programs identified in Appendix 02 and will take advantage of any which further the City's cybersecurity defenses. The City relies minimally on contract vendors in its IT Department, but will work with those vendors to require that they maintain cyber-liability insurance coverage.

R-04. The Grand Jury recommends Cities' IT staff subscribe to CISA updates online.

Recommendation R-04 will be implemented. City staff intend to immediately subscribe to the free Cybersecurity Infrastructure Security Agency's online updates.

R-05. The Grand Jury recommends Cities take advantage of discounted services and cooperative purchasing programs whenever possible.

Recommendation R-05 requires further analysis. The City uses cooperative purchasing and discounted services whenever possible. While the City's IT Department intends to utilize CISA's online resources, a further analysis of the programs and benefits identified in Appendix 02 and elsewhere in the report require further study. Those that bolster its cybersecurity defenses will, within budgetary constraints, be utilized.

R-06. The Grand Jury recommends Cities develop personnel cost-saving opportunities and create a cybersecurity talent pool by recruiting interns or graduating students.

Recommendation R-06 has been implemented. The City currently has a robust internship program and those interested in information technology generally or cybersecurity specifically are encouraged to apply.

R-07. The Grand Jury recommends Cities maintain good vendor management by: 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; and Requiring IT vendors obtain cybersecurity insurance.

Recommendation R-07 will be implemented. The City intends to bolster its due diligence on all vendors providing information technology-related services and will require that they maintain cyber-liability insurance coverage.

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

Recommendation R-08 will not be implemented. As noted above, for security reasons the City does not specifically identify programs involving cybersecurity in the annual budget, but will work to establish a broad cybersecurity line-item in the next IT budget.

The Honorable Kent M. Kellegrew
August 15, 2020
Page 5

R-09. The Grand Jury recommends Cities develop and test cyber incident response, recovery and business continuity plans.

Recommendation R-09 will be implemented as budgetary constraints allow. While such a plan exists within the IT Department, the City recognizes that the plan should be expanded to reference employee awareness, training and response, public and private notification protocols, and system restoration prioritization.

R-10. The Grand Jury recommends Cities implement the best practices for teleworking as published by the California Cyber Security Integration Center.

As noted above, Recommendation R-10 has been and will continue to be implemented. As noted, the City's IT Department continuously educates all City employees regarding the new and existing cyber threats and the City's software is continuously updated and analyzed to detect malware and other virus threats.

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

Recommendation R-11 will be implemented in the future. There are funding challenges, however, primarily related to the COVID-19 pandemic that render completion of the report by December 31, 2020, unlikely. The City has and continues to appreciate the risks associated with cyber threats and will endeavor to complete the report within the current fiscal year.

We thank you for the opportunity to respond to the Report. Should you have any further questions or desire any further information, please contact me or City Manager Dan Singer.

Sincerely,



Richard Aratza
Mayor

cc: Santa Paula City Council
Dan Singer, City Manager
Rich Williamson, Information Technology Manager
Anida Margolis, Foreperson

Landon, Carolyn

From: Boehmer, Richard
Sent: Monday, October 19, 2020 9:28 AM
To: Landon, Carolyn
Subject: FW: Grand Jury Response
Attachments: GrandJuryResponseLetters.copy.pdf

Carrie:

Let's discuss on Tuesday.

Rick

From: Dan Singer <dsinger@spcity.org>
Sent: Thursday, October 15, 2020 2:33 PM
To: Boehmer, Richard <Richard.Boehmer@ventura.org>
Cc: raraiza@spcity.org; Allison Fausset <afausset@spcity.org>
Subject: Grand Jury Response

CAUTION: If this email looks suspicious, DO NOT click. Forward to Spam.Manager@ventura.org

Dear Mr. Boehmer,

Last week the Mayor brought to my attention that he had received letters from the Grand Jury that you had not received our responses to the two recent investigations on *Cybersecurity* and *Human Trafficking*. Although my executive assistant has been out on bereavement leave, I'm entirely certain we mailed off copies in late August. I've attached copies of the letters which were reviewed and authorized to be sent by our City Council when we brought these items to them at a public meeting in mid-August. My sincerest apology that they never reached your office.

Please let me know if the attached pdf is sufficient or if we need to generate new original copies and/or whether you require me to mail hard copies to you. Thanks you.

Dan Singer
City Manager
City of Santa Paula
(805) 933-4225



"This is an electronic transmission from the City of Santa Paula. This electronic transmission, and any documents attached hereto, may contain confidential and/or legally privileged information. The information is intended only for use by the recipient named above. If you have received this electronic message in error, please notify the sender and delete the electronic message."