SANTA CRUZ COUNTY GRAND JURY

grandjury <grandjury@scgrandjury.org>

Scotts Valley Response - Cyber Threat Preparedness

'Cathie Simonovich' via Santa Cruz Grand Jury <grandjury@scgrandjury.org> Thu, Aug 3, 2023 at 9:14 AM

Reply-To: Cathie Simonovich <csimonovich@scottsvalley.gov>
To: "Syda.Cogliati@santacruzcourt.org" <Syda.Cogliati@santacruzcourt.org>, "grandjury@scgrandjury.org" <grandjury@scgrandjury.org>
Cc: Mali LaGoe <mlagoe@scottsvalley.gov>, Stephanie Hill <shill@scottsvalley.gov>

Dear Honorable Judge Cogliati and Members of the Santa Cruz County Grand Jury,

We have attached the completed response packet for the report titled *Cyber Threat Preparedness - Phishing and Passwords and Ransomware, Oh My!* This report was approved by the Scotts Valley City Council at the regular public meeting held on August 2, 2023.

Please confirm receipt of the report.

Best regards,

Cathie Simonovich
City Clerk

City of Scotts Valley
1 Civic Center Drive
Scotts Valley, CA 95066
csimonovich@scottsvalley.gov
Phone: 831-440-5608

NOTE: ***My regular work schedule is Tuesday through Friday from 7:00 AM to 5:30 PM.***

2023-3dR_Cyber_ScottsValleyCC_Packet.pdf
252K

The 2022–2023 Santa Cruz County Civil Grand Jury

Requires the

Scotts Valley City Council

to Respond by August 16, 2023

to the Findings and Recommendations listed below which were assigned to them in the report titled

Cyber Threat Preparedness

Phishing and Passwords and Ransomware, Oh My!

Responses are **required** from elected officials, elected agency or department heads, and elected boards, councils, and committees which are investigated by the Grand Jury. You are required to respond and to make your response available to the public by the California Penal Code (PC) §933(c).

Your response will be considered **compliant** under PC §933.05 if it contains an appropriate comment on **all** findings and recommendations **which were assigned to you** in this report.

Please follow the instructions below when preparing your response.

Instructions for Respondents

Your assigned Findings and Recommendations are listed on the following pages with check boxes and an expandable space for summaries, timeframes, and explanations. Please follow these instructions, which paraphrase PC §933.05:

1. ***For the Findings, mark one of the following responses with an "X" and provide the required additional information:***
   a. **AGREE with the Finding**, or
   b. **PARTIALLY DISAGREE with the Finding** – specify the portion of the Finding that is disputed and include an explanation of the reasons why, or
   c. **DISAGREE with the Finding** – provide an explanation of the reasons why.

2. ***For the Recommendations, mark one of the following actions with an "X" and provide the required additional information:***
   a. **HAS BEEN IMPLEMENTED** – provide a summary of the action taken, or
   b. **HAS NOT YET BEEN IMPLEMENTED BUT WILL BE IN THE FUTURE** – provide a timeframe or expected date for completion, or
   c. **REQUIRES FURTHER ANALYSIS** – provide an explanation, scope, and parameters of an analysis to be completed within six months, or
   d. **WILL NOT BE IMPLEMENTED** – provide an explanation of why it is not warranted or not reasonable.

3. ***Please confirm the date on which you approved the assigned responses:***

   We approved these responses in a regular public meeting as shown in our minutes dated August 2, 2023.

4. ***When your responses are complete, please email your completed Response Packet as a PDF file attachment to both***

   The Honorable Judge Syda Cogliati Syda.Cogliati@santacruzcourt.org **and**

   The Santa Cruz County Grand Jury grandjury@scgrandjury.org.

If you have questions about this response form, please contact the Grand Jury by calling 831-454-2099 or by sending an email to grandjury@scgrandjury.org.

Findings

F15. Although Scotts Valley's managed service provider is very knowledgeable and capable of providing cybersecurity services, there is no single city official with cybersecurity oversight, potentially leading to a poor understanding of the threats and an inadequate response to a cyber attack.

__ AGREE

__ PARTIALLY DISAGREE

_X_ DISAGREE

Response explanation (required for a response other than **Agree**):

We agree that the Scotts Valley managed service provider is very knowledgeable and capable of providing cybersecurity services. In addition, the Administrative Services Director overseas the City's managed services provider contract including cybersecurity services. The Administrative Services Director and City Manager meet at least monthly with the managed service provider where reports of phishing, cyber incidents and training statistics are reviewed and discussed. In the event of an immediate threat or incident, there is immediate communication between the managed service provider, City Manager, and Administrative Services Director. The City Manager and Administrative Services Director have an appropriate understanding of the potential cybersecurity threats and the managed service provider ensures the City has the tools in place to respond to a cyber attack. Therefore we disagree that our organizational structure as the potential to lead to a poor understanding or inadequate response to a cyber attack.

F16. Scotts Valley does not have a current Cybersecurity Plan that defines security policies, procedures, and controls required to protect its networks and devices, potentially increasing the risks of vulnerabilities.

_X_ AGREE

__ PARTIALLY DISAGREE

__ DISAGREE

Response explanation (required for a response other than **Agree**):

F17. Scotts Valley does not have a current Incident Response Plan, which could exacerbate the effects of a cyber incident such as increase the time a network is unavailable or raise the potential financial costs of a resolution.

__ **AGREE**

_X_ **PARTIALLY DISAGREE**

__ **DISAGREE**

Response explanation (required for a response other than **Agree**):

Although the City does not have a written Incident Response Plan, we have reporting channels in place in the event of a cyber incident and access to a cybersecurity response consultant via our risk management insurance pool who is under contract to provide cybersecurity incident response and maintains plans accordingly.

F18. Scotts Valley does not participate in any cybersecurity information sharing groups to enhance best practices, rather they depend on their contractor to stay informed, which makes the City last to know of critical cyber threats.

__ **AGREE**

_X_ **PARTIALLY DISAGREE**

__ **DISAGREE**

Response explanation (required for a response other than **Agree**):

Via the City's insurance pool, MBASIA, cybersecurity information is shared among the 10 city members and our contracted risk management consultants. In addition, our managed service provider stays informed of the cybersecurity environment and alerts the City of potential threats. The City's relationship with a contracted managed service provider does not make the City any less informed or more vulnerable. In fact the team we are served by is more informed and provides a broader skillset, knowledge base and faster response times than we could expect if the contract was replaced by 1-2 City staff. That being said, there are always more opportunities for information sharing and collaboration which the City, via it's managed service provider, will pursue.

Recommendations

R15. By mid-2023, Scotts Valley should assign a city official as the lead for cybersecurity for the city. This individual should oversee the contractor's performance in cybersecurity and ensure city leaders are well informed on emerging threats, cybersecurity challenges, and information provided from regional and state entities. (F15)

__ **HAS BEEN IMPLEMENTED –** summarize what has been done

__ **HAS NOT YET BEEN IMPLEMENTED BUT WILL BE IN THE FUTURE –** summarize what will be done and the timeframe

__ **REQUIRES FURTHER ANALYSIS –** explain the scope and timeframe (not to exceed six months)

_X_ **WILL NOT BE IMPLEMENTED –** explain why

Required response explanation, summary, and timeframe:

The City already oversees the managed service provider's performance via the Administrative Services Director and City Manager.

R16. Working with its IT contractor, by Fall 2023, Scotts Valley should write and implement a Cybersecurity Plan that is shared with all city officials to demonstrate comprehensive security measures and executive-level cyber threat awareness. (F16)

__ **HAS BEEN IMPLEMENTED –** summarize what has been done

_X_ **HAS NOT YET BEEN IMPLEMENTED BUT WILL BE IN THE FUTURE –** summarize what will be done and the timeframe

__ **REQUIRES FURTHER ANALYSIS –** explain the scope and timeframe (not to exceed six months)

__ **WILL NOT BE IMPLEMENTED –** explain why

Required response explanation, summary, and timeframe:

The City will work with the managed service provider in developing a written Cybersecurity Plan by 11/30/2023. The plan will be shared with those who need to know and have a role in implementing security measures. The plan will not be publicly shared or available due to its sensitive nature.

R17. By Fall 2023, Scotts Valley should write an Incident Response Plan that clearly delineates the steps it will take in response to a cyber attack, the responsibilities of identified officials, and the coordination required with state and federal officials for each type and level of cyber attack. (F17)

__ **HAS BEEN IMPLEMENTED –** summarize what has been done

_X_ **HAS NOT YET BEEN IMPLEMENTED BUT WILL BE IN THE FUTURE –** summarize what will be done and the timeframe

— **REQUIRES FURTHER ANALYSIS –** explain the scope and timeframe (not to exceed six months)

__ **WILL NOT BE IMPLEMENTED –** explain why

Required response explanation, summary, and timeframe:

The City will work with our managed service provider and cyber insurance consultant to develop a written Incident Response Plan by 11/30/2023.

R18. Scotts Valley should participate in local, regional, and state cybersecurity organizations for information sharing by the end of 2023. (F18)

__	**HAS BEEN IMPLEMENTED –** summarize what has been done
_X_	**HAS NOT YET BEEN IMPLEMENTED BUT WILL BE IN THE FUTURE –** summarize what will be done and the timeframe
__	**REQUIRES FURTHER ANALYSIS –** explain the scope and timeframe (not to exceed six months)
__	**WILL NOT BE IMPLEMENTED –** explain why

Required response explanation, summary, and timeframe:

The City will work with the managed service provider in identifying and selecting appropriate organizations to share cybersecurity information with by 11/30/2023.