The 2022–2023 Santa Cruz County Civil Grand Jury

Requires the

Capitola 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 _____.

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

F19. With one individual responsible for IT services, Capitola does not allocate sufficient resources to cybersecurity, a status that could lead to poor cyber knowledge and unnecessary vulnerabilities.

__ **AGREE**

__ **PARTIALLY DISAGREE**

_X_ **DISAGREE**

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

The City of Capitola allocates sufficient resources to cybersecurity. The City employs an Information Systems Specialist in the City Manager Department and holds a contract with Exceedio for 24-hour technical support, analysis, and security.

F20. The City of Capitola does not have a robust cybersecurity training program, nor does it conduct phishing tests or routinely remind employees to adhere to cybersecurity measures during potential periods of increased threats.

__ **AGREE**

X__ PARTIALLY DISAGREE

__ **DISAGREE**

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

The City is currently working to address the need for robust employee cybersecurity training. At present, the following is in place:
1. Capitola Police Department mandates twice-annual security awareness training for their IT, Captain & Chief, Officers, and Records Staff, as well as Public Works staff, the Volunteers in Policing (VIPs), and cleaning staff.
2. All City employees are required to complete “Email and Messaging Safety” training on an annual basis.

The City is developing new additions to the training plan, such as:
1. The City’s Information Systems Specialist is developing regular phishing tests to be sent to all employees on a rolling basis, with further help and training available to those employees who ‘fail’ phishing tests.
2. The City’s Information Systems Specialist is implementing mandatory cyber security training as a part of New Employee Onboarding that must be completed prior to new employees’ gaining access to the City’s network, shared files, internet, and email.

F21. The City of Capitola does not have a Cybersecurity Plan to address cybersecurity measures city wide, suggesting the city is not adequately mitigating the potential impact of cyber incidents.

__ **AGREE**

__ **PARTIALLY DISAGREE**

_X_ **DISAGREE**

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

Capitola Police Department has adopted Policy Section 806.11 regarding Information Technology and Cybersecurity.

The City has a functioning cybersecurity plan that addresses security concerns and outlines a response plan to a security breach. Staff is also working with the Santa Cruz County Cyber Security Consortium to draft a more comprehensive Cybersecurity Plan template that can be modified for each jurisdiction.

F22. The City of Capitola does not have an 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**

__ **PARTIALLY DISAGREE**

_X_ **DISAGREE**

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

The City has a Cyber Attack Response plan in place. The plan is modified and updated annually by the Information Systems Specialist.

F23. Capitola does not participate in any cyber-focused information sharing groups, nor does it take advantage of state and federal resources designed to assist small cities with mitigating cyber attacks, thereby forfeiting opportunities to learn best practices and raise their cyber awareness.

__ **AGREE**

__ **PARTIALLY DISAGREE**

_X_ **DISAGREE**

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

The City's Information Systems Specialist participates in:

1. Cyber threat meetings sponsored by Alverez Technology Group
2. NCRIS.ca.gov Regional Information Center meetings regarding cyber threats
3. MISAC.org
4. Santa Cruz County Cyber Security Consortium

Recommendations

R19. By Fall 2023, Capitola should hire a full-time IT Director to replace the IT Director who departed in mid-2022. The IT Director should oversee and expand IT services, including those of the consulting company, and lead cybersecurity initiatives. (F19)

__ **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 has never employed an IT Director and does not intend to create/fill such a position.

R20. The City should develop a more robust cybersecurity training and phishing testing program for all employees by Fall 2023 or earlier. (F20)

X__	**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)
___	**WILL NOT BE IMPLEMENTED –** explain why

Required response explanation, summary, and timeframe:

The City is currently working to address the need for robust employee cybersecurity training:
1. Capitola Police Department mandates twice-annual security awareness training for their IT, Captain & Chief, Officers, Records Staff, as well as Public Works staff, the Volunteers in Policing (VIPs), and cleaning staff.
2. All employees are required to complete “Email and Messaging Safety” training on an annual basis.
3. The City’s Information Systems Specialist is developing regular phishing tests to be sent to all employees on a rolling basis, with further help and training available to those employees who ‘fail’ phishing tests.
4. The City’s Information Systems Specialist is considering including mandatory cyber security training to New Employee Onboarding that must be completed prior to new employees’ gaining access to the City’s network, shared files, internet, and email.

R21. Capitola should establish and implement a Cybersecurity Plan by the end of 2023. Several resources exist to provide a foundation or templates for these plans including NIST Guidelines, CISA resources, and Cal-CSIC guidance. (F21)

__ **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 of Capitola is working with regional entities as a member of the newly formed Santa Cruz County Cyber Security Consortium. One of the group's main goals is to develop a Cyber Security Plan that can be modified for each individual organization.

R22. By Fall 2023 Capitola should prepare an Incident Response Plan that provides detailed guidance for a city response to a cyber attack. (F22)

__	**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 of Capitola is working with the regional entities as a member of the newly formed Santa Cruz County Cyber Security Consortium. One of the group's main goals is to develop a Cyber Security Plan, including an Incident Response Plan, that can be modified for each individual organization.

R23. When appropriately resourced to monitor cyber threats, and by the end of 2023, Capitola should participate in regional cybersecurity information sharing groups, to gain valuable information to best protect the City. (F23)

_X_ **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)

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

Required response explanation, summary, and timeframe:

The City's Information Systems Specialist currently participates in the regional cybersecurity information-sharing groups listed below and will continue to do so.

1. Santa Cruz County Cyber Security Consortium
2. Cyber threat meetings sponsored by Alverez Technology Group
3. NCRIS.ca.gov Regional Information Center
4. MISAC.org

R24. By mid-2023, Capitola city management should raise the priority it assigns to cybersecurity and demonstrate a recognition of their role in ensuring the security of the City's information networks.(F19–F23)

_X_ **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)

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

Required response explanation, summary, and timeframe:

The City Manager Department has increased prioritizing Information Technology and cybersecurity by:

1) Budgeting $250,000 towards information technology and cyber security
2) Joining the Santa Cruz County Cyber Security Consortium
3) Increasing employee training, for example with an annual Email and Messaging Safety training and more in-depth Anti-phishing training
4) Drafting a more comprehensive Cybersecurity Plan template with the assistance of the SCC Cyber Security Consortium