SANTA CRUZ COUNTY GRAND JURY

Grand Jury <grandjury@scgrandjury.org>

Revised Board of Supervisors Response to 2022-2023 Grand Jury Report

Caitlin Smith <Caitlin.Smith@santacruzcountyca.gov> Tue, Oct 3, 2023 at 2:12 PM

Good Afternoon,

Please see attached for the revised Board of Supervisors response to the 2022-2023 Grand Jury Report "Cyber Threat Preparedness". As you may recall, the original response was approved by the Board on August 8th and this revised response was approved on September 19th.

Best,

Caitlin C. Smith

County Supervisors' Analyst

Santa Cruz County Board of Supervisors

701 Ocean Street, Room 500

Santa Cruz, CA 95060

831-454-2200 main

831-454-3516 direct

caitlin.smith@santacruzcountyca.gov

To email all five members of the Board of Supervisors at once,

please use: boardofsupervisors@santacruzcountyca.gov

Revised Board of Supervisors Response to Grand Jury Report Cyber Threat Preparedness.pdf
249K

County of Santa Cruz

BOARD OF SUPERVISORS

701 OCEAN STREET, SUITE 500, SANTA CRUZ, CA 95060-4069
(831) 454-2200 • FAX: (831) 454-3262 TDD/TTY - Call 711

MANU KOENIG	ZACH FRIEND	JUSTIN CUMMINGS	FELIPE HERNANDEZ	BRUCE MCPHERSON
FIRST DISTRICT	SECOND DISTRICT	THIRD DISTRICT	FOURTH DISTRICT	FIFTH DISTRICT

September 29, 2023

The Honorable Syda Cogliati
Santa Cruz Courthouse
701 Ocean Street
Santa Cruz, CA 95060

RE: Revised Response to the 2022-2023 Grand Jury Report "Cyber Threat Preparedness"

Dear Judge Cogliati:

The purpose of this letter is to formally transmit the revised response of the Santa Cruz County Board of Supervisors to the 2022-2023 Grand Jury Report "Cyber Threat Preparedness".

Sincerely,

ZACH FRIEND, Chair
Board of Supervisors

ZF: cs
Attachment

CC: Clerk of the Board
Santa Cruz County Grand Jury

The 2022–2023 Santa Cruz County Civil Grand Jury

Requires the

Santa Cruz County Board of Supervisors

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 September 19, 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

F1. Santa Cruz County does not have a Cybersecurity Plan, and the absence of a current plan that defines security policies, procedures, and controls required to protect its networks and devices increases the risk of vulnerabilities.

_x_ AGREE

__ PARTIALLY DISAGREE

__ DISAGREE

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

In 2019, the County developed an Incident Response Plan for Cyber events and is working on establishing a more formal Cybersecurity Plan that addresses emerging threats and responses. The County has reached out to the four cities and Santa Cruz Regional 911 (SCR911) to convene a regional Cybersecurity Consortium to take a regional approach to developing Cybersecurity and incident response plans that can be leveraged for the individual needs and requirements of each participating agency. The plans will be completed before or by December 31, 2023

F2. Santa Cruz County does not have a sufficiently detailed Incident Response Plan, indicating they would not be prepared to respond rapidly and effectively in the event of a cyber incident.

_x_ AGREE

__ PARTIALLY DISAGREE

__ DISAGREE

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

In 2019, the County developed an Incident Response Plan for Cyber events and is working on establishing a more formal Cybersecurity Plan that addresses emerging threats and responses. The County is coordinating with the four cities and SCR911 to develop a regional plan that can be modified for the individual needs and requirements of each entity. The plans will be completed before or by December 31, 2023

F3. Santa Cruz County participates in multiple information sharing groups at regional and state levels, although it has only minimal interaction with the cities across Santa Cruz County, degrading their ability to fully understand regional vulnerabilities.

__ AGREE

_x_ PARTIALLY DISAGREE

__ DISAGREE

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

The County has reached out in the past to inform cities of Cybersecurity resources, such as the Northern California Regional Intelligence Center and Urban Areas Security Initiative Program. A more formal information sharing has been established through a regional Cybersecurity Consortium to promote and encourage communication and resources. The Consortium began meeting on June 12, 2023.

Recommendations

R1. Santa Cruz County should prepare and implement a Cybersecurity Plan by the end of 2023, ensuring that city officials and all staff are well aware of the plan details, their responsibilities, and associated policies. (F1)

__	**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 County has reached out to the four cities and SCR911 to convene a regional Cybersecurity Consortium to take a regional approach to developing Cybersecurity and incident response plans that can be leveraged for the individual needs and requirements of each participating agency. The plans will be completed before or by December 31, 2023

R2. By the end of 2023, the county should revise and expand its Incident Response Plan to clearly delineate 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. A detailed plan is a requirement for continuity of county operations in a cyber incident. (F2)

__	**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 County is coordinating with the four cities and SCR911 to develop a regional plan that can be modified for the individual needs and requirements of each entity. The plan will provide clear delineated steps for the County to respond to a cyber-attack. The FY 2023-24 budget funds a position to establish a dedicated security analyst that will take on this work on behalf of the County. This will be completed by December 31, 2023

R3. The County's information sharing efforts should be expanded to ensure fulsome information sharing across all government entities in the county, specifically Santa Cruz, Watsonville, Scotts Valley, and Capitola, by the end of 2023. A simple schedule of monthly meetings would permit regular sharing of possible threats, TTPs seen across the county, and information learned from outside organizations such as the Cal-CSIC. (F3)

_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:

On June 12, 2023, a regional Cybersecurity group was formally convened. The focus of the group will be to develop the Cybersecurity policy and plans, along with an incident response plan as noted above. The Santa Cruz Cybersecurity Consortium will meet regularly on at least a monthly basis going forward to look at iterative changes needed for policy and discuss regional approaches to mitigating emerging Cybersecurity threats.