CITY OF STOCKTON

OFFICE OF THE CITY MANAGER
City Hall • 425 N. El Dorado Street • Stockton, CA 95202-1997 • 209 / 937-8212 • Fax 209 / 937-7149
www.stocktonca.gov

September 14, 2022

Honorable Michael D. Coughlan, Presiding Judge
San Joaquin County Superior Court
180 E. Weber Avenue, Suite 1306J
Stockton, CA 95202

CITY OF STOCKTON RESPONSE TO SAN JOAQUIN COUNTY GRAND JURY 2021-2022 CASE NO. 0321 SAN JOAQUIN COUNTY AND ITS SEVEN CITIES: CYBERSECRUITY: LOCAL DEFENSE AGAINST A GLOBAL THREAT

The City of Stockton received the Grand Jury Report on June 16, 2022, regarding findings and recommendations related to Cybersecurity in San Joaquin County and the seven incorporated cities within the county. In general, the City agrees with the findings and is providing additional information in the below responses to the findings and recommendations.

In accordance with Sections 933 and 933.05 of the California Penal Code, the City Council of the City of Stockton offers the following responses to the Grand Jury Report on the above-referenced case. As referenced under *Response Requirements*, the Stockton City Council is responding to the Findings and Recommendations F7.1, F7.2, and R7.1.

Findings:

F7.1 *The City of Stockton does not have a formal internal policy concerning payments or procedures in ransomware attacks. This absence of policy could cause confusion, delay and greater loss of security in the event of an attack.*

RESPONSE:

The City agrees with this finding.

F7.2 *The City of Stockton has a large IT Department which places cybersecurity and disaster preparedness at a high priority, minimizing risk to the City's information and service systems.*

RESPONSE:

The City agrees with this finding.

Recommendations:

R7.1 *By November 1, 2022, the Stockton City Council, in conjunction with the City's IT department, develop, adopt and implement a formal internal policy and procedure for response to a ransomware attack.*

RESPONSE:

A formal internal policy and procedure for response to a ransomware attack was approved by the City Manager on September 1, 2022, and presented to the City Council at its September 13, 2022 public meeting. The approved policy is attached.

HARRY BLACK
CITY MANAGER

Attachment

MEMORANDUM

September 14, 2022

TO: Ms. Trisa Martinez, Staff Secretary to the Grand Jury

FROM: Jay Kapoor, Deputy City Manager

SUBJECT: **CITY OF STOCKTON RESPONSE TO FINDINGS IN CASE #0321**

During its September 13, 2022 public meeting, the City Council, via Motion 2022-09-13-1204: (1) approved the City's proposed responses to the findings and recommendations contained in the San Joaquin County Grand Jury report titled "*San Joaquin County and Its Seven Cities: Cybersecurity: Local Defense Against a Global Threat – Case #0321*; and (2) directed the City Manager to sign the response on behalf of the City Council and transmit the response to the Presiding Judge of the San Joaquin County Superior Court.

As such, pursuant to Sections 933 and 933.05 of the California Penal Code, the City of Stockton is transmitting the following enclosed documents in response to the Grand Jury report:

- Grand Jury response letter addressed to Judge Coughlan, signed by City Manager Harry Black.
- The City of Stockton's formal Ransomware Attack Response Policy effective September 1, 2022.
- Staff report recommending City Council approval of the City Manager's response letter to the Grand Jury, presented to Council at its September 13, 2022 public meeting (File #22-0738).

If you have any questions, please contact me at (209) 937-8212 or jay.kapoor@stocktonca.gov. Thank you.

JAY KAPOOR
DEPUTY CITY MANAGER
CITY OF STOCKTON

RANSOMWARE ATTACK RESPONSE POLICY 14.01.020

SUBJECT: RANSOMWARE ATTACK, INFORMATON SECURITY	**NUMBER:** 14.01.020
RESPONSIBLE OFFICER: City Manager	**EFFECTIVE DATE:** 09/01/2022
POLICY OWNER: Director of IT, Information Technology	**LAST UPDATED:** N/A
POLICY CONTACT: Director of IT, Information Technology	**APPROVED:**

POLICY

The purpose of this policy is to provide direction on the appropriate ransomware response if the City is faced with a ransomware attack.

Upon discovery that a ransomware attack is occurring or has occurred the Information Technology Department will take the following action:

1. Notify City Manager's Office
2. Notify City Attorney's Office
3. Notify the City Council
4. Contact appropriate Federal and State Law Enforcement agencies.
5. Contact Cyber Insurance Provider

If the attackers demand payment to recover files or to refrain from disseminating captured files to the public or by any other means tarnish the reputation or disrupt city operations, then the City Manager or designee in consultation with the stakeholders mentioned above will decide, based on the information and circumstances available, on what the appropriate response is to get the best outcome for the City.

RESPONSIBILITIES

Director of Information Technology

- Notify the City Manager's and the City Attorney's Offices
- Notify the appropriate Federal and State law enforcement agencies
- Contact the City's Cyber Insurance provider
- Provide situational updates to the City Manager

City Manager

- Notify the City Council
- In consultation with stakeholders, formulate the ransomware response plan.

City Council

- Provide the City Manager with the authority to enact the ransomware response plan.

City Attorney

- Consult with City Manager and City Council on legal aspects of ransomware response.
- Work with Public Information Officer and law enforcement on press releases.

Public Information Officer

- Work with City Attorney and law enforcement on information provided in press releases

Information Technology Department

- Work with cyber insurance providers experts to assist with containment and recovery
- Work with law enforcement agencies on evidence gathering
- Work with other third parties assisting with the ransomware incident, as defined in the Information Technology's document titled, *Cybersecurity Incident Response Playbook*

RELEVANT AUTHORITY

RELATED CITY POLICIES

Information Technology Management and Security Policy 14.01.010

RELATED CITY PROCEDURES

Cybersecurity Incident Response Playbook

RELATED FORMS, DOCUMENTS, OR LINKS

N/A

FREQUENTLY ASKED QUESTIONS

N/A

UPDATE HISTORY

09/01/2022 – *Established*

City of Stockton

Legislation Text

File #: 22-0738, **Version:** 1

APPROVE RESPONSES TO THE 2021-22 SAN JOAQUIN COUNTY GRAND JURY REPORT ON CYBERSECURITY, CASE NO. 0321

RECOMMENDATION

It is recommended that the City Council adopt by motion the City's responses to the 2021-22 Civil Grand Jury Report titled "San Joaquin County and Its Seven Cities: Cybersecurity: Local Defense Against a Global Threat," Case No. 0321, and direct the City Manager to sign the response on behalf of the City Council and transmit the response to the Presiding Judge of the San Joaquin County Superior Court.

Summary

Each year it is the duty of the San Joaquin Civil Grand Jury to examine and investigate the activities of local governments within San Joaquin County. The 2021-22 Civil Grand Jury of San Joaquin County conducted three new investigations, of which one investigation requires a response from the City. California Penal Code sections 933 and 933.05 require a response to the Presiding Judge of San Joaquin County Superior Court by September 15, 2022, to comply with the 90 days allotted to the City as a response time. A letter has been prepared for Council consideration that is responsive to the investigation.

DISCUSSION

Background

The 2021-22 Civil Grand Jury Report Investigation Case No. 0321 on Cybersecurity included several countywide findings and recommendations. Two findings and one recommendation were assigned to the City of Stockton. This report was received by the City of Stockton on June 16, 2022 (Attachment A). The Grand Jury Report evaluates the current state of digital security and disaster preparedness of the Information Technology systems of San Joaquin County and the seven incorporated cities within the county.

Present Situation

Pursuant to California Penal Code 933 and 933.05, written responses have been prepared for submittal to the Presiding Judge of the Superior Court of San Joaquin County (Attachment B).

The Information Technology Department has reviewed the Grand Jury findings and recommendation related to the report on Cybersecurity, Case No. 0321. The Grand Jury found that the City met all cybersecurity expectations except for the presence of a documented internal policy and procedure for response to a ransomware attack, but acknowledged that the City has a Cybersecurity Incident

Response Book detailing response procedures for other cyber events. Staff agree with the findings and recommendation as published, and a formal Ransomware Attack Response Policy for the City was subsequently developed and approved by the City Manager on September 1, 2022 (Attachment C), which complies with the Grand Jury Report's deadline of November 1, 2022. The adopted policy will be transmitted to the Grand Jury along with the City's response letter.

FINANCIAL SUMMARY

There is no financial impact in submitting this response letter to the Presiding Judge of the San Joaquin Superior Court.

Attachment A - Grand Jury Report on Cybersecurity, Case No. 0321
Attachment B - City of Stockton Response Letter, Case No. 0321
Attachment C - City of Stockton Ransomware Attack Response Policy