TOWN OF
SAN ANSELMO
EST. 1907

525 San Anselmo Avenue, San Anselmo, CA 94960-2682
(415) 258-4600 | Fax (415) 459-2477
www.townofsananselmo.org

July 28, 2020

The Honorable Judge Kelly V. Simmons
Marin County Superior Court
P.O. Box 4988
San Rafael, CA 94913-4988

Dear Judge Simmons:

The Town of San Anselmo has received the Grand Jury Report "Cyberattacks: A Growing Threat to Marin Government" dated May 11, 2020. The Grand Jury has requested a response to Findings F3-F10 and Recommendations R4-R9. The report was reviewed and considered by the San Anselmo Town Council at the July 28, 2020 regular meeting. Enclosed please find the Town's response.

Should the members of the Grand Jury require any additional information, please contact Town Manager David Donery at ddonery@townofsananselmo.org.

Sincerely,

Ford Greene
Mayor

Enclosure

Cc: Lucy Dilworth, Foreperson

RESPONSE TO GRAND JURY REPORT FORM

Report Title: Cyberattacks: A Growing Threat to Marin Government

Report Date: May 11, 2020

Response By: San Anselmo Town Council

Response Date: July 28, 2020

FINDINGS:

- We agree with the findings numbered F7 & F8
- We disagree wholly or partially with the findings numbered F3, F4, F5, F6, F9, F10

RECOMMENDATIONS:

- Recommendations numbered NA have been implemented.
- Recommendations numbered R4, R5, R6, R9 have not yet been implemented, but will be implemented in the future.
- Recommendations numbered NA has been partially implemented, and remaining parts will be implemented in the future.
- Recommendations numbered R7, R8 has been partially implemented, other parts will be implemented in the future, and parts require further analysis.
- Recommendations numbered NA will not be implemented because they are not warranted or are not reasonable.

Dated: _____ Signed: _____

Ford Greene, Mayor

RESPONSE OF THE TOWN OF SAN ANSELMO TO GRAND JURY REPORT "CYBERATTACKS: A GROWING THREAT TO MARIN GOVERNMENT"

FINDINGS AND RESPONSES

F3. Transparency is lacking regarding cybersecurity because past breaches have not been publicly disclosed, and city and town councils have not facilitated public discussion of cybersecurity issues.

Disagree. In the case of San Anselmo, the Town of San Anselmo has not experienced a security breach that would require public disclosure.

F4. Most elected officials in Marin's cities and towns are not sufficiently engaged in ensuring robust cybersecurity policies and procedures are in place.

Disagree. This is a general statement concerning most elected officials in Marin cities and towns. Some elected officials in Marin are sufficiently engaged and some are likely not in cybersecurity policies. The Town of San Anselmo will not comment on the findings asserting practices of other cities and towns.

For San Anselmo, our Council make policy and procedure decisions for cybersecurity. For example, at the last IT agreement renewal in 2017, Council approved installing monitoring agents on all the machines, as well as SNMP (Simple Network Management Protocol) monitoring for all networking devices on the network back-end. The agents are active 24/7 and provide Marin IT with critical information on the current state of devices (such as computers, laptops, iPads, etc, that have an active user profile in our system), so issues can be monitored, discovered, and dealt with remotely on the days that IT personnel are not on-site. Our Council also made the decision to utilize MIDAS and the expertise of a larger conglomerate for network protocols.

F5. County and municipal officials and managers have been generally unaware of breaches that have occurred outside their own agencies in Marin and therefore have not felt the need to collaborate on measures to improve cybersecurity.

Disagree partially. The Town of San Anselmo has not consistently been made aware of breaches outside of our agency. However, issues of cybersecurity have been discussed by the Marin Managers Association.

F6. Municipalities have been lax in following FBI guidance that cybersecurity breaches be reported to federal law enforcement.

Disagree. The Town of San Anselmo has not experienced a cybersecurity breach that would have been required to be report to federal law enforcement.

F7. Marin's cities and towns have not made a concerted effort to standardize around a common set of best practices with respect to cybersecurity.

Agree. The Town of San Anselmo agrees more can be done to share cybersecurity best practices. While the strategy and approach to cybersecurity in Marin cities and towns have not been standardized amongst all jurisdictions, most of the cities and towns utilizing the MIDAS network share the network security protocols in place for MIDAS and a number of cities and towns have relied on a common service provider to implement local network security solutions through Marin IT. The Town of San Anselmo will work with the most recently formed Marin

Information Security Collaboration (MISC) between Marin County regional agencies to develop best practices for cybersecurity.

F8. The Marin County Council of Mayors & Councilmembers has not made cybersecurity a priority, which has minimized the awareness and engagement of elected officials in cybersecurity matters.

Agree. However, Individual Councils and/or Councilmembers may be aware and engaged in cybersecurity.

F9. The Marin Managers Association has not done enough to facilitate the sharing of cybersecurity information and resources among its members.

Disagree. In December 2019, the City of San Rafael made a presentation to the Marin Managers Association about a recent overhaul of the IT delivery service model, including cybersecurity.

F10. Various low-cost best practices exist that could, if implemented, significantly improve the cybersecurity posture of Marin's cities and towns.

Disagree partially. It is possible that low-cost best practices may exist; however, until staff has researched all of the options with MISC and Marin IT, this statement cannot be fully determined.

RECOMMENDATIONS AND RESPONSES

R4. Starting in fiscal year 2020–2021, the county board of supervisors and the city and town councils should request their managers report, at least annually, regarding their cybersecurity profile and any measures being taken to improve it.

This recommendation will be implemented in the future.

R5. Starting in fiscal year 2020–2021, the county, cities, and towns should convene periodic discussions, at least annually, in a public forum such as a board or council meeting, regarding the importance of good cybersecurity practices for our government, residents, and other organizations.

This recommendation will be implemented in the future. The Central Marin Police Department periodically sends out public communications about known email and internet scams to our residents and staff. Also, starting in October 2020, the County of Marin will host an event that is open to members of the public to facilitate a discussion on cybersecurity. As a member of the recently formed Marin Information Security Collaboration (MISC), San Anselmo will help promote this event to our residents and organizations.

R6. The county and each city and town should adopt a policy to report to federal law enforcement any cybersecurity intrusion that results in financial fraud or unauthorized disclosure of information and make that intrusion public.

This recommendation will be implemented in the future.

The Town of San Anselmo has not had any security breaches, financial fraud or unauthorized disclosure of information that would have required the reporting to federal law enforcement. If the Town were to become the victim to any of the above attacks, staff would work closely with all law enforcement, as required to properly respond to the threat.

The County of Marin has access to existing security policy templates that have been developed in collaboration with California Counties Information Services Director's Association (CCISDA) Information Security Council (ISC). These templates will be shared with the members of the recently formed Marin Information Security Collaboration (MISC) and will be considered for updates to the Town's own security policies.

R7. Within 180 days of the date of this report, cities and towns should implement the first four practices described in the Best Practices section of this report, regarding mandatory user training, email flagging and filtering, password management, and backup.

These recommendations have been implemented: Daily backup, email flagging and filtering.

These recommendations have been partially implemented and require further analysis: Employee training and password management. Employees receive examples of recent phishing attempts and fraudulent emails on a regular basis. Password management is used for some programs. Network security is currently managed by Marin IT, who manages and responds to threats and provides backups of Town files and servers.

For other recommendations to be implemented, staff will determine what timeframe is feasible to implement with some likely extending beyond the timeframe stated in R7.

R8. In fiscal year 2020–2021, cities and towns should complete an analysis of the feasibility of implementing the remainder of the practices described in the Best Practices section of this report.

These recommendations have been implemented: Automated malware detection and removal, firewalls and monitoring systems, requiring the use of virtual private network for personal computers, and an equipment replacement schedule.

Some measures require further analysis and more funding than is currently available, however, we are committed to implementing as many of the best practices as is financially feasible.

R9. In fiscal year 2020–2021, cities and towns should, through the Marin Managers Association, complete an analysis of the feasibility of contracting with a cybersecurity expert to be available to cities and towns on a shared basis, in order to raise the overall level of cybersecurity in Marin's cities and towns.

This recommendation will be implemented in the future.

The Town Manager will work with the Marin Managers Association to discuss shared resources such as a shared cybersecurity firm.