RESPONSE TO GRAND JURY REPORT FORM

Report Title: **Cyberattacks: A Growing Threat to Marin Government**

Report Date: **May 11, 2020**

Response By: **Fairfax Town Council**

Response Date: **August 5, 2020**

FINDINGS:

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

RECOMMENDATIONS:

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

DATED: _____ Signed: _____
Michele Gardner, Town Clerk

Number of pages attached: 4

ATTACHMENT A

RESPONSE OF THE TOWN OF FAIRFAX 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.

Response: Agree.

The Town of Fairfax 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.

Response: Disagree partially. This is a general statement and some elected officials in Marin are sufficiently engaged and some are likely not in cybersecurity policies.

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.

Response: Disagree partially. Fairfax has not consistently been made aware of breaches outside of our agency. However, issues of cybersecurity have been discussed by the Marin Managers Association. In addition, cybersecurity issues, such as breaches, have also been discussed at meetings of the Town's insurance pool, Bay Cities Joint Insurance Powers Authority (BCJPIA), in which the Town is an active board member. BCJPIA has members agencies (i.e., cities, towns, JPAs) throughout northern California.

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

Response: Disagree. The Town has not experienced a cybersecurity breach that would have been required to be reported to federal law enforcement. The Town maintains Department of Justice compliant network connectivity to serve our Police Department.

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.

Response: Agree. The Town of Fairfax 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. Fairfax will work with the recently formed Marin Information Security Collaboration (MISC) between Marin County regional agencies to develop and share 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.

Response: Agree. However, individual Councils and/or Councilmembers are 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.

Response: Disagree. In December 2019, the City of San Rafael made a presentation to the Marin Managers Association about a recent overhaul of their IT service delivery model including cybersecurity. Their presentation included a consultant they hired to conduct an assessment of their service model and the president of the company who manages their cybersecurity.

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

Response: Agree.

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.

Response: 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.

Response: This recommendation will be implemented in the future.

Starting in October 2020, the County of Marin will host an NCSAM 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), Fairfax 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.

Response: This recommendation will be implemented in the future.

The Town of Fairfax has not had any recent cybersecurity breaches, financial fraud, or unauthorized disclosure of information that have required the reporting to federal law enforcement. If the Town were to become victim to any of the above attacks staff would work closely with all law enforcement personnel, including federal 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 the 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.

Response: These recommendations have been implemented: daily backup, some password management practices, and filtering.

These recommendations to be implemented in the future: Email flagging, additional password management, and employee training.

Staff agrees that implementation of the first four practices listed are measures that would strengthen security, and the Town has conducted daily backups with regular testing and filtering for years. Also, some aspects of the best practices for password management has been implemented for years such as requiring passwords to be changed every 90 days. For the other recommendations to be implemented, staff will determine the time and cost to do so. However, given our limited resources, it is likely the Town will need more than 180 days to implement all these best practices.

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, monitoring systems.

These recommendations have been partially implemented:

Use of expert resources, firewalls, hardware and patching.

These recommendations require further analysis:
Management of mobile devices, documentation, vulnerability assessments.

Staff will need to further study this recommendation to determine if resources can be allocated to complete these tasks in Fiscal Year 2020-21.

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.

Response: This recommendation has not yet been implemented but will be implemented in the future.

The Fairfax Town Manager will work with the Marin Managers Association to add the consideration of hiring a cybersecurity firm to the list of potential shared services that is currently in development.