San Mateo Union High School District

Kevin Skelly, Ph.D., Superintendent
Elizabeth McManus, Deputy Superintendent Business Services
Kirk Black, Ed.D., Deputy Superintendent Human Resources and Student Services
Julia Kempkey, Ed.D. Assistant Superintendent of Curriculum and Instruction

December 17, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

Re: Response to the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected."

Dear Judge Chou:

The San Mateo Union High School District has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board of Trustees approved these responses, on December 17, 2020

Findings:

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

The District agrees with this Finding.

2. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. *The direct and indirect costs of Ransomware can be significant.*

The District agrees with this Finding.

4. *Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.*

The District agrees with this Finding.

5. *A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.*

The District agrees with this Finding.

6. *The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.*

The District agrees with this Finding.

7. *Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.*

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

8. *Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.*

The District agrees with this Finding.

Recommendations:

1. *Each of the governmental entities in San Mateo County with an IT department or IT function (whether in-house, handled by another government unit or outsourced to a private enterprise) as listed in Appendix F, should by November 30, 2020, make a request for a report from their IT organization that addresses the concerns identified in the report, specifically:*
    a. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
    b. *Backup & Recovery (In the event of an attack, can you shut down your system quickly? What is being backed up, how it is being backed up, when are backups run, and where are the backups being stored? Have backups been tested? Can you fully restore a Server from a backup?)*
    c. *Prevention (turning on email filtering, setting up message rules to warn users, providing employee training on phishing and providing a reporting system to flag suspect content)*

SMUHSD implemented this Recommendation on November 2, 2020 by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

SMUHSD has the following in place: Router, Firewall, and Layer 3 switches that minimize potential cyber threats. SMUHSD also updates critical updates to servers and network equipment as they become available. Regular patches/updates will be applied after a minimum

of 30 days waiting period.

SMUHSD has malware and phishing detection in place through Gmail. The District will continue to monitor email threats such as phishing and other malware and provide informative warning to the District's end users annually and when necessary.

By June 2021, SMUHSD will implement a "force" password change and implement a stronger password policy.

SMUHSD backups use CBT (change base tracking) which minimizes the amount of time it takes for the backup process to complete, the retention policy for both schedules is two weeks. We receive notification of backup status daily and we can go back and check data for integrity which we will do monthly. We are currently backing up 30TB of district data which includes the SIS, and various other file servers.

Our Restore option gives us the ability to restore virtual machines from two weeks prior to any problem. We also have the ability to do a granular file restore of a virtual machine which means that we can mount the backup image and go and retrieve a file from a particular day for up to two weeks. The Sandbox feature allows us to run a machine in protected mode to ensure that the backup is safe before we restore it.

To date we have not performed a full backup of our data, but we have explored all the features mentioned above and are knowledgeable on how to proceed if the need arises. We will be scheduling a disaster drill once every two to three months and Data recovery drills monthly to ensure all parties are capable of doing this in a crisis situation.

By Summer of 2021, SMUHSD will implement offsite storage. The purpose of an offsite storage is to provide another redundancy of our data environment in a worst case scenario. It would be beneficial to explore having an offsite solution to house a copy of our critical services in the event the data center is compromised or lost by some unforeseen event.

2. *These confidential internal reports should be provided to the governing body by June 30, 2021. This report should describe what actions have already been taken and which will be given timely consideration for future enhancements to the existing cybersecurity plan.*

The District intends to implement Recommendations that are not yet in place, provided that the District may require an extension of time (not to exceed six months) beyond June 30, 2021 depending on the scope, complexity, and feasibility of any recommended actions and/or enhancements.

3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

4. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

Please do not hesitate to contact me if you have questions or require additional information.

Sincerely,

Kevin Skelly Digitally signed by Kevin Skelly Date: 2020.12.11 14:56:23 -08'00'

Kevin Skelly, Ph.D.
Superintendent

San Mateo Union High School District