

RESPONSE TO SAN DIEGO COUNTY GRAND JURY REPORT FORM

Report Title: Cybersecurity In San Diego School Districts
Response Provided by: Richard O Roberts

What is a Compliant Response?

Penal Code § 933.05 is very specific in what is required in a response. First, a respondent must address the findings listed in the report. There are only two responses allowed by the penal code. However, additional information is required if the respondent disagrees with a finding. If a report only lists findings and there are no recommendations, a response agreeing or disagreeing with each finding is not necessary.

FINDINGS

For purposes of subdivision (b) of Penal Code § 933.05, the respondent shall report one of the following two actions regarding each finding.

The respondent agrees with the finding.

The respondent disagrees wholly or partially with the finding; in which case the **response shall specify the portion of the finding that is disputed and shall include an explanation of the reason(s) therefore.**

- I (we) **agree** with the finding(s) numbered: 1-7.
- I (we) **disagree** wholly or partially with the finding(s) numbered: _____.

Describe any portions of the finding(s) that are disputed or not applicable; include an explanation of the reason(s).

RECOMMENDATIONS

For purposes of subdivision (b) of Penal Code § 933.05, the respondent shall report one of the following four actions regarding each recommendation.

The recommendation has been implemented with a summary regarding the implemented action.
The recommendation has not yet been implemented , but will be implemented in the future, with a timeframe for the implementation .
The recommendation requires further analysis, with an explanation and the scope and parameters of an analysis or study, and a timeframe for the matter to be prepared for discussion. This timeframe shall not exceed six months from the date of publication of the grand jury's report.
The recommendation will not be implemented because it is not warranted or is not reasonable, with an explanation , therefore.

- Recommendations numbered 7 **have been** implemented.
(Describe the implemented actions.)
- Recommendations numbered 1-6 **have not yet been** implemented but will be implemented in the future, with a targeted completion date of see attached
Per Penal Code § 933.05(b)(2), a time frame for implementation must be included.
- Recommendations numbered _____ **require further analysis**. The further analysis will be completed by _____.
Describe the scope and parameters of an analysis or study, and a timeframe for the matter to be prepared for discussion by the officer or director of the agency or department being investigated or reviewed, including the governing body of the public agency when applicable. This timeframe shall not exceed six (6) months from the date of publication of the grand jury report.
- Recommendations numbered _____ **will not be** implemented because they are not warranted or are not reasonable.

Provide an explanation.

Signature: Michael J. R. [Signature]

Date: 7-16-2024

Number of pages attached 5.

INSTRUCTIONS FOR RESPONDENTS

The legal requirements affecting respondents and responses to Grand Jury findings and recommendations are contained in California Penal Code § 933.05. The full text of the law is provided at the end of this document.

Two different time periods for responses, and to whom you must respond is defined in California Penal Code § 933(c). They are as follows:

Type of Agency	Time Frame	To Whom
Government Boards	Ninety (90) Days	<ul style="list-style-type: none">• Presiding Judge of the Superior Court
Elective Office or Agency Head	Sixty (60) Days	<ul style="list-style-type: none">• Presiding Judge of the Superior Court• Information copy to Board of Supervisors

An original signed copy of the response must be provided to both of the following:

1. Presiding Judge of the San Diego County Superior Court at the address listed below:

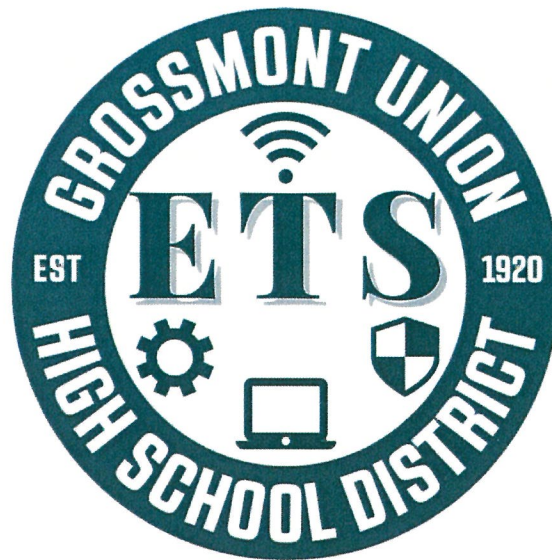
The Honorable Maureen F. Hallahan
Presiding Judge of the Superior
Court County of San Diego
P.O. Box 122724
San Diego, CA 92112-2724

2. San Diego County Grand Jury at the address listed below:

San Diego County Grand Jury
550 W C St STE 860
San Diego, CA 92101-3513

When responding to more than one report, respondents must respond to each report separately.

You are encouraged to use the Response to Grand Jury Report Form, attached, to help format and organize your response. An electronic version of the form is available upon request from the Grand Jury.



Grossmont Union High School District
Educational Technology Services

Response to San Diego County Grand Jury
Cybersecurity in San Diego School Districts

Richard D. Roberts, Executive Director

Richard D. Roberts

Last update: July 16, 2024

Contents

Purpose 1

Findings 1

Recommendations 2

 Implemented 2

 Plan to Implement..... 2

Purpose

This document is Grossmont Union High School District's (GUHSD) formal response to the San Diego County Grand Jury report "Cybersecurity in San Diego Schools" filed and released to the public June 18, 2024. This report is included with to the "Response to San Diego County Grand Jury Report Form." The report addresses findings and recommendations and includes a brief explanation and timeframe where appropriate.

Response, including this report must delivered along with the above-mentioned form to:

The Honorable Maureen F. Hallahan
Presiding Judge of the Superior
Court County of San Diego
P.O. Box 122724
San Diego, CA 92112-2724

San Diego County Grand Jury
550 W C St STE 860
San Diego, CA 92101-3513

Findings

Grossmont Union High School District agrees with all findings numbered 1 through 7 and listed below.

- F1. The San Diego County Office of Education provides high-quality cybersecurity readiness tools and services to county school districts at no or very low cost.
- F2. School districts have varying levels of cybersecurity training: content, frequency, and target audiences.
- F3. Preventable human behavior is the main cause of successful cyberattacks.
- F4. Multi-factor authentication is the most effective cybersecurity technical measure to reduce successful cyberattacks.
- F5. Some school districts do not have a clearly identified role on the district staff responsible for cybersecurity readiness.
- F6. A school district leadership's lack of engagement with cybersecurity issues can impair a district's readiness.
- F7. Obtaining cyber insurance helps a school district to both prepare defenses against and recover from cyber-attacks.

Recommendations

Implemented

Grossmont Union High School District has implemented recommendation 7.

R7. School districts evaluate the feasibility of obtaining cyber insurance coverage by the beginning of the 2025-2026 school year.

Response: Grossmont Union High School District had cyber insurance coverage in place prior to meeting with the Grand Jury in February 2024.

Plan to Implement

Grossmont Union High School District plans to implement recommendations 1 through 6.

R1. School districts provide cybersecurity training to all staff members, at least annually, by the beginning of the 2026-2027 school year.

Response: The district is currently evaluating training material available in the JPA Learning Library, material available through the SDCOE Cybersecurity team, and is in discussion with the district's current endpoint protection provider, Sophos, regarding their staff training program. Target implementation is no later than fall of 2025.

R2. School districts provide cybersecurity training to all students, at least annually, by the beginning of the 2026-2027 school year.

Response: The district is currently evaluating training material available through the SDCOE Cybersecurity team, Google, and is actively looking for other sources of electronic material. The objective is to find relevant material for inclusion in the district's Schoology learning management system for students. Target implementation is fall of 2025.

R3. School districts implement a phishing awareness training solution for all staff members by the beginning of the 2026-2027 school year.

Response: The district has a training session with the SDCOE Cybersecurity team in July of 2024 regarding the capabilities and utility of Red Herring. The district also intends to evaluate training material available through the district's current endpoint protection provider, Sophos. Target implementation is spring of 2025.

R4. School districts implement multi-factor authentication for all staff members by the beginning of the 2026-2027 school year.

Response: GUHSD has two environments that require multi-factor authentication (MFA), Google and Microsoft. Educational Technology Services (ETS) staff will begin investigating MFA solutions for the Microsoft environment no later than January 2025. MFA is already available at user discretion within the Google environment. Discussion with executive leadership and labor partners will begin no later than January 2025 with a target implementation of fall 2025 across both environments for all staff.

R5. School districts designate a single individual as Cybersecurity Lead responsible for cybersecurity readiness in the district by the beginning of the 2025-2026 school year.

Response: Educational Technology Services is engaged in a series of meetings in the spring of 2024 with the following objects:

Current State Updates

- Clearly Defined Roles
- Standardized Project Management Practice
- Cross-Functional Teams
- Cross Training
- Clearly Defined Department Processes and Procedures

Future State Package

- Modernized Job Descriptions
- Modernized Organizational Chart

An outcome of this series of meetings will be the designation of a cybersecurity team of which one member will have the lead role. Target designation of cybersecurity team is October 2024.

R6. School districts require the Cybersecurity Lead to provide an annual report to the school board and the SDCOE on the state of cybersecurity readiness by the beginning of the 2025-2026 school year.

Response: GUHSD ETS staff will draft a framework for the required report to the school board and SDCOE by the end of October 2024. This framework will evolve as the team updates it with content in preparation for presentation to the school board at the end of the 2024-2025 school year and forwarding to SDCOE.