# RESPONSE TO SAN DIEGO COUNTY GRAND JURY REPORT FORM

**Report Title:** Cyber Security in San Diego School Districts

**Response Provided by:** San Diego Unified School District

## 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: (none).

  *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 3, 4, 5 and 7 **have been** implemented.

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

  *Response: The recommendation has been implemented. Beginning in the 2023-24 school year, the district began conducting district-wide phishing awareness training/campaigns using the SDCOE provided solution 'Red Herring'. This training will continue to be part of the overall districtwide cybersecurity awareness and preparedness efforts.*

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

  *Response: The recommendation has been implemented. As of December, 2022 all district employees were required to utilize Multi Factor Authentication (MFA) to access most district applications.*

  *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: The recommendation has been implemented. In March 2022, SDUSD hired its first dedicated Cybersecurity technical position. The position filled is titled Information Systems Architect - Cybersecurity and the district is currently evaluating expanding its Cybersecurity support by creating an additional position that further supports the evolving cyber threats facing education institutions.*

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

*Response: The recommendation has been implemented. SDUSD has carried cyber insurance for several years and continues to keep up with constantly increasing compliance requirements in order to continue cyber insurance coverage in the future.*

- Recommendations numbered 1 and 6 **have not yet been** implemented but will be implemented in the future, with a targeted completion date of the end of the 2024-25 school year.

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

  *Response: The recommendation has not been implemented but will be implemented in 2024-25. All district staff will begin requiring annual email safety training, and basic cybersecurity training starting in the 2024-25 school year as part of the other mandated/mandatory training that district staff must complete annually. As with all mandated/mandatory district training, participation will be tracked and managed for completion of the required training.*

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

  *Response: The recommendation has not been implemented but will be implemented in the 2024-25 school year. SDUSD's IT department did provide the school board a 2023-24 cybersecurity readiness update and will work with SDCOE on the delivery and format required for their reporting requirement.*

- Recommendations numbered 2 **require further analysis**. The further analysis will be completed by December 2024.

  *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.*

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

  *Response: The recommendation requires further analysis, to be completed by December 2024. The SDUSD Instructional Technology Department has developed a student focused Digital Citizenship curriculum for schools to leverage since 2020 and includes some cybersecurity related content, but is currently not required. The district will evaluate adding additional cybersecurity content in the Digital Citizenship curriculum and the implications to require teachers to*

*deliver the content to students annually or via other alternative delivery methods.*

- Recommendations numbered (none) **will not be** implemented because they are not warranted or are not reasonable.

  *Provide an explanation.*

  *N/A*

Signature: Andra M Greene
Andra M. Greene, General Counsel

Date: September 9, 2024

Number of pages attached 0.